

# LUISS



Department of Economia and Management

Chair of Economia Industriale

## Digital trade and cross-border data flows, A comparison between European, US and China policies.

SUPERVISOR:

Prof. Maria Savona

CANDIDATE:

Flavia Basile (253061)

ACADEMIC YEAR

2022/2023

# SUMMARY

<b>INTRODUCTION</b> .....	<b>3</b>
<b>CHAPTER 1</b> .....	<b>6</b>
<b>THE IMPACT OF DIGITALIZATION ON TRADE</b> .....	<b>6</b>
HOW DIGITALIZATION IS CHANGING TRADE .....	6
NEGATIVE SIDES AND CHALLENGES .....	8
DIGITAL TRADE.....	10
CONCLUSIONS.....	12
<b>CHAPTER 2</b> .....	<b>13</b>
<b>WHAT IS DATA AND HOW IT FLOWS</b> .....	<b>13</b>
WHAT IS DATA.....	13
HOW DOES DATA FLOW? .....	15
THE VALUE OF DATA.....	16
IS DATA A PUBLIC GOOD?.....	18
DATA PROTECTION POLICIES.....	19
DATA CHARACTERISTICS AND CONTROL MECHANISMS .....	20
CONCLUSIONS.....	24
<b>CHAPTER 3</b> .....	<b>25</b>
<b>CROSS-BORDER DATA FLOW: OPPORTUNITIES AND CONCERNS</b> .....	<b>25</b>
THE LOCATION OF DATA .....	25
CROSS-BORDER DATA FLOW .....	28
OPPORTUNITIES AND THREATS.....	30
CONCLUSION .....	33
<b>CHAPTER 4</b> .....	<b>34</b>
<b>INTERNATIONAL REGULATORY APPROACHES TO CROSS BORDERS DATA FLOWS</b> .....	<b>34</b>
REGULATORY APPROACHES TO CROSS BORDERS DATA FLOWS.....	34
THE ROLE OF TRUST .....	37
UNILATERAL APPROACHES.....	38
BILATERAL AND PLURILATERAL APPROACHES .....	39
MULTILATERAL APPROACHES .....	40
CONCLUSIONS.....	41
<b>CHAPTER 5</b> .....	<b>43</b>
<b>EU, US, AND CHINA POLICIES</b> .....	<b>43</b>
THE POLICY TRILEMMA .....	43
EU POLICY - A MODEL OF GLOBAL FEDERALISM .....	44
US POLICY- A MODEL OF GOLDEN STRAITJACKET .....	47
CHINA POLICY A MODEL OF BRETTON WOODS COMPROMISE.....	52
CONCLUSIONS.....	55
<b>CONCLUSIONS</b> .....	<b>56</b>
<b>BIBLIOGRAPHY</b> .....	<b>58</b>

## INTRODUCTION

This paper “Digital trade and cross-border data flows, a comparison between European, US, and China policies” briefly provides the main topics for discussion such as the impact of digital transformation on various sectors, including trade, and focuses on the flows of data across borders.

Digital transformation has brought both opportunities and challenges for businesses, policies and society as a whole. With the advent of digital technologies, cross-border trade has become easier and more efficient. It has revolutionized the way businesses operate and trade with each other, the use of digital platforms and online marketplaces has enabled businesses to reach customers all over the world and has created new opportunities for trade by allowing companies to reach new markets, reduce costs and increase efficiency.

However, the impact of digitalization on cross-border trade and data flows is not without its challenges such as privacy and security.

As digitalization continues to transform the global economy, governments, businesses and individuals must work together to ensure that the benefits of digitalization are realized while mitigating the potential risks.

This thesis aims to provide a general introduction to the world of data and its flow, starting with basics such as definitions of the term data and moving on to more complex concepts such as the economic and social role it plays and its policy implications.

Chapter 1 of the thesis focuses on the impact of digitalization on trade.

The first topic of this chapter is how digitalization is changing trade and transforming the way businesses operate. The second topic is the negative sides and challenges associated with it: although digitalization has brought many benefits to businesses, it has also introduced several challenges. For instance, the digital divide between countries has resulted in unequal access to technology.

The third topic of the chapter is “digital trade”, this type of trade has become increasingly popular in recent years; the sub-section discusses the growth of the digital economy and the need for regulations to govern them.

Chapter 2 focuses on explaining the nature of data and how it flows within various systems.

The first section of the chapter defines data and the role it plays through the DIKW hierarchy; the second section explains the various channels through which data moves, such as the internet and networks, and briefly explains encoding and decoding mechanisms. The third discusses the increasing value of data in today's economy and society. The fourth section explores the debate around whether data should be considered a public good, similar to air or water. It touches on the argument that it should be shared freely and made accessible to everyone, or the counterargument that it should be treated as a private asset that individuals and organizations can monetize. The following topic

concerns data protection policies that are an important tool for ensuring that an organization handles personal data responsibly and ethically, while minimizing legal and reputational risks. Finally, the last section discusses the importance of categorization for cross-border data flows. Commercial data and government data are the two main categorizations. Then there is a distinction between personal data and sensitive data and it is explained that both, and especially the second, require more restrictive access and sharing regimes. The idea of personal data ownership is also discussed, but this concept has legal and practical challenges. The sub-section highlights the importance of data protection regulations in protecting individuals' rights and building trust, but compliance can raise costs for firms.

Chapter 3 covers the topic of cross-border data flows, it discusses the policies adopted by countries regarding data location. It highlights that the location of data storage often determines whether its transfers take place across borders. It introduces implications and challenges associated with cross-border data flows and explains why governments are increasingly regulating the internet and restricting information flows for many reasons, such as promoting local companies, causing commercial harm to foreign businesses, and national sovereignty.

Chapter 4 explores three general regulatory approaches to cross-border flows of personal data: the open transfers model, the conditional transfers model, and the limited transfers model. The second sub-section explains why trust is crucial in facilitating data flows and that it can be promoted by government policies and informal initiatives. The challenge for policymakers is to promote the free flow of data while maintaining trust, as the various approaches taken by different regulators have resulted in a fragmented regulatory landscape. However, there are shared characteristics and areas of agreement that policymakers can utilize to establish trust and encourage future collaboration.

The chapter discusses different approaches that countries can take to regulate cross-border data flows. Unilateral approaches involve mechanisms that enable data transfers under certain conditions, such as open or pre-authorized safeguards. Bilateral approaches involve agreements and cooperation between two countries, while plurilateral approaches involve multiple countries working together to establish common rules and standards for the protection of personal data. Multilateral approaches refer to the collective effort of multiple countries to establish a framework or agreement that regulates the movement of digital information across international borders. These approaches can be non-binding and rely on "soft law," or legally binding with stronger enforcement mechanisms.

In the chapters mentioned, there are many references to the strategic choices adopted by Europe, US and China. They will be helpful to prepare the reader for the final chapter where their policies on cross-border data flows are analyzed more in detail.

Chapter 5 focuses on the three main policies adopted: the European Union's General Data Protection Regulation (GDPR) sets out rules for the transfer of personal data outside the EU; the United States

has developed a complex system of regulations and laws that address data privacy, security, and intellectual property protection; China has adopted the Personal Information Protection Law to govern cross-border data flows, that reflect its emphasis on data sovereignty and national security. In the chapter is also explained the trilemma of cross-border transfer of personal data, each country faces unique commercial and technological circumstances that influence their distinct policy approaches to it. Despite conflicts and legal barriers, the three largest economies make compromises through bilateral or multilateral agreements, allowing for the regional free transfer of personal data.

## CHAPTER 1

### THE IMPACT OF DIGITALIZATION ON TRADE

This chapter gives a general introduction to the role of digital transformation on trade over time. Starting from very basic concepts, the reader will understand how digitalization affects businesses, and its importance from both the demand and the supply side. At the end of the chapter, the reader will get the full picture of the implications related to digital trade, including its main challenges and risks.

#### HOW DIGITALIZATION IS CHANGING TRADE

Digitalization is the process of converting information into digital form, storing, managing, and transmitting it using digital technologies. This includes the use of computers, digital cameras, mobile devices, and other electronic devices to capture, store, and manipulate data. Digitalization has revolutionized many aspects of our lives, from the way we communicate and consume media, to the way we do business and access services. It has enabled new forms of innovation, such as online marketplaces and social networks, and created new opportunities for efficiency and cost savings in many sectors.

The digitalization process has its roots in the mid-20th century when electronic computers were first invented. However, the modern digital era, characterized by the widespread adoption of digital technologies and the internet, began in the 1980s and 1990s.

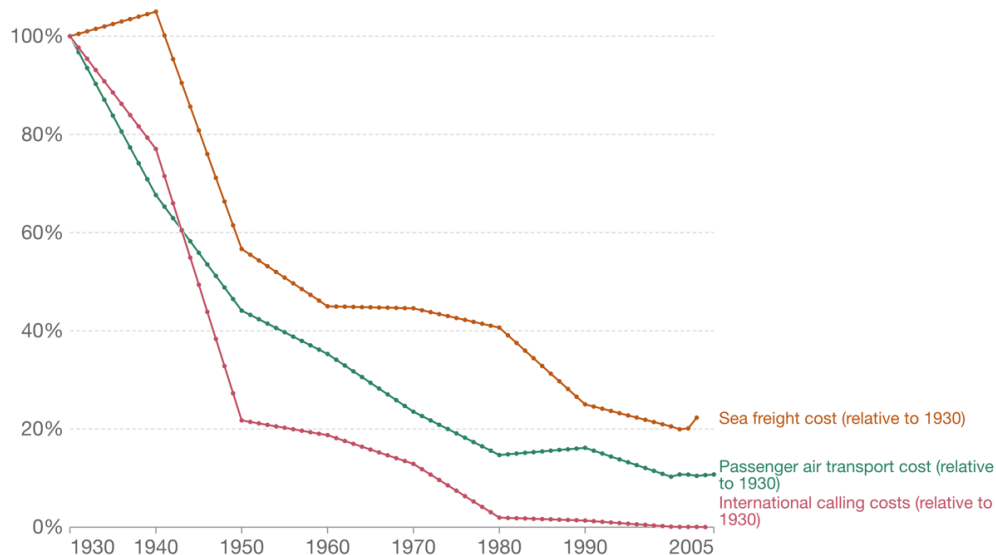
During this period, significant progress was made in the development of personal computers, telecommunications, and the Internet. The introduction of the World Wide Web in 1991 and the subsequent explosion of Internet use in the late 1990s and early 2000s marked a milestone in the process of digitalization. Since then, digital technologies have continued to evolve rapidly, with innovations such as smartphones, social media, cloud computing, and artificial intelligence transforming the way we live, work, and communicate.

Digitalization has completely transformed the business world in terms of both the demand and supply of goods and services.

From a business perspective, the reduction of transport and coordination costs has enabled the fragmentation of production along global value chains in which different stages of the production process are located in different countries. According to the transaction cost theory, companies are

motivated to restructure their operation internationally through outsourcing and offshoring to produce goods wherever the necessary skills and materials are available at both competitive costs and quality<sup>1</sup>.

*CHART 1: The decline of transport and communication costs relative to 1930- Sea freight corresponds to average international freight charges per ton. Passenger air transport corresponds to average airline revenue per passenger mile until 2000 spliced to US import air passenger fares afterward. International calls correspond to the cost of a three-minute call from New York to London. Source: Transaction Costs - OECD Economic Outlook (2007).*



In addition, there has been an increase in the scale and speed of trade due to the breaking down of trade barriers; allowing firms to bring their products and services to digitally connected customers around the world. Thanks to innovative digital tools, businesses overcome their barriers to growth by benefiting from alternative ways of financing such as crowdfunding, which consists of websites that allow interaction between fundraisers and the crowd; moreover, businesses reduce their costs as new business models are changing the production and the supply of goods.

<sup>1</sup> Transaction Cost Theory (TCT) is a key theoretical foundation for explaining ITO decisions and outcomes, as stated by Whitten and Wakefield in 2006. Many IT outsourcing studies have used TCT as their theoretical basis, either alone or in combination with other theories. TCT is particularly useful because it explicitly addresses boundary decisions and is grounded in an economic rationale, offering an alternative view to social, political, and institutional theories, as argued by Lacity and Hirschheim in 1993. Essentially, TCT proposes that several characteristics of a transaction, such as an asset specificity, frequency, and uncertainty, determine the appropriate governance structure for that transaction. These characteristics affect the total transaction and production costs associated with an activity, which, in turn, determine the most efficient governance structure for that activity, whether outsourcing or internal organization. By considering these transaction characteristics, decision-makers can conduct transactions in a cost-efficient manner. – Source: Alagheband, Forough Karimi, et al. "An assessment of the use of transaction cost theory in information technology outsourcing." *The Journal of Strategic Information Systems* 20.2 (2011): 125-138.

Digitalization is also changing the way companies trade goods: online platforms have affected every sector of the economy, particularly finance, communications, retail, and business services. As online shopping continues to grow, sellers will need to find ways to stand out from the competition, they need to leverage what makes their product unique and create engaging experiences that build buyer loyalty. Digitalization also offers opportunities to reach more consumers using online advertising, retail strategies and market segmentation.

If we look at the demand side, consumers feel more comfortable buying online as they become more familiar with the process and its benefits. For instance, online shopping eliminates the need to deal with traffic and parking, it also gives buyers the ability to compare prices and find the best deals.

Furthermore, by increasing market transparency, technology has reduced the costs of information search, which translates into more competition, lower prices, lower price dispersion and increased consumer surplus. Consumers also get services quicker due to fewer intermediaries.<sup>2</sup>

E-commerce has also changed the communication behavior of consumers: the traditional method by which people shared or obtained information before making a decision, the so-called word-of-mouth (WOM), has taken the form of discussion groups, forums, blogs, and networking sites. This phenomenon is so widespread that one can speak of electronic word-of-mouth (eWOM); it has a great social impact as consumers are involved and actively participate in discussions by providing opinions and advice. In this context, involvement, the credibility of information and its quality are important communication vehicles that generate a positive or negative eWOM.<sup>3</sup>

## NEGATIVE SIDES AND CHALLENGES

What has been said so far about the changes and benefits of digital transformation, however, also has negative aspects and challenges.

While first movers benefited most from the digital transformation, other countries have a strong digital divide. The gap is between wealthy countries, which are widely digitally connected, and the poorer ones. That is because richer countries own infrastructures, code and data and reap the benefits of the global digital economy. It is estimated that over 90 percent of the world's data centers are in Western Europe, North America and East Asia. Similarly, a handful of companies (Amazon, Google,

---

<sup>2</sup> Digitalization of Services: What does it imply to trade and development? (UNCTAD/DITC/TNCD/2021/2) 25 Mar 2022.

<sup>3</sup> Hussain, Safdar, Xi Song, and Ben Niu. "Consumers' motivational involvement in eWOM for information adoption: The mediating role of organizational motives." *Frontiers in psychology* 10 (2020): 3055.



Alibaba, Alphabet, Facebook, Microsoft, ...) have achieved a dominant market position, overshadowing all competitors that have lagged in digitalization.<sup>4</sup>

As physical commerce is going digital, a focal point is that the digital economy is generating negative externalities including ratcheting-up climate change. Tech firms are considered the most environmentally damaging in the world, as they need rare minerals to produce their devices. In addition, big corporations have a strong impact on global emissions.

Another major factor in an economy that is so open to international trade is dependent on imports from foreign countries and the risk of a sudden stop in supplies. Interdependence between countries causes the propagation of systemic risk, which means that an economic crisis that erupts in one country has consequences for all countries commercially linked to it.

There are currently new and challenging goals to improve the well-being of citizens by leveraging the potential offered by digital transformation, the main areas to focus on are efficiency, sustainability and inclusivity.

In terms of efficiency, artificial intelligence and machine learning can automate repetitive and time-consuming tasks; organizations can collect and analyze large amounts of data quickly and accurately; employees can work from anywhere, at any time, enabling faster decision-making and problem-solving.

Digital transformation can play a significant role in improving sustainability: digital technologies can help reduce energy consumption by optimizing energy use, automating systems and managing resources more effectively; they enable companies to identify and reduce waste, improve efficiency, and reduce their environmental impact; such technologies can also help companies design sustainable products and identify areas of waste, and monitor environmental impact.

Regarding inclusiveness, for the United Nations Development Programme (UNPD), “inclusive digital transformation is about improving the availability, accessibility and adoption of digital technologies for all”. Inclusiveness can be improved by providing greater access to services and information for people who have been excluded due to physical or geographical barriers; digital technologies enable personalized services and experiences that can better meet the needs and preferences of individual users, especially for people who may have unique needs that require tailored solutions.

