The Contours of Digital Trade: Shaping India's Trade Policy in an Evolving Global Landscape

Digital Trade Report: Analysis of USA, EU, China and India's Free Trade Agreements

Shivang Mishra
Vikas Verma
Vartul Srivastava
Dr. Pritam Banerjee

January 23, 2026

CENTRE FOR WTO STUDIES
CENTRE FOR RESEARCH IN INTERNATIONAL TRADE
INDIAN INSTITUTE OF FOREIGN TRADE
NEW DELHI, INDIA – 100014

Table of Contents

Boxes

Acknowledgement

The authors gratefully acknowledges Ms. Monika, Legal Consultant and Assistant Professor at Centre for WTO Studies for her valuable inputs and comments provided during the drafting of this report. The author is thankful for her mentorship and guidance to understand the digital trade issues and obliged her for sharing documents and her notes. The author greatly appreciates her knowledge of the digital trade issue of International Trade.

Introduction

Digital trade has become a defining feature of the modern global economy, growing exponentially over the past few decades. It now represents 24 per cent of total global trade. But there is still no one commonly agreed definition of digital trade. The following box shows how various international organisations have defined digital trade.

Box 1: Definitions of Digital Trade:

Digital trade has been defined as "*all international trade transactions that are digitally ordered and/or digitally delivered*" (WTO, OECD IMF, and UNCTAD, 2023),[1] and as "exclusively for the purposes of the work program, and without prejudice to its outcome, the term 'electronic commerce' is understood to mean the production, distribution, marketing, sale, or delivery of goods and services by electronic means.".[2]

The OECD (2011) defines e-commerce as, "anything that involves conducting electronic transactions, i.e., the sale or purchase of goods or services, whether between businesses, households, individuals, governments, and other public or private organisations, conducted over computer networks by methods specifically designed for the purpose of receiving or placing orders".

The WTO's Work Programme on Electronic Commerce (WPEC) defines electronic commerce as, "the production, distribution, marketing, sale, or delivery of goods and services by electronic means". The work programme recognises e-commerce as a cross-cutting issue, covering goods and services.

Digital trade has four aspects to it:

1. Digitally ordered trade
    a. Digitally ordered goods
    b. Digitally ordered services
2. Digitally delivered trade
    a. Digitally delivered goods

[1]International Monetary Fund, Organisation for Economic Co-operation and Development, United Nations Conference on Trade and Development, and World Trade Organization, Handbook on Measuring Digital Trade, 2nd ed. (Geneva: World Trade Organization, 2023), https://www.wto.org/english/res_e/booksp_e/digital_trade_2023_e.pdf

[2] Ministry of Statistics and Programme Implementation, "10.12 E-Commerce," Government of India, accessed September 29, 2025, https://mospi.gov.in/1012-e-commerce

b. Digitally delivered services

A significant portion of what is classified as digital trade falls under the category of "digitally ordered trade," which, in practice, primarily refers to merchandise trade conducted over the internet. This includes the sale of physical goods through e-commerce platforms (such as Amazon, Flipkart, Alibaba, Rakuten, etc.) with transactions facilitated by digital payment systems (like PayPal, Unified Payments Interface (UPI), Alipay, etc.). Despite being purchased online, these goods remain subject to traditional customs duties, border taxes and regulatory requirements, including those related to product safety, environmental standards and the protection of public health. Whether ordered in a store or through an online marketplace, their cross-border movements follow the same established trade policies and tariff structures either under most favoured nation (MFN) rates or under preferential trade agreements.

Since the regulatory framework for physical goods trade is already well-defined, the mere act of placing an order digitally does not alter the underlying trade dynamics. Yet, including digitally ordered tangible goods within the broader definition of digital trade risks inflating trade statistics, potentially overestimating the scale of actual digital trade.

Some experts who advocate the inclusion of digitally delivered goods as well argue that many goods that were once available only in physical form have now been digitised and are traded virtually. For instance, books and journals, as well as CDs and DVDs containing audio-visual content, are now also accessible as audiobooks and online movies through streaming on over-the-top (OTT) platforms. The range of digitised products is expected to grow further with technological advancements such as 3D printing.

Another notable type of digital trade may be classified as 'digitally ordered services,' wherein a service is requested digitally via an intermediary platform, such as Uber, Ola or UrbanClap. However, the actual service is rendered in a physical manner rather than online. These services resemble 'digitally ordered trade' and ought to be governed by current WTO laws.

