Trade & Cross-Border Data Flows

Author
Javier López-González

By Javier López-González

Data is the lifeblood of our economic and social interactions. It carried the information used to research this article, powered the software used to write it and delivered the finished product so that it could be read by you today. When you download an app; when you stream your favourite music on your commute to work; when you leave a review of the latest restaurant you went to – you are relying on data flows, many of which cross at least one border. As a result, data is fundamentally, and in a very personal way, changing our lives.

At the same time, data is also changing how business operates. Data has given rise to new information industries; driven the development of innovative technologies (Artificial Intelligence, the Internet of Things and Additive Manufacturing – also known as 3D printing); and changed how global value chains (GVCs) are organized, how services are delivered and how food is grown. Today, firms of all sizes and across all sectors use data, and it is increasingly difficult for an international trade transaction to take place without a cross-border data transfer of some sort.

Cross-Border Data Transfers Enable Trade

Cross-border data transfers have allowed consumers around the world to access a wider range of goods and services, at a lower cost. By allowing SMEs to access IT services, such as cloud computing, and reducing the need for costly upfront investment in digital infrastructure, data flows have enabled the creation of a new breed of micro, small and medium-sized enterprises (MSMEs), the "micro-multinational", which is "born global" and is constantly connected. Better and faster access to critical knowledge and information has also helped SMEs overcome informational disadvantages, notably with respect to larger firms, reducing barriers to engaging in international trade and allowing them more readily to compete with larger firms.

Multinationals also rely heavily on cross-border data flows for their day-to-day operations: they use data from their affiliates around the world for a large number of internal, or back-office, tasks and even routine decisions. This includes moving human resources data to and from headquarters, sending data to R&D facilities located abroad, managing production processes and engaging in after-sale services. Today, efficient supply-chain management requires the smooth flow not just of goods, services and capital, but also of ideas and managerial know-how.

In sum, data has changed how and what we trade. It is a means for widening consumer choice and the affordability of goods and services, helping SMEs reach global markets and a key element of international production through GVCs. It is also a medium for the delivery of digitally enabled services across borders, and, with 3D printing, a means of delivering goods; it is an asset that can itself be traded, and an enabler of trade facilitation.

But Growing Data Flows Have Led to More Regulation

However, the ubiquitous exchange of data across borders has given rise to a range of concerns, especially when personally identifiable information is involved. This has led governments to update their data-related regulation, with a growing number of countries placing conditions on the transfer of data across borders or requiring that data be stored locally *(Chart 1)*. Such regulation can directly affect the ability to trade digitized goods and services, and can also have broader trade consequences, such as when it affects data flows critical for the coordination of global value chains. Even just the patchwork of different regulations can make it harder for MSMEs to benefit from digital trade.

Understanding the evolving landscape is key to delivering policies that are able to balance important policy and economic objectives arising from the flow of data.

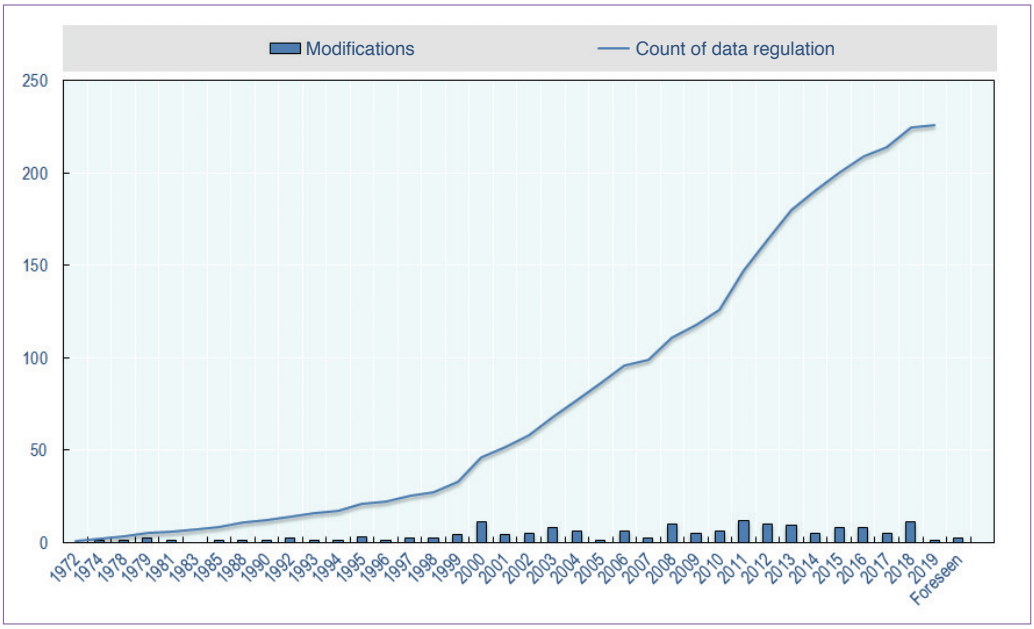
What Is Data & How Does It Flow?