Countries lacking digital resilience and market power fall behind, so ensuring a fairer global digital economy will lead to more fairly distribution of gains and minimization of losses.

---

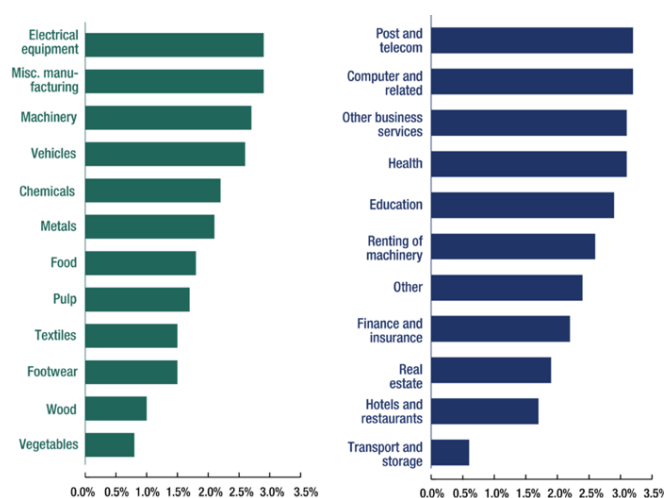
<sup>4</sup> Muggah, Robert, Rafal Rohozinski, and Ian Goldin. "The dark side of digitalization—and how to fix it." *The World Economic Forum*. URL: <https://www.weforum.org/agenda/2020/09/dark-side-digitalization> (дата звернення: 17.10.2020). 2020.

## DIGITAL TRADE

Digital trade refers to the commercial transaction of goods or services enabled by digital technology through digital platforms such as the Internet and mobile networks. Transactions, which can be either digitally or physically delivered, involve consumers, businesses, and governments.

There is a positive relationship between the number of e-commerce companies and economic growth, indicating that when a country's economy continues to grow and e-commerce levels continue to improve, the number of e-commerce companies, trade and user engagement increases. Over the last centuries economic growth has been accompanied by even faster growth in global trade.

CHART 2<sup>5</sup>: Digitalization has a positive impact on trade in goods and services.



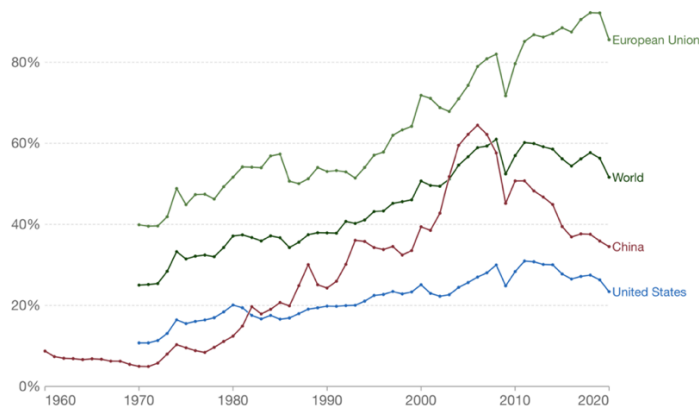
Note: The figure shows the percentage increase in exports as a result of a 10% increase in bilateral digital connectivity and is derived from a gravity model on a sample of 160 countries.

To get an idea of commercial openness around the world, we can use the trade openness index which is an economic metric calculated as the ratio of a country's total trade (the sum of exports and imports) to the country's gross domestic product. The index captures all incoming and outgoing transactions, showing the influence of trade on national economic activity.<sup>6</sup>

<sup>5</sup> Source: López González, J. and J. Ferencz (2018), "Digital Trade and Market Openness", *OECD Trade Policy Papers*, No. 217, OECD Publishing, Paris, <https://doi.org/10.1787/1bd89c9a-en>.

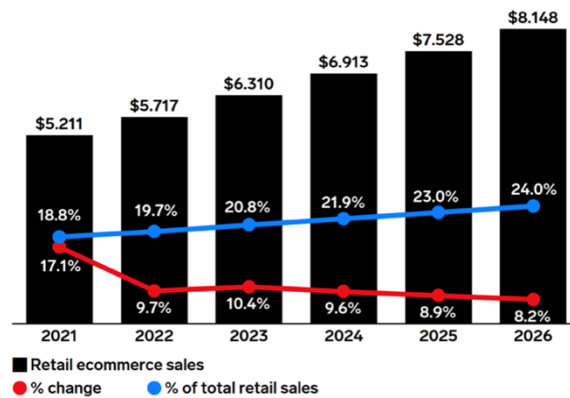
<sup>6</sup> Esteban Ortiz-Ospina, Diana Beltekian and Max Roser (2018) - "Trade and Globalization". Published online at OurWorldInData.org. Retrieved from: '<https://ourworldindata.org/trade-and-globalization>' [Online Resource].

CHART 3: Trade as a share of GDP, 1960 to 2020. Shown is the “trade openness index” – the sum of exports and imports of goods and services, divided by the gross domestic product. Source: World Bank and OECD.



The trade openness index gives us an idea of integration, as it shows that almost 60 percent of the global GDP is related to trade. By analyzing the trend of the index, we can see that it has grown significantly over the last 50 years, from just over 20 percent in the 1970s to 57 percent in 2021. When comparing the European Union, China and the United States, we notice that in the first place, with an index exceeding 80 percent, is the EU, while China and the US remain below the world average (just under 40 percent for China and just over 20 percent for the US).

CHART 4: Retail E-commerce Sales Worldwide, 2021-2026 (trillions of dollars, % change, % of total retail sales).- Source: Emarketer, June 2022.



Note: the chart includes products or services ordered using the internet, regardless of the method of payment or fulfillment; excludes travel and event tickets, payments such as bill pay, taxes, money transfers, food services and drinking place sales, gambling and other vice goods sales.

The size of global retail sales is increasing year by year, in 2021 its value was about \$5.211 trillion, while today (in 2023) it is \$6.310 trillion and it is estimated to continue growing in the coming years,

in 2026 its value is expected to reach \$8.148 trillion. E-commerce sales will increase by about 9.7% compared to last year, while growth is expected to decrease, albeit slightly, in the coming years.<sup>7</sup>

## CONCLUSIONS

Digitalization has favored the process of globalization allowing for a strong integration between countries. As said before, that is a big opportunity but also a source of risk for individuals and the economy in general. The process is now unstoppable, it has reached an exponential dimension and it is expected that will continue to grow in the following years. In this context, the role of the policies is to address the potential of digitalization to economic and sustainable growth.

At the heart of digital trade there is the movement of data, which will be discussed afterward.

---

<sup>7</sup> *Worldwide Ecommerce Forecast Update 2022 - Digital Sales Growth Plummets as Overall Retail Returns to Pre-Pandemic Trendlines- Report by Ethan Cramer-Flood | Jul 29, 2022*

## CHAPTER 2

### WHAT IS DATA AND HOW IT FLOWS

After having introduced the concept of digitalization, the analysis focuses on the role of data. Before talking about more complex topics, in this thesis will be defined the basic concepts of data such as the meaning of the term and the way it flows, and then move on to more technical analyses such as the economic value it assumes, and the ethical discussions related to it such as whether or not it is a public good. Finally, we will analyze the task of data policies and the role of data control mechanisms.

#### WHAT IS DATA

The term “data” comes from the Latin noun “datum” which literally means “something given” and refers to an assumption or premise from which inferences may be done. Today, the word refers to individual facts, statistics or numbers collected to help the decision-making process.

In computing science, the term describes “the quantities, characters, or symbols on which operations are performed by a computer, which can be stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media”<sup>8</sup>. According to this understanding, then, data is translated into an electronic form (binary digital form) that can be stored and used by a computer for movement or processing.

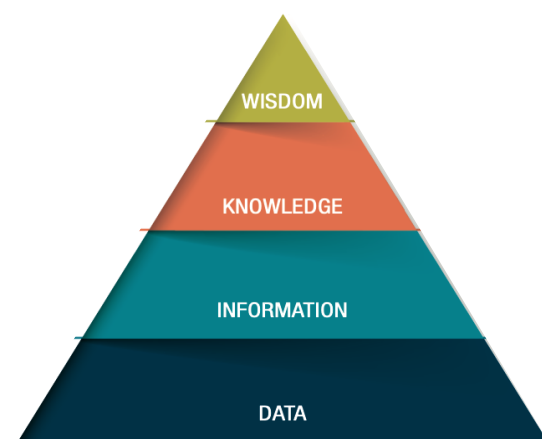
Starting from the definition, data itself, given without context, is useless as it is a collection of unprocessed and unorganized points. The quote: “You can have data without information, but you cannot have information without data” by Daniel Keys Moran helps to better explain what has been said so far.

According to the Data-Information-Knowledge-Wisdom hierarchy, data becomes information when analyzed or aggregate to identify a relationship between them. Knowledge comes from the ability to understand how to apply information. Finally, “wisdom” occurs when acquired knowledge is used to make proactive decisions.

---

<sup>8</sup> What is data? – Source: Data Education in schools

FIGURE 1<sup>9</sup>: The DIKW hierarchy. - Source: UNCTAD, based on United States Chamber of Commerce Foundation (2014).



The DIKW model shows the potential value and the importance of data as the basis for the decision-making process, providing valuable insights that can be useful to solve complex problems and improve processes while minimizing error margins.

Reality is different, because knowledge is much more complex and the DIKW model does not reflect the many factors that influence the way people understand and use information, but it is still used as a simple and strong metaphor.

The starting point of our analysis is based on the idea that data is the backbone of the decision-making process.

Organizations recognize the value of data and strive for its efficient and effective management, increasingly consolidating into data-driven business models, harnessing data and digital technologies to support their strategic choices, acquire innovation capabilities, capture the value demanded by the market and be more competitive.

Data-driven prediction machinery can improve productivity through the value chain and enable the production of more customized products and services in both business-to-consumers (B2C) and business-to-business (B2B), they can also be used to create complex and detailed user profiles. It is estimated that an organization that adopts Big data technology has the potential to increase its profit

---

<sup>9</sup> UNCTAD. *Digital Economy Report 2021: Cross-border Data Flows and Development-For Whom the Data Flow*. UN, 2021.

margin by approximately 60 percent (Nedelcu, 2013); unfortunately, on average, between 60 percent and 73 percent of all data produced by a company remains unused for analysis.<sup>10 11</sup>

## HOW DOES DATA FLOW?

Data are generated during every daily activity, from a variety of sources and in different formats; the development of technologies such as the Internet of Things (IoT), big data analytics, smart devices, and software applications, has led to exponential growth in the volume of data.

Once generated, data are gathered according to their types and sources; there are two main ways for collecting data in business analytics<sup>12</sup>:

- The primary methods imply first-hand data collected by researchers through surveys, interviews, focus groups, forms, and social media monitoring. Primary data are highly accurate, but this method is expensive and time-consuming.
- The secondary methods consist of “second-hand data collected by other parties and already having undergone statistical analysis” (Simplilearn, 2023). To get secondary data, researchers consult data sources such as sales reports, trade magazines, the internet, and financial statement.

After data is processed, it can be stored for later use or it can flow through a system comprised of software, hardware, or both.

Data flows are defined using a model or diagram in which the entire process of movement of data from a source to a destination is mapped within a program or system, taking into account how it changes shape during the process. Dataflow diagrams (DFD) are types of flowcharts designed to map the transmission of data throughout a system.<sup>13</sup> DFD symbol system presents four components: external entities, processes, data stores and data flows.

---

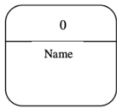

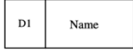
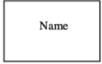
<sup>10</sup> Gualtieri, Mike. "Hadoop is data's darling for a reason." *Jan-2016*. [Online]. Available: <https://go.forrester.com/blogs/hadoop-is-datas-darling-for-a-reason/>. [Accessed: 08-Apr-2018] (2016).

<sup>11</sup> The potential of open data to help businesses- The World Bank. <https://wdr2021.worldbank.org/spotlights/the-potential-of-open-data-to-help-businesses/>

<sup>12</sup> Taherdoost, Hamed. "Data Collection Methods and Tools for Research; A Step-by-Step Guide to Choose Data Collection Technique for Academic and Business Research Projects." *International Journal of Academic Research in Management (IJARM)* 10.1 (2021): 10-38.

<sup>13</sup> Li, Qing, and Yu-Liu Chen. "Data flow diagram." *Modeling and Analysis of Enterprise and Information Systems*. Springer, Berlin, Heidelberg, 2009. 85-97

FIGURE 2<sup>14</sup>: Symbols for DFD elements.

Symbol	Element Name
	Process
	Data Flow
	Data Store
	External Entity

The main medium enabling data flows is the Internet, which is a global network of computers, each of whom is identified by an IP (Internet Protocol) address. Since its dissemination, it has provided an opportunity for people to connect and share ideas and information in real-time and with almost no costs of transaction.

Data flow on the internet through a complex network of devices and systems. The data sent is first converted into digital signals and transmitted over a physical network of wires, fiber optic cables, or wireless connections. Data travels through various intermediary devices such as routers, gateways, and switches which help direct the data to its intended destination. These devices determine, with the support of complex algorithms, the most efficient path for the data to take, based on factors such as network congestion, bandwidth availability, and the distance between the source and the destination. Once data arrives at its destination, it is decoded back into a format that can be understood by the receiving device by involving protocols and encryption.

Data sent through the internet travel in “packets”. Initially, it is not possible to know the path that packets will take to reach their destination. However, after the process is concluded it is possible to trace the route that they followed.

## THE VALUE OF DATA

The metaphor “Data is the new oil”, used by the mathematician Clive Humby in 2006, is particularly helpful for understanding the role of this asset in a digital economy. Like oil, raw data is not valuable in itself, value is created when it is gathered accurately and linked to other data.

---

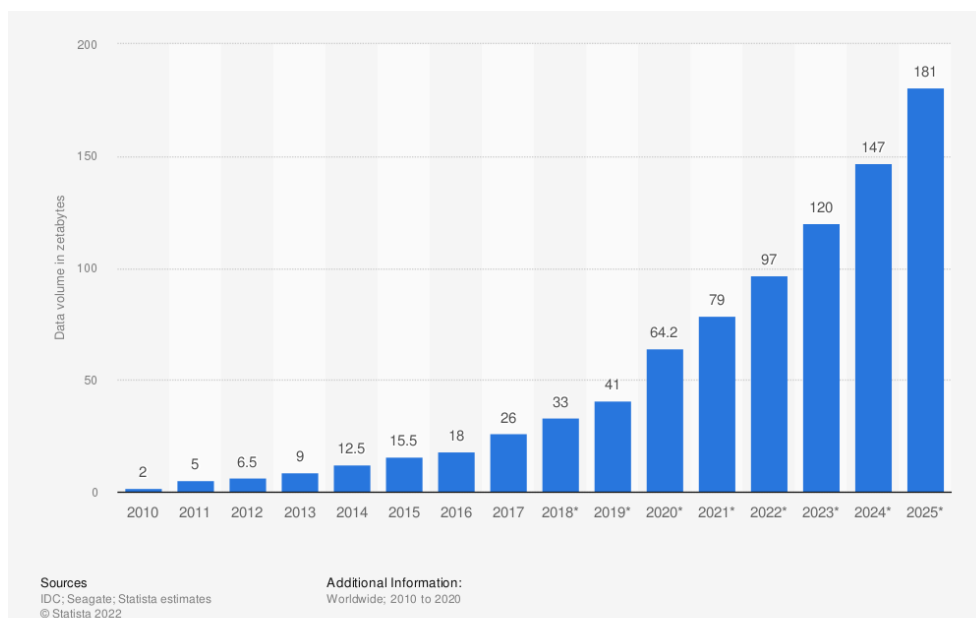
<sup>14</sup> Ibrahim, Rosziati. "Formalization of the data flow diagram rules for consistency check." arXiv preprint arXiv:1011.0278 (2010).



Currently, this quote is even outdated as data is way more valuable than that, suffice it to think that only in 2021, International Data Corporation estimated the value of the data economy in the U.S. at USD 255 billion, and that of the European Union at USD 110 billion<sup>15</sup>.

In 2021, the amount of data generated, copied, and captured in the world was estimated to be around 79 zettabytes and this amount is expected to double by 2025. Growth in the volume of data used has been exponential over the past decade and from 2020, it has been higher than previously expected due to increased demand from the COVID-19 pandemic as more people began working from home. Of all the data now available in the world, only 10% of them is new data while approximately 90% of it is replicated data.<sup>16</sup>

*CHART 5: Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025(in zettabytes).<sup>17</sup>*



<sup>15</sup> How Canada is growing its data economy – Souce: Pavel Abdur-Rahman Partner & Head of Trusted Data & AI, IBM Consulting. May 9, 2022.