Beyond digitally ordered goods, digital trade also extends to digital services, encompassing a wide range of subscription-based offerings such as music streaming (Spotify, YouTube Music), over-the-top (OTT) platforms (Netflix, Amazon Prime, Disney+ Hotstar), software-as-a-service (SaaS) products (Adobe Creative Suite, Microsoft 365, ChatGPT), and gaming services (Apple Arcade, PlayStation Plus). These digital services, unlike physical goods and services,

operate within an evolving regulatory landscape, often facing issues related to cross-border data flows, content regulation and digital taxation. As global digital trade policies continue to take shape, distinguishing between digitally ordered trade in physical goods and truly digital transactions will remain essential for ensuring clarity in trade analysis and policy formulation. Services are classified under four different types of modes by the WTO. Box 2 explains the four modes of services delivery. Of these, Mode 1 is also called "Digitally Delivered Services" and is the most important aspect of digital trade.

Box 2: Different Modes of Services as per WTO
As per WTO's General Agreement on Trade in Services (GATS), there are 4 modes of supply:[3] 1. Mode 1: Cross-border supply: When services flow from the territory of one WTO member into another 2. Mode 2: Consumption abroad: When a person consumes a service in another member's territory 3. Commercial presence: When a service supplier of one member establishes a commercial presence in another member's territory to provide a service, which accounted for about 60 per cent of global services trade in 2017 4. Mode 4: Movement of natural persons: when individuals of one WTO member temporarily enter the territory of another to supply a service.

Several studies have attempted to estimate the size of digitally delivered goods, but a definitive figure remains unavailable. The WTO (2024) estimates that global exports of digitally delivered services (DDS), primarily Mode 1 (Box 2) services, reached US$4.78 trillion in 2024, reflecting an annual growth rate of 10 per cent and accounting for more than 13 per cent of total global goods and services exports and 54 per cent of global services exports. However, there is no agreement among WTO members on the exact scope, coverage or definition of electronic transmissions, though they are generally understood in trade discussions as referring to digitally delivered trade.

[3] World Trade Organization, "@WTO X-post, status update, 1354439724878987268," X (formerly Twitter), posted Month Day, Year, time, https://x.com/wto/status/1354439724878987268

The OECD, in its Handbook on Measuring Digital Trade, takes the position that digitally delivered trade applies only to services, such as Mode 1 or cross-border services trade.

Box 3: India's IT Sector and the Shift Toward Digital Delivery
India's IT sector has long relied on a multimodal approach to service delivery, combining various trade modes to cater to global clients. A significant portion of projects are executed in India and delivered digitally under Mode 1, while firms also establish commercial presence abroad (Mode 3) to facilitate operations. Additionally, for specialised projects, high-level professionals are deployed overseas under Mode 4. However, Indian IT/ITeS exports are increasingly shifting towards digital delivery (Mode 1) as advancements in technology enable remote service provision. Historically, India's trade negotiations have prioritised securing Mode 4 commitments, ensuring easier movement of professionals across-borders. However, with the rise of virtual service delivery through video conferencing and digital platforms, Mode 1 has gained prominence. In this evolving landscape, India must recalibrate its trade strategy to secure multimodal commitments, placing greater emphasis on Mode 1, while ensuring flexibility across all service delivery channels.[4]

The structure of digital trade has also evolved. Digitally delivered trade now accounts for more than 50 per cent of total trade in 2024. The dominance of OECD countries has declined, while China's share has grown to 6.7 per cent and India's to nearly 4 per cent. India, in particular, has seen digital trade become a vital part of its economy, with 35 per cent of its total exports now represented by digital trade.[5] The increasing digitisation of commerce has been especially beneficial for India's micro, small, and medium enterprises (MSMEs), enabling them to expand market reach via e-commerce platforms, social media and digital payments. Digital imports have also shown a positive correlation with the gross value added (GVA) of MSMEs, helping

[4] Pritam Banerjee, Vartul, Saptarshee Mandal, and Divyansh Dua, "Negotiating for Digitally Delivered Services — Framework for a Comprehensive Approach," CRIT/CWS Working Paper No. 82 (Centre for WTO Studies, Centre for Research in International Trade, Indian Institute of Foreign Trade, March 26, 2025), https://wtocentre.iift.ac.in/workingpaper/CWS_WorkingPaper_82.pdf

[5] Organisation for Economic Co-operation and Development, Of Bytes and Trade: Quantifying the Impact of Digitalisation on Trade, OECD Digital Economy Papers (Paris: OECD Publishing, 2019), https://www.oecd.org/en/publications/of-bytes-and-trade-quantifying-the-impact-of-digitalisation-on-trade_11889f2a-en.html

bridge the gap between small firms and large corporations by providing access to new technologies and information flows.