Data transfers are, at their most functional level, related to the transmission of bits and bytes across different networks. When this article was sent from a computer in France to a recipient in Japan, the file was first broken down into "packets". These are small parcels of information marked with the Internet Protocol (IP) address, a device identifier, of the sender, the IP address of the recipient and a code identifying the sequence in which the packets are to be reassembled at destination. Upon leaving my computer, each crossed different networks taking different routes to arrive at the destination where they were reassembled into the original file.

How data flows and where it is stored is often a technical matter reflecting individual firm choices. Some outsource digital solutions to companies with servers located in different countries. Others rely on "mirrors", replicating webpages in different countries to increase delivery speed. And, today, with "the cloud", data, and copies

CHART 1

Data regulation is growing



Note: Data protection regulations include regulation on cross-border data flows and local storage requirements. Numbers are affected by the way in which regulations are structured, as this varies by country; some countries may have a single regulation covering a wide range of measures; others will have several different regulations covering, for example, restrictions on data flows for different types of data, and local storage requirements.

Source: Casalini and López-González (2019)

thereof, lives in many places at once. This means that the geography of data is different from the geography of trade flows.

How Do We Value Data?

How bits and bytes translate into dollars and cents is also difficult to establish. Data is valued at use, not at volume. That is, although Netflix is the largest single source of Internet traffic, estimated at 15% of bandwidth (according to "The Global Internet Phenomena Report" published by Sandvine.com in October 2018), it does not represent 15% of the value of data flows. It is the information that the data codifies that is of value. Moreover, the value of a particular dataset can differ across users. A file with 100 personal shopping entries may occupy the same memory space as one with 100 personal health records but its underlying value will be different to a retailer or a health service provider. The value of data can also increase when merged to become greater than the sum of its parts. For instance, the shopping entries linked to the health records can help target advertisements towards the health conscious shopper. Data also has both inherent and potential value, meaning that information not used today can become valuable tomorrow with changing business dynamics or combined with different data yet to become available.

Although data has been described as the "new oil", this characterisation is misleading. Like oil, it is an essential input into the economy, but data is not scarce, and the consumption of data by one person (or company) does not prevent its consumption by others since data can be copied and transferred at virtually no cost. This makes data different, *sui generis*.

Why Is Data Regulation Emerging?

The reasons why governments restrict or condition data flows, including the use of local storage requirements, can reflect a number of objectives and affect a range of data.

- Much of the debate about data flows revolves around the movement of personally identifiable information, which raises concerns about **privacy**. Today's economic and social interactions leave a larger information trail than in the past. But what information is being gathered and the use made of it is not always clear to the consumer. Since different people and cultures have different concepts of privacy, approaches to privacy differ widely across countries.
- Some measures conditioning data flows are aimed at **meeting different regulatory objectives**, such as access to information for audit purposes. In this sense, requirements for data to be

stored locally can be seen as the online equivalent of a longstanding practice in the offline world of ensuring that information is readily accessible to regulators. Such measures can be sector-specific, reflecting particular regulatory requirements and targeting specific data such as business accounts, telecoms or banking data.