<sup>16</sup> Holst, A., 2021. Amount of data created, consumed, and stored 2010-2025. Technology & Telecommunications Retrieved, pp.06-29.

<sup>17</sup> IDC, & Statista. (June 7, 2021). Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025 (in zettabytes) [Graph]. In Statista. Retrieved April 19, 2023, from <https://www.statista.com/statistics/871513/worldwide-data-created/>

As its value plays a central role in our economy and society, the implications of data sharing and data processing are at the center of the discussion from both political and legal perspectives. The main concerns of the authorities relate to data protection and cybersecurity.<sup>18</sup>

A key question is therefore whether and to what extent third parties (users, competitors, non-competing businesses, public bodies) get the possibility to access and (re-)use each other's data for further purposes.

Static efficiency and aspects of dynamic efficiency argue in favor of broad access to data as a public good. On the other hand, if access to data is granted too widely, this can lead to adverse effects since the availability of certain sensitive information may even restrict or distort competition.<sup>19</sup>

### IS DATA A PUBLIC GOOD?

Once we have explained what data is and the role it plays, we need to understand whether it is a public good. This distinction is crucial in regulating access to data: state property pursues public purposes, so public property is accessible to all; on the other hand, private property can be used independently by the possessor to dispose of it for personal purposes.

The starting point of our analysis is to understand the dynamics behind the trade-off between the free flow of data and the exclusive control of data.

Let's start the analysis by describing reasons in favor of data as a public good.

In economics, a public good is a commodity that is both non-excludable, as it can be used by anyone without preventing others from accessing it, and non-rivalrous as the usage of data by one person does not diminish others' ability to consume it. Both characteristics, if artificial restrictions like paywalls, copyright, official and corporate secrecy, and direct censorship are not considered, are inherently applicable to the scope of the data and information generated by them.<sup>20</sup>

Another reason why data should be considered a public good is that it can be used to create social value, such as by providing insights into public health, economic trends, or environmental conditions. Access to data can also facilitate the creation of new products and services, promote innovation, and support scientific research.

---

<sup>18</sup> Schweitzer, Heike, and Robert Welker. "A legal framework for access to data—A competition policy perspective." *German Federal Ministry of Justice and Consumer Protection/Max Planck Institute for Innovation and Competition (eds.): Data Access, Consumer Interests and Public Welfare* (2021): 103-153.

<sup>19</sup> Leistner, Matthias, and Lucie Antoine. "IPR and the use of open data and data sharing initiatives by public and private actors." *Study commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the Committee on Legal Affairs* (2022).

<sup>20</sup> "Information as a public good"- World press Freedom Day 2021, United Nations Educational, Scientific and Cultural Organization. [https://en.unesco.org/sites/default/files/wpfd\\_2021\\_concept\\_note\\_en.pdf](https://en.unesco.org/sites/default/files/wpfd_2021_concept_note_en.pdf)

In many cases, data is created using public funds or resources. It means that the public has a stake in the data and should have access to it. Making data available to the public leads to positive externalities and spillovers as it can help to maximize the return on public investment and promote transparency and accountability. For example, publicly available data sets such as census data, weather data, and scientific research data can be used to inform policy decisions, support scientific research, and drive innovation.

To take one example, effective management of smart health data is critical to improving patient care and health outcomes. Healthcare providers can diagnose diseases, create treatment plans, and improve the quality of patient care by collecting and analyzing data. In addition, that can prompt public health policymakers to respond quickly to problems and provide better health services. Citing a recent case in point, during the COVID-19 pandemic, data provided by patients was used to calculate: the number of cases, and reproduction rates of the virus and help to estimate effective models to aid vaccine creation.

On the other hand, data can also be considered a private good when it is controlled and used by individuals or organizations for their purposes. In these terms, data can be considered excludable and rivalrous.

Excludability means that individuals or firms can prevent others from using it, while rivalry means that its use by one company may limit the availability of the same data for another company. For example, companies may collect and analyze data to gain insights into customer behavior, improve their products and services, and gain a competitive advantage.

Overall, the classification of data as a public or private good can depend on how it is used, who controls it, and what benefits are derived from its use.<sup>21</sup>

## DATA PROTECTION POLICIES

To ensure that data is used ethically, legally, and in the best interests of individuals and society, we need data policies.

First and foremost, data plays a key role in protecting the privacy rights of individuals by regulating how it is collected, stored and shared. This includes ensuring that personal information is kept confidential and that individuals have the right to know how their data is used and regulating how organizations share personal data with third parties; this may require contracts or agreements that specify its use and sharing.

---

<sup>21</sup> Taylor, Linnet. "The ethics of big data as a public good: which public? Whose good?" *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 374.2083 (2016): 20160126.

Policies can demand organizations implement appropriate data security measures to protect the collected data from unauthorized access to sensitive information, hacking, theft, or breaches. These policies also provide guidelines for the responsible use of data that can include the use of encryption, firewalls, and access controls.

Moreover, such policies can require organizations to delete personal data when it is no longer necessary or when requested by individuals so that it is not stored unnecessarily. Additionally, they can foster the development of new technologies and business models that leverage data in ethical and beneficial ways.

In the corporate sector, Data Protection Policy (DPP) is a set of internal guidelines and rules that an organization implements to ensure the privacy, confidentiality, security, and accuracy of personal data collected and processed by the organization. The policy outlines the measures the organization takes to protect personal data against unauthorized access, use, disclosure, alteration, and destruction. Typically, the policy outlines the organization's approach to data protection, including the types of personal data that are collected and processed, the purposes for which it is used, how it is protected, how long it is retained, and how individuals can exercise their rights regarding their data. The DPP should outline the security measures that are in place to protect personal data against unauthorized access and specify the procedures for notifying individuals and relevant authorities in the event of a breach.

A Data Protection Policy is an important document for any organization that collects and processes personal data as it helps to demonstrate the organization's commitment to protecting individuals' privacy and can also help to ensure that it is complying with data protection laws and regulations.<sup>22</sup>

## DATA CHARACTERISTICS AND CONTROL MECHANISMS

Data categorization is the basis for the processing of cross-border data flows: classifying data has important implications for how it is regulated, shared, and used.

The first way of categorizing data is by who produces and uses it: commercial data and government data will be discussed below.

Commercial data, which results from B2B and B2C interactions, is subject to legal agreements and internal company rules. For cross-border organizations, it is crucial to preserve the control and confidentiality of data, which is at the heart of the company's competitive advantage.

Government data is often considered more sensitive and subject to national regulations, such as encryption and storage requirements. However, there is also a trend towards sharing data between government and non-profit organizations to create economic and social value, particularly in areas

---

<sup>22</sup> The Difference Between a Data Protection Policy and a Privacy Policy - Beverly Davis, 21 February 2022

such as trade, corporate databases, regional governance, and national security. Open data initiatives have also been successful in promoting data sharing and standardization, such as the International Aid Transparency Initiative<sup>23</sup>.

Digital technologies have made interactions between consumers and foreign companies more common, and that caused cross-border data flows involving consumers to require additional rules due to personal data being involved.

After defining data sources, it is necessary to distinguish between personal data and sensitive data. Personal data can be defined as any information related to an identified or identifiable living individual. Information that can lead to the identification of a specific person is also considered personal data as, even if anonymized, data may still indirectly identify an individual. Consequently, if data is encrypted in a way that makes the individual no longer identifiable, it is not considered personal data anymore.<sup>24</sup>

Once classified as personal data, access to and sharing of this data become predominantly governed by the applicable privacy framework.

As global data protection regulations have increased, researchers have explored new methods to effectively anonymize data while maintaining its usefulness. Two examples of these techniques include data perturbation, which adds random noise to data to ensure individual anonymity while maintaining structure, and synthetic data, which generates artificial data that mimics the characteristics of real data without representing individuals. With the spread of machine learning, trained data models and algorithms may also be used as an alternative to personal data and, once properly trained, model data can be shared for applications with lower risks. These approaches to anonymization are important for the protection of human rights, as they reduce the risk of identifying users and could potentially support the sharing of personal data as digital public goods in the future. Personal data is considered sensitive if it reveals: “racial or ethnic origin, political opinions, religious or philosophical beliefs; trade-union membership; genetic data, biometric data processed solely to

---

<sup>23</sup> International Aid Transparency Initiative is a global initiative to increase the openness of humanitarian and development resources and the outcomes they provide to combat poverty and crises. IATI brings together governments, multilateral organizations, businesses, and organizations from the civil society to promote the transparency of aid going to developing nations.

It encourages all organizations who disperse or invest resources to disclose statistics regarding their humanitarian and development efforts using the IATI data standard. This is a set of guidelines and standards to make ensuring that information is simple to find, comprehend, and use. -Source: <https://iatistandard.org/en/>

<sup>24</sup> What is personal data? -Source: European Commission.EU

[https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data\\_en](https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en)

identify a human being; health-related data; data concerning a person's sex life or sexual orientation" (Article 4, Article 9 and Recitals 51-56 of the GDPR).<sup>25</sup>

Sensitive data is subjected to additional rules on storage or flows.

Thus, from a privacy perspective, personal and especially sensitive data requires more restrictive access and sharing regimes than, (non-personal) public sector ones, which in many cases can be shared through open data.<sup>26</sup>

The idea of individuals owning their data has been proposed as a solution to data inequalities and to enable individuals to control how it is used. However, the concept of personal data ownership faces legal and practical challenges, such as the difficulty of identifying the party with the clearest interest in the data and how to compensate interested third parties if their rights are breached. Furthermore, personal data ownership might incentivize vulnerable individuals to sell their data, exacerbating existing inequities. Even current case law does not support ownership rights over personal data.<sup>27</sup>

For data governance frameworks to have broad applicability, it is important to distinguish between three distinct domains of data as outlined in the OECD's 2019 report<sup>28</sup>. These domains are:

- The personal domain includes all data that pertain to an identified or identifiable individual (i.e., personal data) that is of interest to subjects in terms of privacy.
- The private domain includes proprietary data that is usually protected by intellectual property rights (IPRs), such as copyright and trade secrets, or other access and control

---

<sup>25</sup> What personal data is considered sensitive? –Source: European Commission.EU

[https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive\\_en](https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en)

<sup>26</sup> “The term “Open Data” means that data or content is open if anyone is free to use, re-use or redistribute it, subject at most to measures that preserve provenance and openness.

There are two dimensions of data openness:

1. The data must be legally open, which means they must be placed in the public domain or under liberal terms of use with minimal restrictions.
2. The data must be technically open, which means they must be published in electronic formats that are machine readable and non-proprietary, so that anyone can access and use the data using common, freely available software tools. Data must also be publicly available and accessible on a public server, without password or firewall restrictions. To make Open Data easier to find, most organizations create and manage Open Data catalogs.” Source: “Open Data Essentials”- The World Bank.

<sup>27</sup> Who owns personal data? – Source: The World Bank

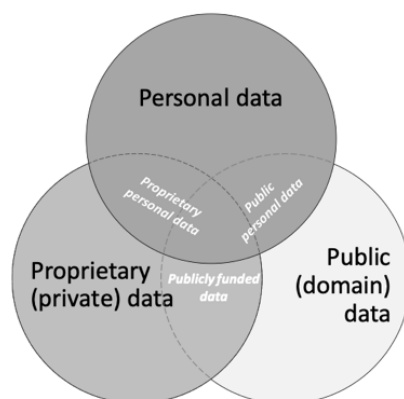
<https://wdr2021.worldbank.org/spotlights/who-owns-personal-data/>

<sup>28</sup> Casalini, F., J. López González and T. Nemoto (2021), "Mapping commonalities in regulatory approaches to cross-border data transfers", OECD Trade Policy Papers, No. 248, OECD Publishing, Paris, <https://doi.org/10.1787/ca9f974e-en>.

rights (e.g., contract and cyber-criminal law), and that has enough economic value to justify the exclusion of others.

- The public domain encompasses data that is not subject to IPRs or any other rights with similar effects and therefore falls under the "public domain" (interpreted more broadly than as simply being free from copyright protection), making certain types of such data accessible and available for reuse.

FIGURE 3: *The personal, private and public domain of data. Source: OECD (2019), Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*



The figure illustrates how the three domains - personal, private, and proprietary - overlap and are subject to different data governance frameworks that can impact each domain differently. Privacy regulatory frameworks typically govern the personal domain, while the private domain may be governed through contractual frameworks or, in some cases, covered by intellectual property rights (IPRs). These overlaps can partly explain the conflicting views and interests of various stakeholder groups, such as those related to "data ownership."

The complexity of data governance, particularly in the context of cross-border data flows, can also be attributed to these overlaps. Depending on the jurisdiction, some domains may be prioritized differently than others, as seen in the variation of privacy and portability rights across countries.

While data portability aims to empower individuals and give them more control over their data, it is unclear which types of data fall within the scope of data portability across different initiatives, reflecting implicit priorities of the personal domain versus the proprietary domain.

Data protection regulations are important for protecting individuals' data rights and building trust, but compliance can raise costs for firms, especially the smaller ones. Data protection policies that reduce the incentives to share personal data or restrict its use can entrench incumbent positions and reduce innovation opportunities. The design of data protection regimes can be reviewed to minimize adverse impacts on the competition while respecting data rights. Evidence shows that the GDPR, as we will analyze more fully below, increased concentration in the web technology sector, with small vendors

losing the most market share; to avoid this phenomenon, differentiated regulatory treatment based on firm size or age may be an option, subject to maintaining data rights. There is growing agreement that a firm's offering on the protection of user data has value to consumers and could be considered a non-price outcome of the competition. Data spillovers may complicate matters, and low-income groups who are price sensitive may be more willing to relinquish their data for "zero" price products or services. Improved cooperation between competition authorities and data protection authorities can help policymakers understand how to develop appropriate data-focused competition remedies while ensuring data protection.<sup>29</sup>

## CONCLUSIONS

This chapter provides background information and insight into the complexity in data categorization and how critical the latter is in data regulation. In fact, regulations rely on these definitions to set stringent policies depending on the type of information that can be transmitted and who uses it.

The analysis conducted also made it clear that access to data should not be too stringent because it can be essential for pursuing public and common good purposes, as was recently the case during the pandemic, and that data also have high potential in the health care area from both a preventive and disease treatment perspective.

To make the most of the opportunities provided by data exchange, it is advisable that data should be able to flow in complete security within countries even while making use of the latest technologies to protect the privacy of individuals.

In the next chapter, the analysis will focus on cross-border data flows so that the reader can better understand the role they play.

---

<sup>29</sup> Balancing data protection and competition - Source: The World Bank

<https://wdr2021.worldbank.org/spotlights/balancing-data-protection-and-competition/>



## CHAPTER 3

### CROSS-BORDER DATA FLOW: OPPORTUNITIES AND CONCERNS

Before talking about opportunities and concerns consequent to the flow of data across borders, we will introduce the central role of data location with a particular focus on the policies adopted by the United States, China, and the European Union and then we will introduce the general concept of cross-border data flows. Finally, we will analyze the consequences that the dataflows have and what are the challenges that it is facing.

#### THE LOCATION OF DATA<sup>30</sup>

The location of data storage often determines whether data transfers take place across borders. The server hosting the website or application with which a user interacts can be located anywhere in the globe. A considerable portion of the world's data is stored in a few industrial-scale data centers, connected to crucial cloud servers, infrastructure, and cloud data warehouses. These data centers are mostly located in developed countries.

In the European Union, the issue of data localization is a matter of controversy, with some countries, including France and Germany, advocating for localization in relevant policies, while others, such as Sweden, advocate for the free flow of data across borders. The European Commission has been working towards creating a Digital Single Market to eliminate obstacles that hinder digital economic activity, such as those that require data localization. The DSA (Digital Service Act), which came into force on 16 November 2022, is a set of rules to protect people from harmful content and to give them more control over online content.

The formation of a Digital Single Market promotes economic growth and generates new jobs. Every citizen can enjoy digital services and content, anywhere in the EU, and every company can offer and sell its products to a market of 500 million people, using online channels without barriers between countries. Today, a small business seeking to expand in the EU no longer has to deal with 27 different regulations for consumer and data protection, for taxation and contract drafting, this reduces costs for both citizens and businesses.