Despite its rapid growth, digital trade is also at the centre of a complex regulatory debate. The Work Programme on Electronic Commerce, adopted by the WTO General Council in 1998, tasked four WTO bodies with exploring the implications of e-commerce on existing trade agreements. A major point of contention is the moratorium on customs duties on electronic transmissions, which prohibits WTO members from imposing tariffs on digital products and services. While high-income countries such as the United States and the European Union support the continuation of the moratorium, arguing that it fosters a stable digital trade environment, several developing nations, including India, have called for its removal to ensure policy space for potential tariff imposition.

This report examines the varying philosophies behind the regulation of digital trade as prevalent in three countries the USA, the EU, and China, and places the countries on a spectrum based on how conducive their policy environment is for the growth and advancement of digital trade. Then it discusses where India stands in comparison to its peers and what steps India should take to regulate and grow its digital economy.

The report demonstrates that the United States adopts the most liberal policy framework for its digital economy, operating within a predominantly free-market structure that has enabled the emergence of major global technology firms such as Meta, Google, and Nvidia. The European Union follows, maintaining an open digital market while simultaneously enforcing strong consumer protections and a rights-based regulatory framework.

India is positioned slightly to the right of the EU, adopting a balanced regulatory approach that seeks to promote the growth of the digital economy while ensuring adequate protection for its citizens. In contrast, China represents the most restrictive end of the spectrum, characterised by extensive state surveillance, broad government access to data, and stringent limitations on foreign digital service providers—conditions that have facilitated the rise of its domestic technology giants.

Digital Trade Guiding Philosophies for the US, EU, China and India

At the heart of digital trade governance lies a contest between three dominant regulatory philosophies, shaped by the world's leading digital powers—the United States, China, and the

European Union referred to as "digital empires".[6] These actors have established three competing models of digital capitalism, each influencing global trade rules, corporate behaviour and national regulations.

1. The United States champions a market-driven approach, advocating free data flows, minimal restrictions and strong intellectual property protection to support its global technology firms.
2. China employs a state-driven model, emphasising sovereign control over data, strict cybersecurity measures and digital infrastructure dominance to secure its geopolitical and economic interests.
3. The European Union has developed a rights-driven regulatory framework, balancing consumer protection, privacy (through policies like GDPR) and strict platform accountability to maintain public trust in the digital economy.

India, as an emerging digital economy, finds itself navigating this contested terrain, balancing economic liberalisation with strategic regulation. While it seeks to leverage digital trade for growth, it also emphasises data sovereignty and domestic regulatory autonomy, making its position unique within this global spectrum. As digital trade continues to expand, India's evolving stance will play a crucial role in shaping not only its own digital future but also the broader international discourse on trade, data governance and digital sovereignty.

The report looks at the guiding philosophies of these four regions in detail in the following section along with industry comparison, showing how companies registered in these regions are faring in the international markets and providing evidence for why the countries follow their particular philosophies. Later in the report, we also compare their commitments in various trade agreements related to digital trade.

Table 1 shows the growth in trade of digitally delivered trade from 2005 to 2024 as per the World Trade Organization.[7]

Table 1: Annual Digitally Delivered Services Trade				
Country	2005		2024	
	Imports	Exports	Imports	Exports

[6] Digital Empires: The Globalization of New Worlds, 2023 ed. (Oxford: Oxford University Press, [year]), https://global.oup.com/academic/product/digital-empires-9780197649268?cc=&lang=en&

[7] World Trade Organization, "Digitally Delivered Services Trade Dataset," World Trade Organization, updated July 2025, https://www.wto.org/english/res_e/statis_e/gstdh_digital_services_e.htm

(world share in brackets)	(in billion USD)	(in billion USD)	(in billion USD)	(in billion USD)
USA	113 (12.09%)	173 (16.94%)	454 (11.45%)	741 (15.51%)
EU	423 (44.91%)	395 (38.6%)	1694 (42.63%)	1872 (39.17%)
China	26 (2.7%)	14 (1.4%)	165 (4.16%)	220 (4.62%)
India	17 (1.9%)	30 (3%)	120 (3%)	275 (5.77%)
Source: WTO | Digitally Delivered Services Trade Dataset				

US Philosophy on Digital Trade

In 2025, the US digital economy was valued at $4.9 trillion, up from $4.2 trillion in 2022 (Figure A2.1, Annex II) and made up 18 per cent of its GDP. As will be shown in this report, the administrative policies of the US focus on addressing barriers to digital trade and emphasise the importance of free cross-border data flow, with limited exceptions.