- Other measures relate to **national security**, either in terms of protection of information deemed to be sensitive, or the ability of national security services to access and review data. The latter in particular can be very broad in nature, providing wide scope of access to any form of data.
- Other reasons for conditioning the flow of data or mandating that it be stored locally can be motivated by the desire to use a pool of data to encourage or help develop domestic capacity in digitally intensive sectors, a kind of **digital industrial policy**. This can reflect a view that data is a resource that needs to be made available first and foremost to national producers or suppliers. These approaches can be sector specific or apply to a range of data.

In discussing data regulation, it is important to bear in mind the underlying goals of the government. As for all policy-making, it is important to consider how effective the measures are in achieving their stated aims, the associated costs and trade-offs, and whether there are alternative measures that would enable a better balance among different aims to maximize overall benefits for the population. From a trade policy perspective, of interest is whether the same policy objective can be fulfilled in a way that has a less restrictive effect on trade.

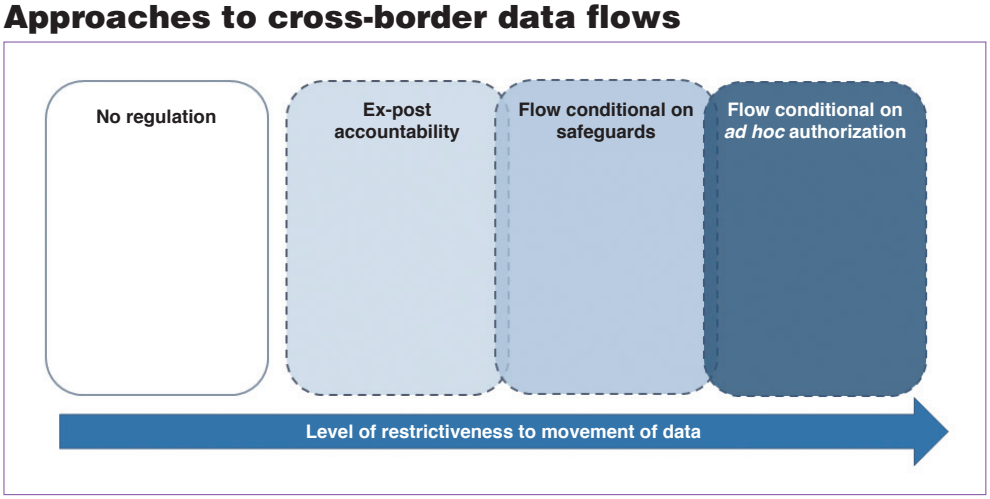
How Are Countries Regulating Data?

Due to differences in objectives, preferences and trade-offs, data regulation varies widely across countries. However, four broad approaches have emerged *(Chart 2)*. These are not mutually exclusive: different approaches can apply to different types of data even within the same jurisdiction. For example, health data might be subject to more stringent approaches than data related to product maintenance.

1. At one extreme, there is **no regulation** of cross-border data flows, usually because there is no data protection legislation at all. While this implies no restrictions on the movement of data, the absence of regulation might affect the willingness of others to send data.
2. The second type of approach does not prohibit the cross-border transfer of data nor does it require any specific conditions to be fulfilled, but provides for **ex-post accountability** for the data exporter if data sent abroad is misused (e.g. firms send data but if something goes wrong they are legally accountable).
3. A third approach, **flows conditional on safeguards**, includes approaches relying on the determination of adequacy or equivalence as ex-ante conditions for data transfer. These rulings can be made by a public authority or by private companies and can include requirements about how data is to be treated. Where an adequacy determination has not yet been made, firms can move data under options such as binding corporate rules, contractual clauses and consent.
4. The last broad type of approach, flow conditional on *ad hoc* authorization, relates to systems that only allow data to be transferred on a **case-by-case basis** subject to review and

CHART 2

Approaches to cross-border data flows



Note: Different approaches can apply to different types of data, even within the same jurisdiction.
Source: Casalini and López-González (2019)

approval by relevant authorities. This approach relates to personal data for privacy reasons but also to the more sweeping category of "important data", including in the context of national security.