The United States has implemented several data localization requirements in the context of public procurement. The most recent example is the exemption of financial services data from data flow

---

<sup>30</sup> Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? - Source: ITIF By Nigel Cory, May 1, 2017

<https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost/>

barrier rules in the Trans-Pacific Partnership. However, the US sought to limit the scope of this provision through bilateral discussions and provisions in ongoing Trade in Services Agreement negotiations. Federal agencies are required to restrict the location of information systems that process federal tax information within US territories, embassies, or military installations under IRS publication 1075. The Department of Defense also mandates that all cloud-computing service providers that work for them must store data domestically. Some state and local governments impose similar requirements on contractors: for example, the City of Los Angeles required Google to store its data within the continental United States.

China's data-localization policies are among the most extensive in the world, limiting the flow of data between China and other countries. The Ministry of Public Security operates the Golden Shield program, also known as the "Great Firewall of China," which blocks access to certain websites and services critical of the Chinese Communist Party. In addition, China has introduced policies that restrict the transfer of data across its borders, particularly after the Snowden revelations<sup>31</sup>.

For instance, China has implemented measures that require companies involved in e-banking to store their servers in China since 2006. It has also enacted laws prohibiting the offshore processing, analyzing, or storage of Chinese personal financial information since 2011. Similarly, in 2013, new regulations were implemented, mandating that all credit information of Chinese citizens be processed and stored in China. In 2014, rules were put in place to require health and medical information to be stored solely in China. In 2016, rules that compelled companies engaged in Internet-based mapping services to store data locally were implemented.

The Counter-Terrorism Law, which came into effect in 2016, requires providers of critical information infrastructure, including the Internet and telecommunication companies, to store data on Chinese servers and provide encryption keys to government authorities; any movement of data offshore must undergo a security assessment. The same year, a cybersecurity law was passed, requiring various companies to store their users' personal information and other crucial business data within China.

Furthermore, in April 2017, a draft circular outlining extensive localization requirements for businesses transferring data overseas was released. It extended data localization requirements from critical information infrastructure to all network operators: any outbound data transfer that poses a

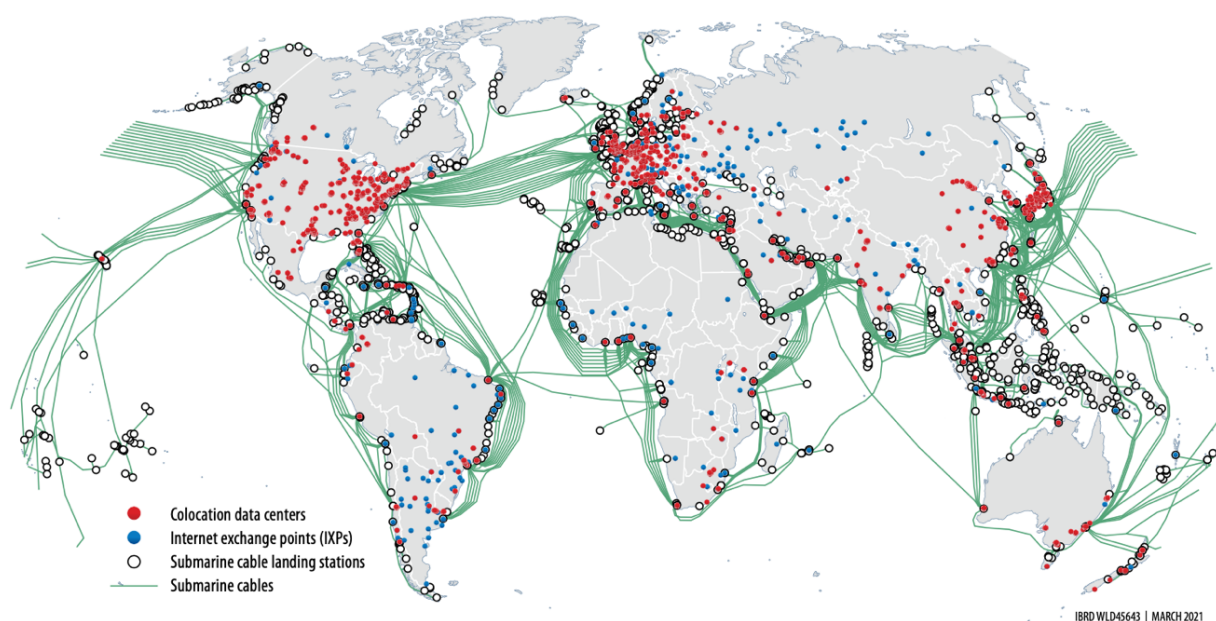
---

<sup>31</sup> Edward Snowden was a 29-year-old technical assistant for the CIA who was responsible, in 2013, for one of the most significant leaks in US political history: he revealed that the National Security Administration was conducting mass surveillance of US residents. His revelations sparked discussions about surveillance, government secrecy, and how to strike a balance between national security and data privacy. These discussions had a significant impact on society and the tech sector.

risk to the security of China's national political system, economy, science and technology, or national defense would be prohibited.

These regulations directly affect trade; in fact, they make it more or less attractive for a foreign company to trade in a particular country. More stringent regulation hinders trade because aligning with regulations is very costly and can discourage firms, especially the smaller ones.

FIGURE 4<sup>32</sup>: Data infrastructure is not yet widespread across all parts of the world. Sources: PeeringDB, Interconnection Database, Packet Clearing House Report on Internet Exchange Point Locations (database), accessed December 14, 2020; TeleGeography, Submarine Cables (database).



Local data storage is often done to address jurisdiction and security concerns as when data is stored outside a country's borders, it can be difficult to access it for legal purposes. Although mutual legal assistance treaties<sup>33</sup> exist to facilitate access to such data, not all countries have them in place. Even when the United States requests data, it can take between 6 weeks to 10 months to obtain access

<sup>32</sup> PeeringDB, Interconnection Database, <https://www.peeringdb.com/>; PCH Packet Clearing House, Packet Clearing House Report on Internet Exchange Point Locations (database), accessed December 14, 2020, <https://www.pch.net/ixp/summary>; TeleGeography, Submarine Cables (database), <https://www.submarinecablemap.com/>. Data at [http://bit.do/WDR2021-Map-O\\_4](http://bit.do/WDR2021-Map-O_4).

<sup>33</sup> “Mutual legal assistance is a form of cooperation between different countries for the purpose of collecting and exchanging information. Authorities from one country may also ask for and provide evidence located in one country to assist in criminal investigations or proceedings in another.”- Source: Mutual legal assistance and extradition- European Commission

[https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/mutual-legal-assistance-and-extradition\\_en](https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/mutual-legal-assistance-and-extradition_en)

(Brehmer, 2018) moreover there have been notable cases where access to data for security reasons has not been granted.

Local storage of data has also been justified for cybersecurity and economic reasons, as it exposes them to the risk of national data surveillance by third countries; economically, local data storage supports infrastructures and drives the digital economy. To mitigate risks, companies often choose to store their data in various locations to ensure diversification.

The localization of data also depends on technical factors such as the availability and reliability of energy.

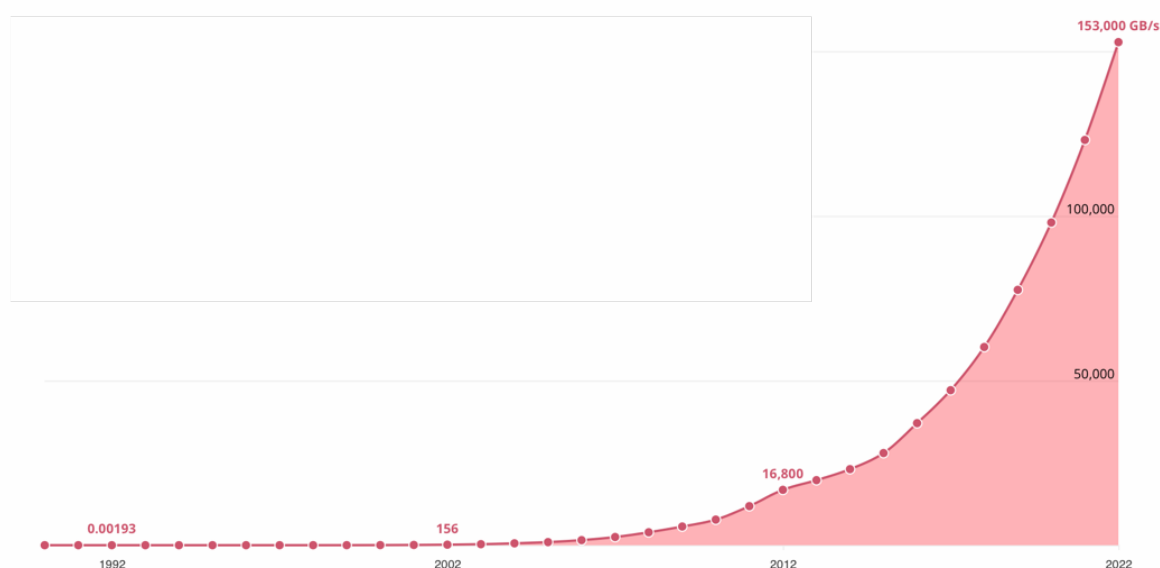
## CROSS-BORDER DATA FLOW

Cross borders data flows support the trading of goods and digital services.

Measuring data traffic is difficult but measuring cross-border data flows is even more challenging: in terms of volume, the measure that is used the most is the total used capacity of international Internet bandwidth. It shows the amount of data flowing without giving any information about the direction of the flows and the nature of the data.

In 2020, global internet traffic was estimated to be more than 3 zettabytes, which is equivalent to 1GB per person per day (WorldBank, 2021). To understand how much the role of the digital economy has grown, one only has to think that in twenty years (2002-2022) the amount of data exchanged has reached a 1,000-fold increase.<sup>34</sup>

*CHART 6: Growth of global internet traffic in the past 30 years, Source: WDR 2021 team calculations and Cisco Visual Networking Index: Forecast and Trends, 2017–2022.*



<sup>34</sup> Crossing borders – The World Bank <https://wdr2021.worldbank.org/stories/crossing-borders/>

The cross-border data flows have increased economic productivity and efficiency and have risen the standard of living and welfare.

Data is intangible and non-rival, it results in varying degrees of excludability as it can be limited by legal or technical means, it also has a multidimensional nature as it can provide both private and social value, it is related to privacy and human rights and national security.

The characteristics of data mean that it requires distinct treatment compared to traditional products and services, including in the way they are transferred. With the emergence of a data-driven digital economy, notions like ownership and jurisdiction are facing new questions. Rather than fixating on the question of data ownership, the crucial factors are determining who possesses the authority to access, manage, and exploit the data.

The management of international trade is influenced by data that depend on the nature, value, and places involved in trading, such as the origin and destination. However, it becomes complicated, or even impractical, to gather statistical data for cross-border data flows because there are no official records for such information. The traditional methods that are widely used for international trade regulations, like rules of origin, cannot be directly applied to digital data because of its nature, which is why cross-border data flows require a different regulation.

Moreover, the concept of digital trade excludes the transfer of raw data that is not directly related to the exchange of goods or services (as defined in the Handbook on Measuring Digital Trade developed by various international organizations).

Interaction by a user within an app could trigger a series of diverse cross-border data transfers. This includes the collection of user data, retrieval of data from cloud storage, and the exchange of data for advertising or other purposes, which may involve intermediate services and organizations.

The United States and China are the leading countries in terms of their ability to participate in and benefit from the data-driven digital economy. They possess half of the world's hyperscale data centers, have the highest rates of 5G adoption globally, account for 94 percent of funding for AI start-ups over the past five years, have 70 percent of the world's top AI researchers, and control nearly 90 percent of the market capitalization of the world's largest digital platforms. These platforms, which include Apple, Microsoft, Amazon, Alphabet (Google), Facebook, Tencent, and Alibaba, are investing in all aspects of the global data value chain, from data collection to data analysis and use through AI.<sup>35</sup> Although these companies have an edge in data because of their platform component, they have evolved into global digital corporations with a global reach, immense financial, market, and technological power, and control over large amounts of user data. During the pandemic, their

---

<sup>35</sup> Inequalities threaten wider divide as digital economy data flows surge – UNCTAD 29 September 2021.

<https://unctad.org/news/inequalities-threaten-wider-divide-digital-economy-data-flows-surge>

size, profits, market value, and dominant positions have increased significantly due to the acceleration of digitalization. For example, between October 2019 and January 2021, while the New York Stock Exchange Composite Index increased by 17 percent, the stock prices of top platforms such as Facebook rose by 55 percent and Apple by 144 percent.<sup>36</sup>

## OPPORTUNITIES AND THREATS

As we have said, cross-border data flows have a significant impact on globalization and the digital economy, but they also raise concerns regarding data privacy, security, and national sovereignty.

The open nature of the Internet has underpinned innovation and created new businesses based on social networking and crowdfunding. However, government interference on the internet is increasingly challenging its original libertarian nature. While some regulation is motivated by the need to address physical world harms that are replicable online, other governments are restricting internet and information flows for less legitimate reasons, such as causing commercial harm to foreign businesses and promoting local companies. Governments are using complex tools to restrict access to the internet and cross-border data flows, including blocking the backbone or access points of the web, filtering domain names, and indirectly regulating search engines.

Within the context we have described through this analysis, we can understand the opportunities and threats arising from cross-border data flows.<sup>37</sup>

Firstly, cross-border data flows allow for collaboration between companies, researchers, and other stakeholders from different countries. This collaboration has great potential to benefit society as it can lead to joint research projects, knowledge sharing, and the development of new technologies. The benefits of data collaboration are not yet exploited except for a small part of their potential: to improve on this front, it is necessary to build trust between data suppliers and users (this point will be discussed in the next chapter).

One of the main opportunities for cross-border data flows comes from the great imbalances that exist in the world. Especially in less developed countries, only 20 percent of people use the Internet and most of them do so at low speeds and high prices. Moreover, in the least developed countries, less than 1 in 10 Internet users shop online, while in developed countries the percentage rises to 8 in 10.

---

<sup>36</sup> Digital Economy Report 2021 - Cross-border data flows and development: *For whom the data flow*. Source: UNCTAD.

[https://unctad.org/system/files/official-document/der2021\\_en.pdf](https://unctad.org/system/files/official-document/der2021_en.pdf)

<sup>37</sup> Meltzer, J. P. (2015). The Internet, Cross-Border Data Flows and International Trade. *Asia & the Pacific Policy Studies*, 2(1), 90-102.



There are also significant differences between rural and urban areas and between genders. The digital divide between developed and developing countries is a challenge for development.<sup>38</sup>

Another opportunity comes from data localization. Although the localization of data centers may not offer significant direct economic benefits, in some cases their presence may be a crucial element of a larger plan to invest in a nation's data capacity and resources. The policy of mandating national data storage may only yield desirable results in larger countries that can achieve the critical mass and scalability necessary to generate value from data. Furthermore, confining data within national borders can only foster economic growth if the country can convert the data into digital insights and capitalize on it. Improving the capacity of developing countries would enable them to equip themselves with the infrastructure and capacity to manage data, which would narrow the gap with developed countries. Data has the potential to bring benefits to both individuals and businesses. People can benefit from improved access to information, goods, and services, while businesses can utilize data to access markets and coordinate global value chains. Cross-border data flows can also foster improved research outcomes in areas such as health, the environment, or law enforcement. For example, sharing health data across borders can facilitate targeted research, as seen during the COVID-19 pandemic. Sharing data for environmental research or to combat crime and detect money laundering can also lead to better outcomes for societies and individuals.<sup>39</sup>

Data flows also offer opportunities for companies to grow their business and expand their markets and access new customers in different countries. It also put MSMEs<sup>40</sup> on an equal footing with large multinationals as it reduces MSMEs' barriers to entry into new markets, enables economies of scale and lower investment barriers facilitating them in accessing market information and know-how. From the cost perspective, cross-border data flows can help companies to reduce costs by allowing them to access services and expertise from different countries at a lower cost, they can also strengthen resilience and reduce vulnerability.

Nonetheless, the transfer of data across borders presents potential hazards and obstacles that must be addressed regarding various public policy goals. The widespread dissemination of data, which includes cross-border movement, has sparked apprehension regarding the utilization and possible abuse of information. This concern extends to power dynamics among companies, interactions

---

<sup>38</sup> Digital Economy Report 2021 - Cross-border data flows and development: *For whom the data flow*. Source: UNCTAD.

[https://unctad.org/system/files/official-document/der2021\\_en.pdf](https://unctad.org/system/files/official-document/der2021_en.pdf)

<sup>39</sup> OECD (2022), "Fostering cross-border data flows with trust", *OECD Digital Economy Papers*, No. 343, OECD Publishing, Paris, <https://doi.org/10.1787/139b32ad-en>.

<sup>40</sup> Micro, Small and Medium Enterprises

between firms and consumers, and the relationship between governments and citizens, particularly concerning privacy and safeguarding personal data.

It is essential to understand that cross-border data flows expose to serious threats if not used correctly. If a global digital platform collects data from users in a specific country and utilizes it for its private gains, without offering any compensation or opportunities for domestic companies to utilize that data effectively, it can create an unfair advantage for foreign entities in terms of data analysis and processing. Even with access to their data, developing countries may find it challenging to catch up to the first-mover advantage held by these entities. To solve this problem, a comprehensive international framework for regulating cross-border data flows should ensure equitable access and guarantee that income gains from data are distributed fairly when access is limited.

Cybersecurity is one of the most discussed points about cross-border data flows. The more data that is being transmitted across borders, the greater the risk of cyber-attacks and data breaches. This can result in significant financial losses and reputational damage for companies. Also, it exposes the country to national security concerns such as cyber espionage, terrorist threats, cyberattacks on critical infrastructures and monitoring of strategic entities and activities like central banks.

Regarding the economic impact of cross-border data flows, it can be negative on certain regions or industries. For example, if companies can outsource jobs to countries with lower labor costs, this can result in job losses in higher-cost countries. This can also lead to concerns about unfair competition and trade imbalances.

Cross-border data flows can also raise concerns about the protection of intellectual property rights: companies may be hesitant to share valuable intellectual property (including trademarks, copyrights, and trade secrets) with partners in other countries due to concerns about theft or misuse.<sup>41</sup>

To improve best practices in data governance, governments should offer various mechanisms for transferring personal data across borders, which should be accessible to firms of all sizes; businesses should enhance transparency about their data management practices, including on a global level, by routinely revealing information about government requests for data. Governments could also endorse initiatives aimed at developing and utilizing digital technology and standards and safeguarding cloud-based government data and services by ensuring that cloud providers comply with national and international standards, sector-specific regulations, national certifications, and global accreditations.

---

<sup>41</sup> Cory, Nigel, and Luke Dascoli. *How barriers to cross-border data flows are spreading globally, what they cost, and how to address them*. Information Technology and Innovation Foundation, 2021.

Chaisse, J. (2023). 'The Black Pit: Power and Pitfalls of Digital FDI and Cross-Border Data Flows. *World Trade Review*, 22(1), 73-89.



Developed economies should provide technical assistance and capacity-building support to developing economies to assist them in establishing their data governance framework.

On one hand, cross borders data flows allow countries to capture value in the global data value chain, on the other hand, appropriate rules are indispensable for guaranteed data rights and support economic development; to find the right compromise between restrictions that may lead to no benefit at all.

## CONCLUSION

The reader has now an idea of the implications related to data location and storage, the main reasons that can push countries to make certain choices and how these choices directly affect the attractiveness of a country in terms of foreign trade.

The chapter has provided an outlook on cross borders data flows and how they can be an opportunity for the catching up process as they can address investments in building infrastructures, for firms as they reduce barriers between countries, and for people as they have easier access to information. On the other hand, the misuse of data can lead to dramatic consequences for both individuals and society. A successful establishment of an open, innovative, and rule-based digital economy on a global scale would require collaboration between a select few proactive and ambitious nations. This approach acknowledges the absence of a universal platform for advancing data-related matters, which is not yet necessary. The Prime Minister of Japan, Abe, introduced the idea of "data free flow with trust," which envisions a mutually beneficial relationship between openness and trust, rather than a conflicting one. Nonetheless, this concept remains theoretical and undefined. To achieve this objective, nations committed to this cause must collaborate and devise novel standards, regulations, cooperative frameworks, and treaties to tackle valid apprehensions arising from transnational data transmission while concurrently promoting the unrestricted flow of data.<sup>42</sup>

---

<sup>42</sup> Greenleaf, Graham. "G20 makes declaration of 'Data Free Flow With Trust': Support and dissent." (2019).

## CHAPTER 4

### INTERNATIONAL REGULATORY APPROACHES TO CROSS BORDERS DATA FLOWS

Many countries are currently regulating cross-border transfers of personal data. This chapter introduces the general regulatory approaches; then it discusses the role of trust to make the system work and finally gives a general overview of the mechanisms of data transmission.

#### REGULATORY APPROACHES TO CROSS BORDERS DATA FLOWS<sup>43</sup>

There are three main general regulatory approaches to cross-border flows of personal data. They are the limited transfers model, the conditional transfers model and the open transfers model. These three data models have become a reference for many other countries when defining their rules on personal data.

The model of open transfers is characterized by the absence of any restrictions on cross-border transfers of personal data. In addition, countries following this model usually rely on a baseline set of privacy principles and leave to companies the flexibility to self-regulate voluntarily. Moreover, under this model, firms usually remain accountable for how personal data is treated, and when they may be transferred to a recipient in a third country. 39 of 116 countries surveyed for the WDR, including the United States, have adopted this model; however, several countries are classified into this model by default, given that they have not (yet) adopted a general framework for personal data transfers or imposed any regulatory rules regarding data protection. This is the case, for instance, in Bolivia, Cambodia, Pakistan, and Saudi Arabia.

The second type of data model is based on conditional transfers, which attempt to balance the protection of personal data with the need for open data transfers. This involves a country establishing a set of regulatory safeguards that its trading partners must comply with in order to allow for the free flow of personal data between companies on both sides. Once these safeguards are met, data can be shared with other jurisdictions that meet certain standards for data protection or with companies that have implemented mandatory data protection protocols, such as binding corporate rules or contractual clauses. Out of 116 countries surveyed, 66 have adopted the conditional transfers model, including

---

<sup>43</sup> Ferracane, Martina Francesa, and Erik van der Marel. "Regulations on Personal Data: Differing Data Realms and Digital Services Trade." *Background paper for World Development Report* (2021).

[https://elibrary.worldbank.org/doi/abs/10.1596/978-1-4648-1671-0\\_ch5](https://elibrary.worldbank.org/doi/abs/10.1596/978-1-4648-1671-0_ch5)

Crossing borders- Source: The World Bank

<https://wdr2021.worldbank.org/stories/crossing-borders/>

the European Union (EU) with its General Data Protection Regulation (GDPR). Many countries outside the EU, including some lower-income countries, have also adopted this model, such as Argentina, Colombia, Korea, Malaysia, Senegal, and South Africa.

The third type of data model follows a limited transfers approach, which imposes strict requirements on the cross-border flow of personal data for companies and organizations. This often includes obtaining prior authorization from the government after a security assessment, and a condition that personal data must be stored and sometimes processed within the country of origin. Eleven countries follow this model, such as China, which imposes strict conditions and requirements on the transfer of personal and important data for operators of "critical information infrastructure" in various sectors. Foreign companies may need permission before transferring personal data out of the country. Similarly, Russia mandates that personal data about Russian citizens must be stored and processed in databases physically located in Russia, while allowing for cross-border transfers of data copies once this requirement is met. Vietnam requires both domestic and foreign companies providing telecommunications, internet, and value-added services to store related personal data within the country.

To summarize, the open transfers model aims to reduce regulatory barriers for service providers in sharing data across borders. This provides companies with more freedom to conduct business but may not establish sufficient safeguards to ensure the trustworthiness of data transfers. The limited transfers model prioritizes security concerns, which results in stricter limitations on data transfers. The conditional transfers model provides a compromise between the two by permitting international transfers but requiring additional guarantees for personal data protection in the destination market. As a result, this model increases the cost of digital service trading somewhat.

FIGURE 5<sup>44</sup>: Regulations on personal data: Differing transfer models for different countries

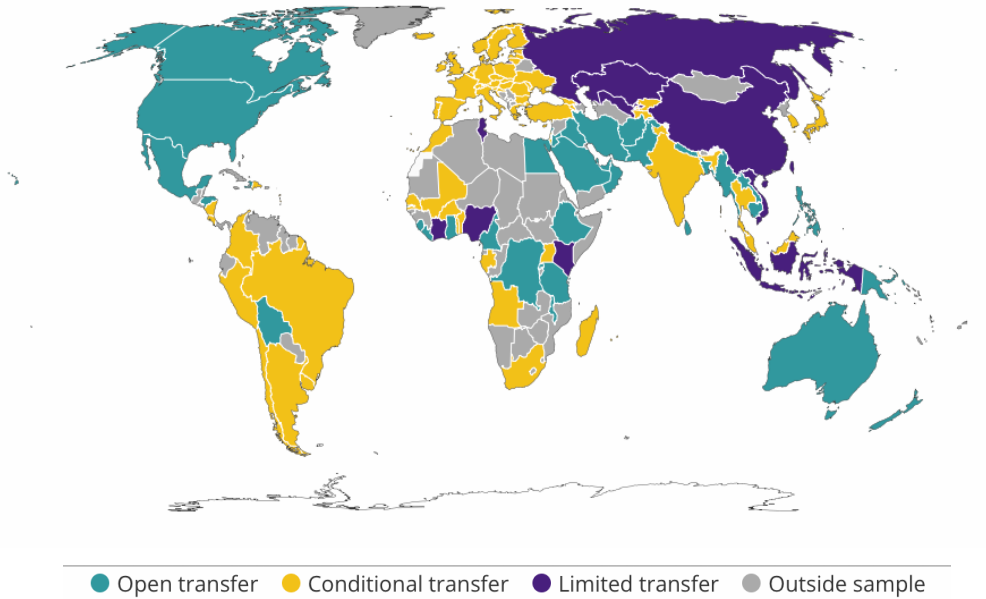
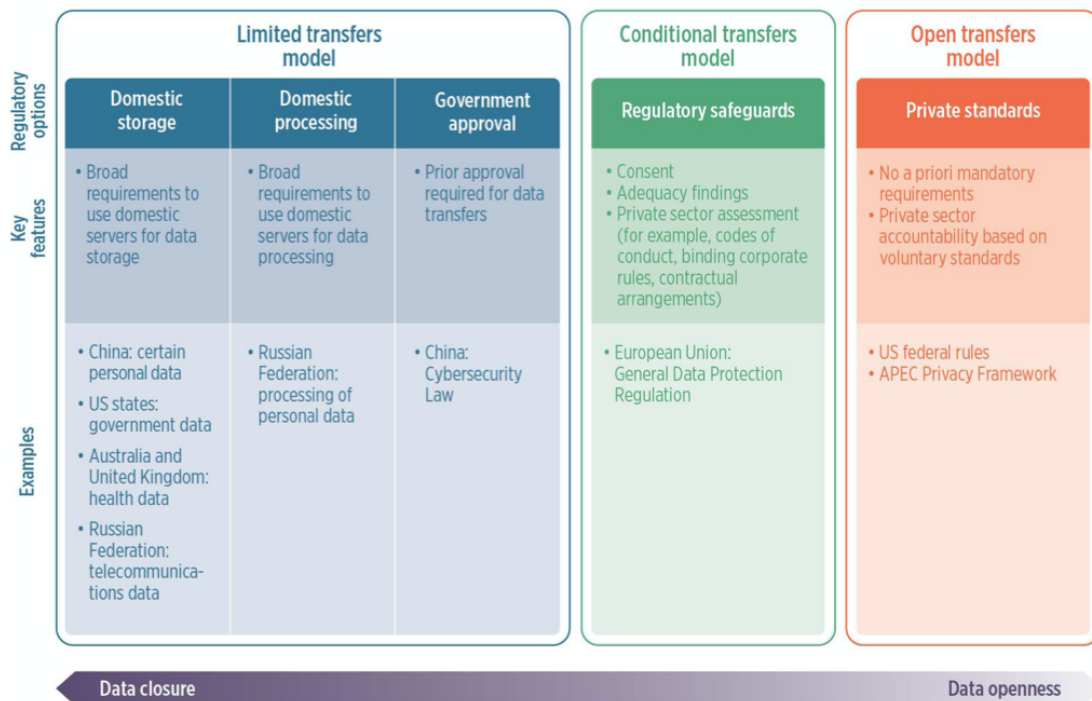


FIGURE 6<sup>45</sup>: Regulatory approaches to cross-border personal data flow, Source: Worldbank.



<sup>44</sup> Cross Border Data and Digital Trade: Impact and policy approaches for better lives – Source: World Development Report 2021, The World Bank.

<https://thedocs.worldbank.org/en/doc/1eca7ab3a21d58fb30d9478365a83c64-0050012022/original/WDR-Chapter-7-Data-and-Digital-Trade-Presentation.pdf>

<sup>45</sup> Ferracane, Martina Francesa, and Erik van der Marel. "Regulations on Personal Data: Differing Data Realms and Digital Services Trade." *Background paper for World Development Report (2021)*.

[https://elibrary.worldbank.org/doi/abs/10.1596/978-1-4648-1671-0\\_ch5](https://elibrary.worldbank.org/doi/abs/10.1596/978-1-4648-1671-0_ch5)

CHART 7: Policy bases for regulating cross-border personal data, WDR 2021 team.<sup>46</sup>

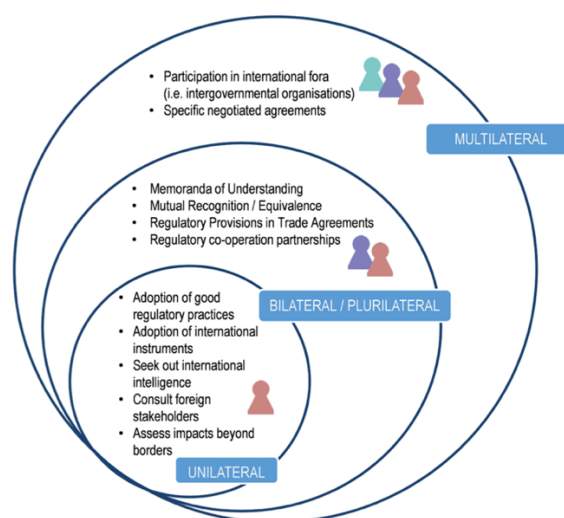
Model	Policy goal	Regulatory costs	Digital trade flows
Limited transfers	Cybersecurity and other security concerns	Higher	Limited by transfer approval or data localization requirements
Conditional transfers	Protection of personal data	Medium	Subject to regulatory conditions
Open transfers	Business freedom	Lower	Largely open

## THE ROLE OF TRUST<sup>47</sup>

The degree of trust in the digital environment is a crucial factor that determines the benefits of digitalization for economic and social interactions. As the sharing, transfer, and use of data increasingly impact individuals and societies, trust becomes even more important. Without trust, businesses may face obstacles in taking advantage of the benefits of scale on a global level. The concept of trust also affects how governments and individuals interact with each other, promoting regulatory cooperation.

Trusted data flows can be facilitated by various government policies, which may include regulatory measures like unilateral mechanisms, intergovernmental agreements, and trade and digital economy deals. Alongside these formal approaches, a variety of informal initiatives that promote dialogue between different stakeholders and emphasize the use of technological and organizational tools can also help foster trust.

FIGURE 7: The multiplicity of international regulatory cooperation approaches, OECD (2022), "Fostering cross-border data flows with trust", OECD Digital Economy Papers, No. 343



<sup>46</sup> World Bank. *World development report 2020: Data for better lives*. The World Bank, 2021.

<https://wdr2021.worldbank.org/the-report/>

<sup>47</sup> OECD (2022), "Fostering cross-border data flows with trust", *OECD Digital Economy Papers*, No. 343, OECD Publishing, Paris, <https://doi.org/10.1787/139b32ad-en>.

Policymakers are faced with the challenge of promoting the free flow of data while maintaining trust; however, the various approaches taken by different regulators have resulted in a fragmented regulatory landscape, making it challenging for individuals, businesses, and governments to operate in a "trusted" environment. Despite this, there are several shared characteristics, synergies, and areas of agreement that policymakers can utilize as a foundation to establish trust and encourage future collaboration.

These include emerging commonalities in regulatory and policy instruments, growing convergence in privacy and personal data protection frameworks, and complementarity between instruments.

## UNILATERAL APPROACHES

“Unilateral mechanisms enable the transfer of certain types of data to countries across borders under certain conditions”.<sup>48</sup>

The development of domestic mechanisms is mostly centered around the transfer of personal data and comprises the use of two types of safeguards: "open safeguards" and "pre-authorized safeguards". Open safeguards involve accountability principles that are applied after the transfer of data, contractual agreements, and private sector adequacy. Conversely, pre-authorized safeguards require approval from the public sector before the transfer of data, and include measures such as public adequacy decisions, standard or pre-approved contractual clauses, and binding corporate rules. Open safeguards give entities more flexibility in how they protect the data being transferred and hold them accountable for any mishandling, while pre-authorized safeguards involve public sector approval beforehand.