International Instruments for Transferring Data Across Borders

As new rules on data flows have emerged, so too have a range of international instruments seeking to ensure interoperable approaches towards data protection, including across borders.

- **Privacy Shield** establishes rules and principles that meet European Union adequacy requirements. Companies operating in the United States can voluntarily choose to be liable for such privacy protection under US law in order to be able to freely move personal data between the EU and the US.
- **The APEC Cross-Border Privacy Rules (CBPR) System** is a framework to promote the interoperability of privacy regulation through enforcement of minimum standards. It is voluntary, requiring participating businesses to implement data privacy policies consistent with the CBPR. To date, six of the 21 APEC economies are participating, with 27 firms from two economies registered.
- **The OECD Privacy Guidelines** aim to ensure the protection of privacy in the face of new challenges posed by technologies and to avoid unjustified restrictions on data flows and the economic and social benefits they enable.
- **Convention 108**, or The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, is a treaty protecting the right to privacy of individuals with respect to personal data which is automatically processed. To date, 53 states have committed to establish, under their own domestic law, sanctions and remedies for violations of the Convention's provisions (see Annex A for more details).
- Data flows are also addressed in **Regional Trade Agreements** (RTAs) such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the US-Mexico-Canada Agreement (USMCA). In Article 14.11 of the CPTPP, for example, *"Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means."* However, *"each party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person"*. The Article also foresees measures inconsistent with this provision, but only *"to achieve legitimate public policy objective[s], provided that the measure: is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and… [when it] does not impose restrictions on transfers of information greater than are required to achieve the objective"*. The EU has adopted a new horizontal approach on cross-border data flows and personal data protection in trade agreements that it is pursuing in all its trade negotiations. This clause prohibits different forms of data localization and data storage measures. At the same time, the EU considers privacy and data protection as fundamental rights, and the EU clause provides that *"each party may adopt and maintain the safeguards that it deems appropriate for the protection of personal data and privacy"*. The cross-border flow of personal data is also not included in the EU-Japan Economic Partnership Agreement signed in 2018. However, Japan and the EU agreed to allow free flow of personal data through "mutual adequacy" of their respective data protection systems.

The Role of Trade Policy

As governments regulate cross-border data flows, it will be increasingly important that the trade impacts are also considered, to ensure that privacy, security, protection of intellectual property and the benefits of digital trade are all comprehensively understood, considered, and balanced. There are encouraging signs that regulators are trying to develop a shared sense of international good practice in data governance (e.g., the OECD Privacy Guidelines are being reviewed, and work is underway on principles on AI, both involving countries beyond OECD membership).

While the Internet was born global, and offers new opportunities for firms of all sizes, it also raises considerable challenges for policy in a world where borders and regulatory differences between countries remain. The trading system has experience in promoting open exchange in the context of regulatory difference: in seeking greater interoperability among approaches, requirements that standards be transparent, non-discriminatory and that they avoid unnecessary trade restrictiveness can play an important role. Indeed, interoperability between different data protection systems can be important not simply for trade but, equally, for ensuring that public policy objectives such as privacy and security can be met in a globalized digital world.

Note: The opinions expressed and arguments employed are those of the author and do not represent the official views of the OECD or of its member countries. This article draws heavily from joint work with Francesca Casalini found in Casalini, F. and J. López-González (2019), "Trade and Cross-Border Data Flows", OECD Trade Policy Papers, No. 220, https://doi.org/10.1787/b2023a47-en. JS

Dr. Javier López-González is a senior trade policy analyst at the Trade and Agriculture Directorate of the Organisation for Economic Cooperation and Development (OECD) and is responsible for the work on Digital Trade.