The primary distinction between open safeguards and pre-authorized safeguards pertains to who is responsible for designing and evaluating compliance. Under open safeguards, the entity transferring the data assesses adequacy based on objectives established by the government while with pre-authorized safeguards, adequacy determinations are made by the government. In the first case, the entity determines the provisions to be included in contracts or corporate rules, while the government creates model contracts that must be utilized by firms or approve corporate rules after review.

There is an increasing number of countries creating model contractual clauses, which offer protection when data is transferred overseas. These clauses have different variations depending on the type of transfer involved, such as to data controllers or intermediaries/processors. Public authorities develop these ready-made clauses to be integrated into contracts, and they are generally considered to provide

---

<sup>48</sup> OECD (2022), "Fostering cross-border data flows with trust", *OECD Digital Economy Papers*, No. 343, OECD Publishing, Paris, <https://doi.org/10.1787/139b32ad-en>.

adequate safeguards for data transfers, even to countries that do not have equivalence or adequacy recognition.

To enable international data transfers, most countries utilize adequacy, standard contractual clauses, or binding corporate rules that assess data protection for personal data before allowing data flows.

Some countries employ government approval for data transfer plans as a unilateral mechanism to facilitate data-free flow with trust. Indonesia uses this approach for geospatial data, health data, and personal data protection, while Turkey's banking law and regulation on private archival material also allow them to prohibit international data flows.

Moreover, several laws and regulations require the data subject's consent as a condition for international data flows, particularly in the context of personal data.

Data localization requirements represent another approach that limits or conditions data to flow freely. For instance, personal data generated in the Russian Federation and by its inhabitants must be stored locally before it can be transferred abroad, and Brazil mandates a recent data backup to be maintained within its territory in the context of cloud computing.<sup>49</sup>

## BILATERAL AND PLURILATERAL APPROACHES

Bilateral approaches involve agreements and cooperation between two countries, where they work together to ensure that personal data is transferred in a secure and compliant manner. They can take various forms, such as the negotiation of mutual recognition agreements (MRAs) or the establishment of joint supervisory authorities.

The laws submitted by Canada, Mexico, Singapore, and the United States pertain to contracts and memoranda of understanding that facilitate international data flows, particularly personal data and data related to commodities trading. These laws also place the responsibility on local data controllers to ensure that foreign data processors comply with relevant safeguards.

Creating a regulatory environment that promotes data flows and instills trust also involves regulatory cooperation on data protection, which can be achieved through various means, such as agreements between governments and dialogues between regulators on enforcement issues.

Plurilateral arrangements refer to agreements or arrangements that involve multiple countries working together to establish common rules and standards for the protection of personal data. They may focus on a specific sector or issue, such as e-commerce or intellectual property rights. Plurilateral approaches prioritize the participation of like-minded countries and seek to create targeted, sector-specific agreements.

---

<sup>49</sup> G20 Members' Regulations of Cross-Border Data Flows (UNCTAD)

22 Mar 2023 [https://unctad.org/system/files/official-document/dtlecdc2023d1\\_en.pdf](https://unctad.org/system/files/official-document/dtlecdc2023d1_en.pdf)



In terms of cross-border data flows, a plurilateral approach may be more flexible and able to respond quickly to changes in technology and the global economy.

They can take various forms, such as free trade agreements, regional agreements, or sector-specific agreements. These arrangements can help to promote data flows by establishing clear and consistent rules for the transfer of personal data, as well as mechanisms for ensuring compliance with those rules.

## MULTILATERAL APPROACHES

Multilateral approaches to cross-border data flows refer to the collective effort of multiple countries to establish a framework or agreement that regulates the movement of digital information across international borders in response to the rapid growth of digital technologies and the internet, which has resulted in an exponential increase in the volume of data that is transmitted across borders daily. Multilateral approaches aim to address data flow concerns by promoting cooperation between nations and setting out common rules and standards: numerous strategies exist for establishing multilateral agreements concerning privacy and data protection, which vary in their level of enforceability.

One such strategy involves non-binding plurilateral arrangements that depend on "soft law" to motivate parties to embrace data protection principles and facilitate the interoperability of privacy protection systems to enable the cross-border transfer of data. An example is the 1980 "OECD Privacy Guidelines"<sup>50</sup>, which provides a comprehensive framework for privacy protection that is applicable across multiple sectors and industries. The guidelines have been widely recognized and adopted by many countries around the world. However, it is important to note that they are not legally binding and do not have the force of law. Instead, they provide a set of principles and best practices that countries can use to develop their own privacy laws and regulations.

Binding multilateral approaches involve stronger enforcement mechanisms.

One example is the General Data Protection Regulation (GDPR) introduced by the European Union (EU) in 2018. The GDPR sets out a comprehensive set of rules and standards for the handling of personal data, including cross-border transfers of data. It requires companies to obtain explicit consent from users before transferring their data to countries outside of the EU, unless there is an adequate level of data protection in the recipient country.

Another example is the Asia-Pacific Economic Cooperation (APEC) Privacy Framework, which provides a set of principles and guidelines for the protection of personal information in the Asia-

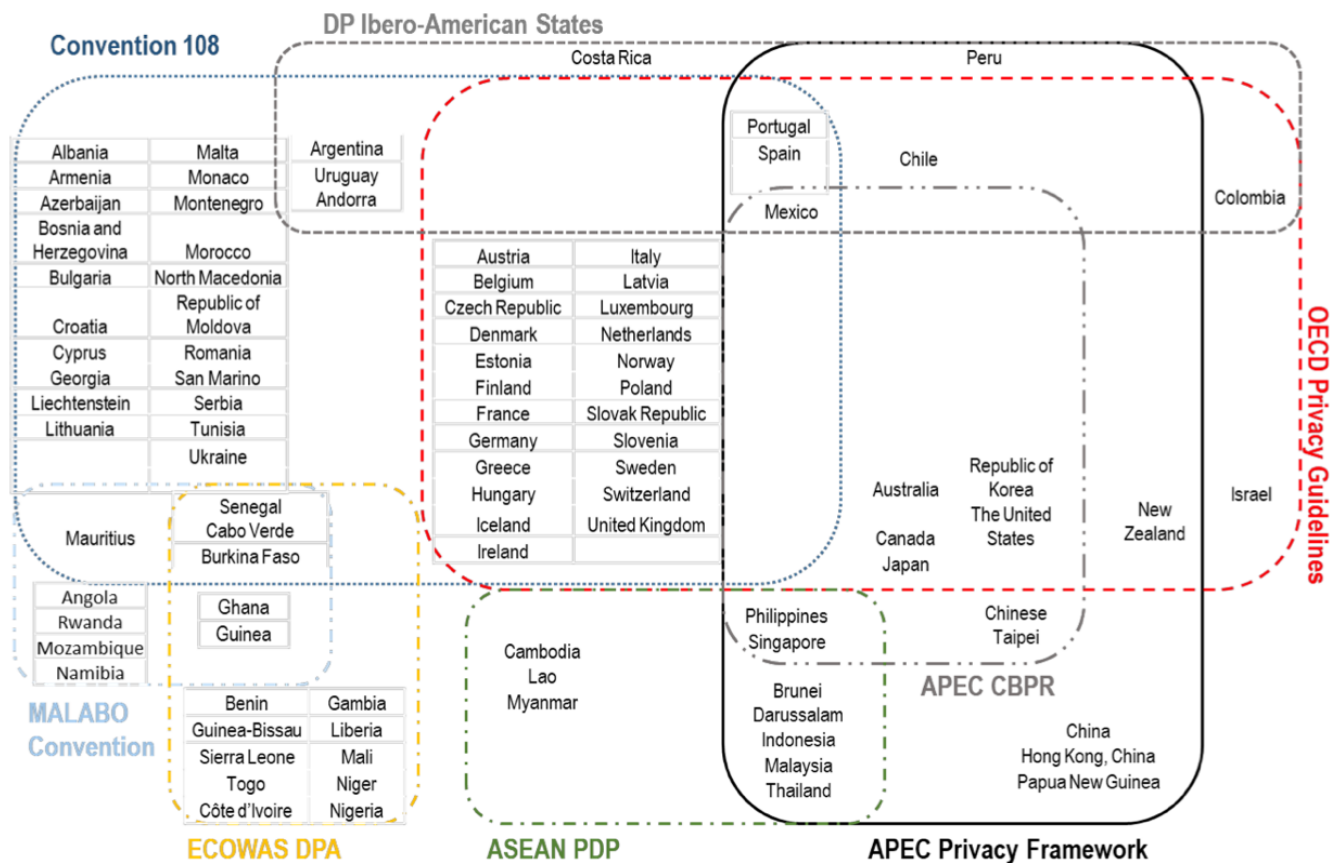
---

<sup>50</sup> Casalini, F., J. López González and T. Nemoto (2021), "Mapping commonalities in regulatory approaches to cross-border data transfers", *OECD Trade Policy Papers*, No. 248, OECD Publishing, Paris, <https://doi.org/10.1787/ca9f974e-en>.



Pacific region. The Cross-Border Privacy Rules (CBPR) system, which is a voluntary, multilateral framework promotes the free flow of information while also protecting the privacy of individuals. In addition to these frameworks, there are ongoing efforts to establish international agreements on data flow, such as the World Trade Organization's (WTO) discussions on e-commerce and digital trade. These negotiations aim to establish a global framework for cross-border data flows that balances the benefits of data flows with privacy and security concerns.

CHART 8: The overlapping memberships of multilateral arrangements <sup>51</sup>



## CONCLUSIONS

In this chapter the analysis is focused on the goals and costs of the different regulatory approaches to cross-border data flows based on the three main transfers models. The trust between entities involved in the flows is essential; so, to guarantee it, countries have stipulated many international cooperation approaches that involve two or more countries.

<sup>51</sup> Casalini, F., J. López González and T. Nemoto (2021), "Mapping commonalities in regulatory approaches to cross-border data transfers", *OECD Trade Policy Papers*, No. 248, OECD Publishing, Paris, <https://doi.org/10.1787/ca9f974e-en>.

In next chapter EU, US and China policies are analyzed to better understand the different strategies adopted by the main world's economies.

## CHAPTER 5

### EU, US, AND CHINA POLICIES

As mentioned before, many countries have developed their own legal frameworks to govern cross-border data flows, often based on international agreements and treaties.

The protection of personal electronic data across borders is a concern for governments and has implications for the transmission of information. Different countries have varying approaches to protecting privacy and exporting consumer data.

International economic bodies are addressing privacy laws and their impact on international trade, with the APEC Privacy Framework seeking to balance protecting private information with the cross-border transfer of information. Government access to personal data for criminal investigations or national security reasons is regulated differently across countries.

Next, the policy choices made by Europe, the United States, and China will be compared to understand what are the implications arising from these policies.

#### THE POLICY TRILEMMA<sup>52</sup>

With the rise of big data, personal data has taken on immense commercial value. As a result, the demand for cross-border transfer has increased, prompting lawmakers to prioritize its consideration when creating relevant regulations. However, in crafting specific policies, policymakers face a regulatory trilemma. This term, which originates from international finance, suggests that the free movement of capital, a fixed exchange rate, and an independent monetary policy are mutually exclusive - a country can only have two out of the three.

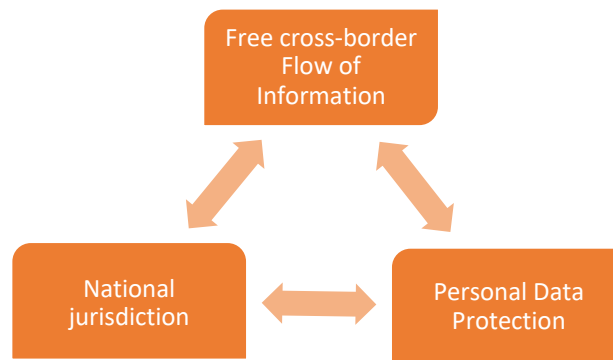
In the field of cross-border transfer of personal data, a similar trilemma exists, comprising personal data protection, free flow of information across borders, and the expansion of national jurisdiction.

The development of personal data protection standards has progressed incrementally. Initially, in the 1980s, the OECD Privacy Guidelines and Council of Europe Convention 108 were established as the first generation of international standards for safeguarding personal data. The second generation was introduced with the Data Protection Directive (DPD) in 1995. In 2016, the General Data Protection Regulation (GDPR) was introduced in the EU and has the potential to serve as the global gold standard for data protection.

---

<sup>52</sup> Zheng, Guan. "Trilemma and Tripartition: The Regulatory Paradigms of Cross-Border Personal Data Transfer in the EU, the U.S. and China." *Computer law and security report*. 43 (2021): n. pag. Web.

CHART 9: *Trilemma of cross-border transfer of personal data.* Source: *personal processing based on Zheng, Guan. “Trilemma and Tripartition: The Regulatory Paradigms of Cross-Border Personal Data Transfer in the EU, the U.S. and China.”*



A comparison of the regulatory frameworks of the EU, the US, and China highlights their differing regulatory paradigms. These differing approaches to regulating cross-border data transfer have caused conflicts and legal barriers. Despite this, the three largest economies make compromises through bilateral or multilateral agreements, allowing for the regional free transfer of personal data. Each faces unique commercial and technological circumstances, which influence their distinct policy approaches to cross-border data transfer. As a result, there are divergent legislative attitudes toward the three components of the policy trilemma.<sup>53</sup>

#### EU POLICY - A model of global federalism

The European Data Protection Directive (DPD) was passed by the EU in 1995, setting out the minimum standards for data privacy and security. Each member state then created its own implementing law based on this directive.<sup>54</sup>

The EU prioritizes personal data protection and the free flow of information across borders as its main values and goals in legislation, as stated in the full title of the DPD. To achieve a unified market, the EU must maintain a high standard of data protection for natural persons while promoting the free movement of goods, services, capital, and people. The DPD emphasizes the importance of equivalent data protection standards for cross-border transfers, requiring third countries to ensure adequate levels of protection comparable to those of the EU. The GDPR, which replaced the DPD, has been directly applicable to EU member states since May 25, 2018, and further strengthens this approach.

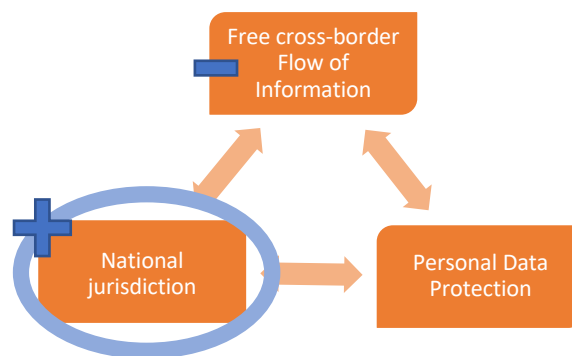
<sup>53</sup> Zheng, G. (2021). Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the US and China. *Computer Law & Security Review*, 43, 105610.

<sup>54</sup> “What is GDPR, the EU’s new data protection law?”- GDPR.EU

This new standard prioritizes individual informational self-determination and the right to prevent illegal breaches. It also limits or prohibits government and enterprise misuse of personal data and provides effective judicial remedies for data subjects. These guidelines have influenced national legislation on personal data protection worldwide.

In case of a significant data breach, the GDPR mandates that the company must inform all impacted individuals and the supervisory authority within 72 hours. These requirements extend to all data originating from EU citizens, regardless of whether the collecting company operates within the EU, and to all individuals whose data is stored within the EU, regardless of their citizenship. The GDPR further outlines the consequences of failure to comply with its regulations.

The EU's focus on maintaining a uniformly high standard of data protection means that member states and third countries face restrictions on their jurisdiction, this is known as a global federalism model.



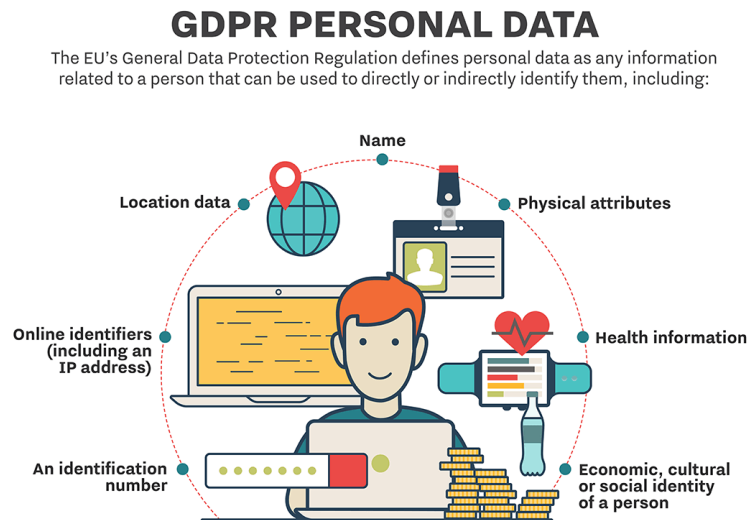
The objective of GDPR is to safeguard individuals and their associated data, while ensuring that the organizations collecting this data do so responsibly. The regulation also requires that personal data is securely maintained, and protected against unauthorized or illegal processing, accidental loss, destruction, or damage.

The GDPR outlines specific reasons for gathering personal data, which must be lawful and for legitimate purposes.

The EU has adopted a combination of constitutional and statutory laws which highlights the importance of protecting the fundamental right to privacy.

Article 7 of the Charter of fundamental rights of the European Union states that: “Everyone has the right to respect for his or her private and family life, home and communications”, while Article 8(1) guarantees a constitutional right to protect personal data.

FIGURE 8: GDPR Personal Data. - Source: General Data Protection Regulation (GDPR), TechTarget.com



However, these rights are not absolute, and any limitations on them must be provided for by law, respecting the essence of these rights as expressed in Article 52(1) of the Charter.<sup>55</sup>

Individual consent is the core provision of the regulation, under which the processing of data by governments and businesses should fall. The EU requires the consent of the data subject to be "freely given, specific, informed and unambiguous," (Art.4 GDPR) and provided for "one or more specific purposes" (Art. 6 GDPR). The data controller is responsible for demonstrating compliance with legal requirements on data subjects' consent. The GDPR also provides effective remedies for data subjects, even if the misuse of personal data by the processor has not caused material damage. Data subjects can complain to a supervisory authority or take legal action, where the processor is liable for damages caused by its improper processing.

The EU also believes in the free flow of information, which is necessary for international trade. However, this may lead to a risk of inadequate data protection in the receiving country, in this scenario the EU prioritizes personal data protection over commercial interests and requires the same high standards of data protection for the free flow of information. The differences in personal data protection among member states, lead to the consideration of a cross-border transfer system. The EU divided cross-border transfers into internal and external flows and prohibits limitations on internal

---

<sup>55</sup> Article 52: Scope of guaranteed rights. (1): Any limitation on the exercise of the rights and freedoms recognized by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others.

transfers while ensuring uniform personal data protection standards. For external transfers, the third country is required to ensure an adequate level of protection equivalent to that in the Union.<sup>56</sup>

The GDPR applies not only to companies established in the EU but also to those that offer goods or services to EU data subjects or monitor their behavior.

The extraterritorial application of the GDPR has been controversial, especially regarding the adequacy test. This test evaluates whether a third country offers an adequate level of data protection, and the EU can unilaterally evaluate the standards of protection in partner countries. If a third country is deemed adequate, personal data can flow from the EU to that country without further safeguards. The European Commission has recognized several countries as adequate, but the adequacy test has become more stringent over time.

If a third country is not deemed adequate, a controller or processor can still transfer personal data to that country if appropriate safeguards are in place. These safeguards include legally binding and enforceable instruments, binding corporate rules, standard data protection clauses, approved codes of conduct, or approved certifications.

The EU's approach may become a global standard for data privacy protection. In order to maintain consistency, the EU limits the jurisdiction of member states and requires third countries to refer to EU regulations for data protection standards. The GDPR directly limits national jurisdiction, and the European Commission is now solely responsible for assessing the adequacy of privacy protection in third countries. The CJEU has emphasized the importance of protecting data subjects' rights and ensuring certainty and proportionality when it comes to interference by foreign authorities.

#### US POLICY- A model of golden straitjacket

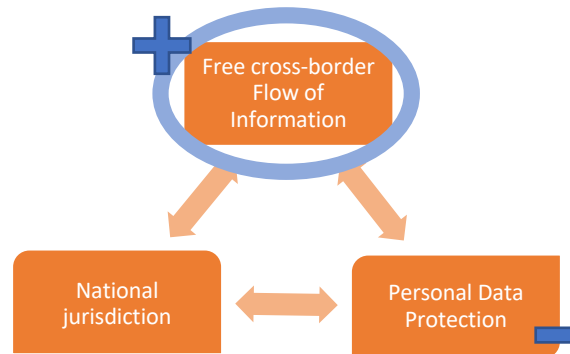
Unlike the EU, the US places more importance on the free movement of information across borders than on protecting information privacy. This is because the US views personal data as a valuable commodity, and therefore prioritizes free information flow. Commercial interests is prioritized over privacy in its digital trade policy, adhering to the notion of free trade. This ideology has been in place since the Clinton administration<sup>57</sup>, advocating for the maximum possible free flow of cross-border

---

<sup>56</sup> Chin, Y.-C.; Zhao, J. Governing Cross-Border Data Flows: International Trade Agreements and Their Limits. *Laws* 2022, *11*, 63. <https://doi.org/10.3390/laws11040063>

<sup>57</sup> In July 1997, the Clinton Administration released "A Framework for Global Electronic Commerce". The report proposed five general policy principles aimed to address the administration's views on Internet commerce: the private sector should lead; governments should avoid undue restrictions on electronic commerce; where government involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce; governments should recognize the unique qualities of the Internet; electronic Commerce

information and ensuring that regulatory differences between countries don't become trade barriers. The US promotes the free flow of cross-border data through bilateral and regional free trade agreements, with market access being the core norm of these agreements. Although this approach has led to the growth of the technology industry and protects free speech, it also means that personal data privacy is limited. The US government has been able to access the personal data of individuals in other countries through multinational corporations, which expands its jurisdiction over data privacy.<sup>58</sup> This approach can be seen as a model of the Golden Straitjacket.



At the constitutional level, the Fourth Amendment and Fourteenth Amendment are two provisions relevant to information privacy protection, but the Fourth Amendment only applies to searches and seizures and is not well-suited to governmental use of big data technology. This Amendment, for instance, aims to protect citizens from government surveillance, rather than private actors<sup>59</sup>. The Due Process Clause of the Fourteenth Amendment's recognition of the right to information privacy

---

over the Internet should be facilitated on a global basis. - Malawer, Stuart S. "Internet Commerce and Trade Policy." *International Initiatives for E-Trade* (2007).

<sup>58</sup> Chin, Y.-C.; Zhao, J. Governing Cross-Border Data Flows: International Trade Agreements and Their Limits. *Laws* 2022, *11*, 63. <https://doi.org/10.3390/laws11040063>

<sup>59</sup> Amendment IV: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

The goal of the Fourth Amendment is to protect people's right to privacy from unreasonable intrusions by the government.



remains controversial and uncertain<sup>60</sup>. In contrast, the First Amendment's free speech clause<sup>61</sup> and Article III's standing requirement<sup>62</sup> provide significant safeguards for the free flow of data, allowing for convenient data processing for commercial purposes but requiring privacy consumers to suffer concrete and particularized injuries to merit legal remedy.

The regulation of data protection is complex and fragmented, with federal and state laws governing different sectors and types of information. Privacy protection at the contractual level is provided by the contract between data processors and private consumers and the supervision of the Federal Trade Commission (FTC) that disciplines companies through the FCT Act which has undergone hundreds of enforcements in the last two decades. "The FTC's past work, however, suggests that enforcement of the FTC Act alone may not be enough to protect consumers. The FTC's ability to deter unlawful conduct is limited because the agency generally lacks the authority to seek financial penalties for initial violations of the FTC Act. By contrast, rules that establish clear privacy and data security requirements across the board and provide the Commission the authority to seek financial penalties for first-time violations could incentivize all companies to invest more consistently in compliant practices"<sup>63</sup>. Additionally, personal data are not restricted from being transferred by private entities, and there is a clear tendency towards market-based governance. Even recent state-level efforts to strengthen consumer privacy rights, such as those in California, differ significantly from the EU model of fundamental rights protection.

The US Constitution does not regulate the collection and use of personal data by companies, and there is no constitutional mandate for citizens' right to privacy, resulting in privacy being discussed more academically than legally. While the Federal Supreme Court has confirmed the right to constitutional protection of personal data, courts have generally avoided making decisions regarding this right. At the statutory level, there is no comprehensive law on privacy protection, with protection taking the form of a patchwork of statutes and regulations for various industries.

---

<sup>60</sup> The Fourteenth Amendment's Due Process Clause provides that no state may "deprive any person of life, liberty, or property, without due process of law".

<sup>61</sup> First Amendment: Congress shall make no law respecting an establishment of religion or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

<sup>62</sup> In order to be considered a party with standing, it is necessary to demonstrate that one's own legal interests have been impacted by an "injury in fact". This means that the party must have actually suffered some form of harm, typically in relation to their protected legal rights and freedoms. If a party is unable to establish such harm, they lack standing and are not qualified to appear before a court. The mere possibility of an injury or being a concerned citizen is insufficient for establishing standing.

<sup>63</sup> Federal Trade Commission. "FTC Explores Rules Crackdown on Commerical Surveillance and Lax Data Security Practices." (2022).

The United States considers personal data as a market commodity at the statutory level, which means that enterprises processing personal data should only be restricted or prohibited by law. As a result, relevant protective provisions are found in industry regulations, technical norms, or specific types of information. This leads to legal loopholes, as various ways to process personal data are not explicitly prohibited by sectoral laws. At the contractual level, the consumer protection system fails to provide adequate remedies for these loopholes. The "notice and choice" approach taken by companies and consumers in privacy agreements is insufficient to support rational decision-making, and consumers are often left with no alternatives. The Federal Trade Commission (FTC) is the most influential regulatory authority on information privacy in the US, but its authority does not extend to public operators or financial institutions, and it lacks legislative authority and sufficient resources to comprehensively protect consumer privacy.

The U.S. aims to foster the growth of the internet technology industry by loosening privacy protections and lifting strict limitations on cross-border personal data transfer. The country generally adheres to domestic privacy protection regulations and imposes minimal restrictions on transborder data flows, with only a few limitations on public procurement contracts. The federal government requires data storage localization in the United States territories, embassies, or military installations for federal tax information, as stated in the IRS's Tax Information Security Guidelines for Federal, State, and Local Agencies. Additionally, the U.S. Department of Defense mandates data localization for all cloud service providers in 2015. Certain states, like Tennessee, limit personal data transfer offshore through government vendor business outsourcing by preferring local vendors for state procurement contracts that require data entry.

The United States, as the birthplace of the internet, has a dominant position in information technology, and its internet companies have expanded globally. However, this expansion puts the personal information of individuals in other countries at risk of potential abuse by the U.S. government. The U.S. uses its technological power and commercial activities to proactively expand its jurisdiction. The Clarifying Lawful Overseas Use of Data Act, known as the CLOUD Act, which regulates the information transmission obligations of U.S. companies, exemplifies this policy. It was enacted in 2018 as a legislative response to Microsoft's claim against the U.S. government<sup>64</sup> and extends the

---

<sup>64</sup> Microsoft has run a free web-based email service for the general public since 1997 (Outlook.com). The majority of the data related to this service is kept in datacenters run by Microsoft and its affiliates, which are dispersed globally. At the heart of the debate is the question of whether, under 18 U.S.C. § 2703, a mandated e-mail provider is obligated to provide the federal government with access to e-mail even if it is stored only abroad. While this case was pending, the President signed into law the CLOUD Act, which amended the Stored Communications Act, to require email providers to disclose emails in its "possession, custody, or control," even if they are stored outside of the United States.

jurisdiction of the Stored Communications Act (SCA) to information located both inside and outside the United States. The CLOUD Act aims to assist the U.S. government in accessing personal data stored abroad, which reflects its aggressive and expansive approach to jurisdiction. The U.S. government's enactment of the CLOUD Act suggests an attempt to achieve global expansion of its jurisdiction in the area of personal data due to the leading position of U.S. technology companies in the global industry and their strong commercial capabilities.

This is in contrast to the General Data Protection Regulation which aims to safeguard and reinforce individuals' integrity and empower them with control over their data. According to Article 6 of the GDPR, a legal basis is required for any data transfers<sup>65</sup>. Article 48 of the GDPR mandates that court orders for data transfer outside the EU are only valid if grounded in an international agreement<sup>66</sup>, such as a Mutual Legal Assistance Treaty (MLAT). Other legal bases are not acceptable for such requests under EU law. In certain established circumstances, the protection of a data subject or another person's vital interest may suffice as a legal basis. However, Recital 46 of the GDPR clarifies that this can only be used if another legal basis is not applicable.

Additionally, the GDPR authorizes data transfers when the controller's legitimate interests outweigh the data subject's interests or fundamental rights and freedoms. The European Data Protection Board, however, holds that the data subject's interests or fundamental rights and freedoms would take precedence over the controller's interests, such as avoiding repercussions from the US for a potential breach of the request. From a GDPR perspective, this once more shows a weak legal foundation.

Consequently, the GDPR and the CLOUD Act conflict significantly concerning the GDPR's stringent requirements for a legal basis for data processing. This means that from a GDPR compliance perspective, warrants issued based on the CLOUD Act are only acceptable if based on the EU-US MLAT.<sup>67</sup>

---

Source: "The CLOUD Act: Mooting the Microsoft Ireland Case, but Not Forecasting Clear Skies Just Yet", Columbia Business Law Review, Aug 13, 2019.

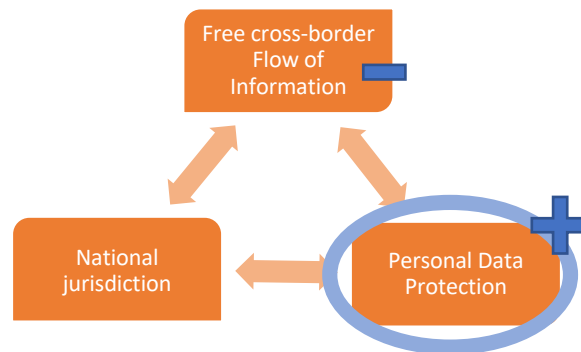
<sup>65</sup> Art. 6 GDPR, Lawfulness of processing. (3): "The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by: Union law; or Member State law to which the controller is subject."

<sup>66</sup> Art. 48 GDPR, Transfers or disclosures not authorised by Union law: "Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter."

<sup>67</sup> "U.S. CLOUD Act vs. GDPR", Klaus Foitzick, 29 February 2020.

## CHINA POLICY A model of Bretton Woods compromise

The Chinese government has made personal data protection a crucial principle with the introduction in August 2021 of the Personal Information Protection Law (PIPL) which aims to prevent companies from misusing consumers' personal information. The regulation also strengthens the authority over personal data usage within the country and sets additional requirements for cross-border data transfer. China has prioritized personal data protection and national jurisdiction, thus presenting a regulatory model similar to the Bretton Woods Compromise.



China's legal protection of personal information was previously fragmented and scattered across public and private laws, with each concerning only personal data protection for a particular industry sector. This led to a variety of regulatory authorities, which failed to provide comprehensive and effective protection for data subjects. To address this, China passed the PIPL which provides a general and integrated approach to regulate the access and use of personal data. The law defines personal information and its processing, provides seven legal grounds for personal information processing, emphasizes the importance of informed consent, and requires processors to comply with legal requirements.

The PIPL places a heavy emphasis on processing personal information: the PIPL, like the GDPR, applies to the processing of personal information that occurs outside of China if it serves one of the following purposes: providing products or services to individuals in China, analyzing or evaluating the behavior of individuals in China, or any other purposes specified by relevant laws and regulations (Article 3).

Furthermore, under the PIPL, "personal information processing entities" outside of China that are subject to the regulation must establish a "dedicated office" or appoint a "designated representative" in China to oversee the protection of personal information (as stated in Article 53). This provision closely resembles the GDPR's requirement for offshore controllers to appoint an "EU representative". Moreover, similar to the GDPR, the PIPL mandates that businesses have a legitimate reason for processing personal data. However, unlike the GDPR, the PIPL does not include "legitimate interests"

as a legal justification for processing. Rather, in addition to approval, Article 13 provides seven kinds of legal grounds for personal information processing<sup>68</sup>. Consent must be expressed on the premise of being fully informed, and personal information must be processed lawfully and properly for a clear and legitimate purpose.

Article 4 of the PIPL defines personal information and its processing: “Personal information refers to various kinds of information related to identified or identifiable natural persons recorded by electronic or other means, excluding the information processed anonymously. Processing of personal information includes the collection, storage, use, processing, transmission, provision, publication, and erasure of personal information”.

Unlike in the case of a GDPR violation<sup>69</sup>, if an entity processing personal information violates PIPL requirements, regulators can take several corrective measures such as issuing warnings, confiscating illegal income, suspending services, or imposing fines. The fine can go up to either 50 million RMB or 5% of the organization's annual revenue for the previous fiscal year (as per Article 66), but it is unclear if the revenue is only limited to China or includes global turnover. Moreover, regulators have a lot of leeway when it comes to imposing penalties, as the PIPL does not stipulate a minimum

---

<sup>68</sup> PIPL Article 13:

Only under any of the following circumstances may a personal information processor process personal information:

- (I) where the consent of the individual concerned is obtained;
- (II) where it is necessary for the conclusion or performance of a contract to which the individual concerned is a party, or to implement human resources management in accordance with labor rules and regulations formulated according to law and collective contracts concluded according to law;
- (III) where it is necessary for the performance of statutory duties or statutory obligations;
- (IV) where it is necessary for coping with public health emergencies or for the protection of the life, health, and property safety of a natural person;
- (V) where such acts as news reporting and supervision by public opinions are carried out for the public interest, and the processing of personal information is within a reasonable scope;
- (VI) where the personal information disclosed by individuals themselves or other legally disclosed personal information is processed within a reasonable scope in accordance with the provisions of this Law; and
- (VII) other circumstances provided by laws and administrative regulations.

Individual consent shall be obtained for the processing of personal information stipulated in the other clauses of this Law, but in the circumstances specified in the preceding paragraph from (II) to (VII), the individual's consent is not required.

<sup>69</sup> “For especially severe violations, listed in Art. 83(5) GDPR, the fine framework can be up to 20 million euros, or in the case of an undertaking, up to 4 % of their total global turnover of the preceding fiscal year, whichever is higher. But even the catalogue of less severe violations in Art. 83(4) GDPR sets forth fines of up to 10 million euros, or, in the case of an undertaking, up to 2% of its entire global turnover of the preceding fiscal year, whichever is higher.” – GDPR, Fines/Penalties.

punishment. In addition to monetary fines, the processing entity's violations may be noted in their "credit files" under China's national social credit system (as per Article 67). Furthermore, if processing entities infringe on personal information rights and interests, they will be held responsible for tort damages (as per Art. 69). If these entities harm the rights and interests of a considerable number of individuals, the People's Procuratorate and other designated organizations may file public interest lawsuits (as per Article 70).

The PIPL applies to a broad range of sectors and aims to provide comprehensive and effective protection for data subjects as it includes legal norms that strictly limit the cross-border flow of personal data in three ways: the reasons for transfer, security assessment, and legal grounds. Chinese lawmakers have imposed additional statutory conditions and limitations that lead to severe restrictions on the free flow of personal data. A cross-border transfer can only occur when the data processor "truly needs" to transfer data abroad for business reasons, and the transfer must meet specific security requirements. The legal ground for cross-border transfer is limited to the informed consent of the data subject. Furthermore, the informed consent of the data subject and security examination must both be met before a cross-border transfer takes place. These legal requirements are in line with the lawmakers' aim of protecting the rights and interests of the data subject, regulating personal data processing activities, and promoting the lawful use of personal data. However, this has restricted the free flow of personal data while enhancing its protection, partially expanding the national jurisdiction defensively.

The PIPL addresses two issues related to personal data jurisdiction, namely extraterritorial application and defense against foreign government interference. Article 3 of the PIPL specifies the territorial and personal scope of the application, which includes the processing of personal data within China and data subjects falling under the scope of the law. The law applies if the information is processed for certain purposes, such as providing products or services to persons inside China, analyzing or assessing their conduct, or in other circumstances set out by law and regulation. The PIPL expands its jurisdiction through an extraterritorial application, which means that even if data processors and data subjects are outside borders, the PIPL can still apply if the processing activities occur in China. The law also protects not only Chinese citizens but also residents and data subjects with other types of legal status. Additionally, the PIPL adopts defensive measures against expanding jurisdiction by foreign authorities that may infringe on or limit national jurisdiction. If a foreign judicial or law enforcement authority requires personal data stored in China, the information can only be provided with the approval of the competent authority, without violating international treaties or agreements regulating the transfer of personal data that China has concluded or acceded to. The PIPL also adopts the principle of reciprocity in public international law, emphasizing that countries should treat each other identically or equivalently. Therefore, if any foreign country or region adopts any

discriminatory measures against China in terms of personal data protection, China may take reciprocal measures (Art. 43 PIPL).<sup>70</sup>

## CONCLUSIONS

The analysis conducted shows the differences between the policy choices chosen by the US, Europe and China.

While the EU has adopted a model of global federalism, prioritizing robust personal data protection and promoting the free flow of information while limiting domestic jurisdiction, the US prioritizes free cross-border data transfer while weakening personal data protection and expanding its control over personal information based on its technological and commercial power, resulting in a Golden Straitjacket model. China, on the other hand, leans towards protecting personal data and national jurisdiction at the expense of cross-border information transfer, leading to a Bretton Woods Compromise model.

By observing these models through a somewhat accurate cross-comparison, the analysis has shed light on the different issues and opportunities that policies face in the regulation of cross borders data flows. For example, China's stringent policy on data processing and data protection appears to be at odds with the policy of industrial expansion in the field of telecommunications and generally in technologies focused precisely on ICT and digital data processing.

---

<sup>70</sup> PIPL, Article 43: “Where any country or region takes discriminatory prohibitive, restrictive or other similar measures against the People’s Republic of China in respect of the protection of personal information, the People’s Republic of China may, as the case may be, take reciprocal measures against such country or region.”



## CONCLUSIONS

The redefinition of business models and the impact of technological innovation puts digital trade in the face of the need for constant transformation: companies, in a people-driven economy, are obliged to design new ways to reach audiences by increasingly exploiting the possibilities offered by the Web. Today's increasingly liquid and complex markets require Professionals who are dynamic in grasping these changes and devising strategies that respond concretely to a plurality of individuals and groups who are aware of their role in relation to brands. Digital commerce is developing strongly mainly because the customer experience, thanks to the latest technologies, has improved significantly.

For example, content personalization through cookies, small snippets of code that allow Web sites to "remember" users, has revolutionized the online customer experience. Moreover, digital retailers have begun to incorporate augmented and virtual reality as additional touch points during the customer journey. For instance, online clothing retailers might use augmented reality to create digital fitting rooms where customers can try on clothes virtually.

Moreover, large retailers use sophisticated programming to identify product inventories in physical stores nationwide, using store supplies to fulfill online customer orders.

Those who visit sites and buy online provide data to companies and are unknowingly subject to profiling.

Because users have access to sites located in every part of the world, it is necessary that such information, which travels hundreds of miles, is used properly and for lawful purposes. To protect consumers and ensure security in the marketplace, policies have intervened to protect sensitive data and restrict cross-border data flows.

Since issues related to data flows through digital technologies are relatively new, each economy has developed its own laws. These laws, however, often conflict with each other and cause restrictions on the flow of data.

In particular, the comparison of European, U.S., and Chinese policies revealed the peculiar aspects of each of these realities and the goal for each of them to focus on some aspects of the "policy trilemma" to the detriment of others: EU focuses on national jurisdiction, US focuses on the free flow of information and China focuses on personal data protection. It is not possible to say which regulatory choice is better since each of them protects different objectives based also on their own historical, cultural, and political aspects.

To solve problems due to the unevenness in regulation, governments, international organizations, and businesses must work together to develop a regulatory framework that balances the need for data protection with the benefits of cross-border data flows. This requires careful consideration of legal,



ethical, and economic factors, as well as an understanding of the complex interactions between different stakeholders.

Ultimately, if the challenges of cross-border data flows can be successfully addressed, digital trade has the potential to transform the global economy, opening new opportunities for businesses and consumers alike in a more effective way by bringing benefits that the whole society can enjoy.

Through this thesis, characteristics, advantages, and benefits related to digital commerce and data flow have been outlined, and it is intended to strongly encourage a homogenization of data regulatory policies so that the potential benefits that global trade opening brings will materialize.

## BIBLIOGRAPHY

- “Information as a public good”- World Press Freedom Day 2021, United Nations Educational, Scientific and Cultural Organization. [https://en.unesco.org/sites/default/files/wpfd\\_2021\\_concept\\_note\\_en.pdf](https://en.unesco.org/sites/default/files/wpfd_2021_concept_note_en.pdf)
- “The CLOUD Act: Mooting the Microsoft Ireland Case, but Not Forecasting Clear Skies Just Yet”, Columbia Business Law Review, Aug 13, 2019.
- “U.S. CLOUD Act vs. GDPR”, Klaus Foitzick, 29 February 2020.
- “What is GDPR, the EU’s new data protection law?”- GDPR.EU
- Alagheband, Forough Karimi, et al. "An assessment of the use of transaction cost theory in information technology outsourcing." *The Journal of Strategic Information Systems* 20.2 (2011): 125-138.
- Balancing data protection and competition - Source: The World Bank
- Casalini, F., J. López González and T. Nemoto (2021), "Mapping commonalities in regulatory approaches to cross-border data transfers", *OECD Trade Policy Papers*, No. 248, OECD Publishing, Paris, <https://doi.org/10.1787/ca9f974e-en>.
- Chaisse, J. (2023). ‘The Black Pit:’ Power and Pitfalls of Digital FDI and Cross-Border Data Flows. *World Trade Review*, 22(1), 73-89.
- ChatGPT
- Chin, Y.-C.; Zhao, J. Governing Cross-Border Data Flows: International Trade Agreements and Their Limits. *Laws* 2022, 11, 63. <https://doi.org/10.3390/laws11040063>
- Cory, Nigel, and Luke Dascoli. How barriers to cross-border data flows are spreading globally, what they cost, and how to address them. Information Technology and Innovation Foundation, 2021.
- Cross Border Data and Digital Trade: Impact and policy approaches for better lives – Source: World Development Report 2021, The World Bank. <https://thedocs.worldbank.org/en/doc/1eca7ab3a21d58fb30d9478365a83c64-0050012022/original/WDR-Chapter-7-Data-and-Digital-Trade-Presentation.pdf>
- Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?- Source: ITIF By Nigel Cory, May 1, 2017 <https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost/>
- Crossing borders- Source: The World Bank <https://wdr2021.worldbank.org/stories/crossing-borders/>

- Digital Economy Report 2021 - Cross-border data flows and development: For whom the data flow. Source: UNCTAD.
- Digitalization of Services: What does it imply to trade and development? (UNCTAD/DITC/TNCD/2021/2) 25 Mar 2022.
- Esteban Ortiz-Ospina, Diana Beltekian and Max Roser (2018) - "Trade and Globalization". Published online at OurWorldInData.org. Retrieved from: 'https://ourworldindata.org/trade-and-globalization' [Online Resource].
- Federal Trade Commission. "FTC Explores Rules Crackdown on Commercial Surveillance and Lax Data Security Practices." (2022).
- Ferracane, Martina Francesca, and Erik van der Marel. "Regulations on Personal Data: Differing Data Realms and Digital Services Trade." Background paper for World Development Report (2021).
- G20 Members' Regulations of Cross-Border Data Flows (UNCTAD) - 22 Mar 2023 [https://unctad.org/system/files/official-document/dtlecdc2023d1\\_en.pdf](https://unctad.org/system/files/official-document/dtlecdc2023d1_en.pdf)
- Greenleaf, Graham. "G20 makes declaration of 'Data Free Flow With Trust': Support and dissent." (2019).
- Gualtieri, Mike. "Hadoop is data's darling for a reason." Jan-2016.[Online]. Available: <https://go.forrester.com/blogs/hadoop-is-datas-darling-for-a-reason/>. [Accessed: 08-Apr-2018] (2016).
- Holst, A., 2021. Amount of data created, consumed, and stored 2010-2025. Technology & Telecommunications Retrieved, pp.06-29.
- How Canada is growing its data economy – Source: Pavel Abdur-Rahman Partner & Head of Trusted Data & AI, IBM Consulting. May 9, 2022.
- [https://elibrary.worldbank.org/doi/abs/10.1596/978-1-4648-1671-0\\_ch5](https://elibrary.worldbank.org/doi/abs/10.1596/978-1-4648-1671-0_ch5)
- Hussain, Safdar, Xi Song, and Ben Niu. "Consumers' motivational involvement in eWOM for information adoption: The mediating role of organizational motives." *Frontiers in psychology* 10 (2020): 3055.
- Ibrahim, Rosziati. "Formalization of the data flow diagram rules for consistency check." *arXiv preprint arXiv:1011.0278* (2010).
- IDC, & Statista. (June 7, 2021). Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025 (in zettabytes) [Graph]. In Statista. Retrieved April 19, 2023, from <https://www.statista.com/statistics/871513/worldwide-data-created/>
- Inequalities threaten wider divide as digital economy data flows surge – UNCTAD 29 September 2021.

<https://unctad.org/news/inequalities-threaten-wider-divide-digital-economy-data-flows-surge>

- Leistner, Matthias, and Lucie Antoine. "IPR and the use of open data and data sharing initiatives by public and private actors." Study commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the Committee on Legal Affairs (2022).
- Li, Qing, and Yu-Liu Chen. "Data flow diagram." *Modeling and Analysis of Enterprise and Information Systems*. Springer, Berlin, Heidelberg, 2009. 85-97
- López González, J. and J. Ferencz (2018), "Digital Trade and Market Openness", OECD Trade Policy Papers, No. 217, OECD Publishing, Paris, <https://doi.org/10.1787/1bd89c9a-en>.
- Malawer, Stuart S. "Internet Commerce and Trade Policy." International Initiatives for E-Trade (2007).
- Meltzer, J. P. (2015). The Internet, Cross-Border Data Flows and International Trade. *Asia & the Pacific Policy Studies*, 2(1), 90-102.
- Muggah, Robert, Rafal Rohozinski, and Ian Goldin. "The dark side of digitalization— and how to fix it." The World Economic Forum. URL: <https://www.weforum.org/agenda/2020/09/dark-side-digitalization> (дата звернення: 17.10. 2020). 2020.
- Mutual legal assistance and extradition- European Commission
- OECD (2022), "Fostering cross-border data flows with trust", OECD Digital Economy Papers, No. 343, OECD Publishing, Paris, <https://doi.org/10.1787/139b32ad-en>.
- PeeringDB, Interconnection Database, <https://www.peeringdb.com/>; PCH Packet Clearing House, Packet Clearing House Report on Internet Exchange Point Locations (database), accessed December 14, 2020, <https://www.pch.net/ixp/summary>; TeleGeography, Submarine Cables (database), <https://www.submarinecablemap.com/>. Data at [http://bit.do/WDR2021-Map-O\\_4](http://bit.do/WDR2021-Map-O_4).
- Schweitzer, Heike, and Robert Welker. "A legal framework for access to data—A competition policy perspective." German Federal Ministry of Justice and Consumer Protection/Max Planck Institute for Innovation and Competition (eds.): Data Access, Consumer Interests and Public Welfare (2021): 103-153.
- Taherdoost, Hamed. "Data Collection Methods and Tools for Research; A Step-by-Step Guide to Choose Data Collection Technique for Academic and Business Research Projects." *International Journal of Academic Research in Management (IJARM)* 10.1 (2021): 10-38.

- Taylor, Linnet. "The ethics of big data as a public good: which public? Whose good?." *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 374.2083 (2016): 20160126.
- The Difference Between a Data Protection Policy and a Privacy Policy - Beverly Davis, 21 February 2022
- The potential of open data to help businesses- The World Bank. <https://wdr2021.worldbank.org/spotlights/the-potential-of-open-data-to-help-businesses/>
- Transaction Costs - OECD Economic Outlook (2007).
- UNCTAD. Digital Economy Report 2021: Cross-border Data Flows and Development-For Whom the Data Flow. UN, 2021. [https://unctad.org/system/files/official-document/der2021\\_en.pdf](https://unctad.org/system/files/official-document/der2021_en.pdf)
- What is data? – Source: Data Education in schools
- What is personal data? -Source: European Commission.EU [https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data\\_en](https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en)
- What personal data is considered sensitive? –Source: European Commission.EU [https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive\\_en](https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en)
- Who owns personal data? – Source: The World Bank <https://wdr2021.worldbank.org/spotlights/who-owns-personal-data/>
- World Bank. World development report 2020: Data for better lives. The World Bank, 2021. <https://wdr2021.worldbank.org/the-report/>
- Worldwide Ecommerce Forecast Update 2022 - Digital Sales Growth Plummetts as Overall Retail Returns to Pre-Pandemic Trendlines- Report by Ethan Cramer-Flood | Jul 29, 2022
- Zheng, Guan. "Trilemma and Tripartition: The Regulatory Paradigms of Cross-Border Personal Data Transfer in the EU, the U.S. and China." *Computer law and security report*. 43 (2021): n. pag. Web.