Table 1 shows that total trade in digitally delivered services reached USD 1.2 billion in 2025, of which around USD 741 million were exports and USD 454 million were imports. The US's exports of digitally delivered exports account for 15.5 per cent of total world exports.

The US digital economy surpasses the entire GDP of India. According to a 2022 report by the US Bureau of Economic Analysis,[8] the US digital economy can be broken into the following four key activities:

1. **Priced Digital Services:** Representing the largest segment, priced digital services accounted for a gross output of USD 1.80 trillion and a value-added contribution of USD 2.56 trillion in 2022. This activity comprises more than 40 per cent of the digital economy.

[8] Bureau of Economic Analysis, "U.S. Digital Economy: New and Revised Estimates, 2017–2022," Survey of Current Business, December 6, 2023, https://apps.bea.gov/scb/issues/2023/12-december/1223-digital-economy.htm

2. **Infrastructure:** The second-largest segment, infrastructure, recorded a gross output of USD 1.32 trillion and a value-added contribution of USD 1.06 trillion in 2022, constituting approximately 30 per cent of the total digital economy.
3. **E-commerce:** E-commerce activities generated a gross output of USD 1.14 trillion and a value-added contribution of USD 599 million in 2022, representing about 25 per cent of the digital economy.
4. **Federal Non-defence Digital Services:** The smallest segment, federal non-defence digital services, contributed less than 1 per cent of the digital economy, with a gross output of USD 457 million and a value-added contribution of USD 300 million in 2022.

In the WTO, the United States and 84 other WTO members are participating in the Joint Statement Initiative on E-Commerce[9] (Box 4), where they are committed to pursuing a high-standard outcome that will meaningfully reduce digital trade barriers around the world. In December 2019, the United States joined a consensus in the WTO General Council to continue the long-standing moratorium on duties on electronic transmissions and the Work Program on Electronic Commerce. The United States continues to work to develop support for making this moratorium permanent and binding under the WTO. The US considers all forms of commercial activities by electronic means as part of digital trade, including both goods and services.[10] The US argues that duty-free digital trade boosts global economic growth. The moratorium has been critical to fostering digital trade for over two decades, benefiting economies, jobs and global communication. The US, along with the EU and other countries, prioritised renewing this moratorium at the WTO's 13th Ministerial Conference and it has been extended until the WTO 14th Ministerial Conference or March 2026, whichever is earlier, though concerns remain over its long-term sustainability.[11]

The US believes that data localisation, requiring data to be stored within a country's borders, acts as a trade barrier and brings inefficiencies and increases the cost of doing business. Although there is no federal data privacy law, the US government has introduced bills aimed at addressing data protection concerns.

[9] World Trade Organization, "Joint Statement Initiative on E-Commerce," accessed September 29, 2025, https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm

[10] Congressional Research Service, Digital Trade and Data Policy: Key Issues Facing Congress, CRS Report IF12347 (Washington, DC: Congressional Research Service, 2023), https://crsreports.congress.gov/product/pdf/IF/IF12347

[11] Meghna Bal and Niharika, A Primer on India's Digital Trade Policy (New Delhi: Friedrich-Ebert-Stiftung India Office, April 2023), https://library.fes.de/pdf-files/bueros/indien/20262.pdf

It believes that source code protection and encroachment of intellectual property rights (IPR) can limit a company's ability to capitalise on its innovations, especially in the context of the rapid growth of artificial intelligence (AI) and its rising importance.[12] So, it is also concerned about forced transfers of source code and proprietary algorithms, as these also pose security risks. It proposes prohibiting mandatory source code transfers as they make companies vulnerable to IP theft, especially small and medium enterprises (SMEs), who, unlike larger firms, may not be able to recover from IP theft. Although difficult to quantify, costs associated with IPR infringement could exceed the sales volume of a company. It supports trade rules that protect proprietary information and opposes forced technology transfers and discriminatory technology requirements.

However, it needs to be noted that in fall 2023, the US Trade Representative (USTR) withdrew support for certain proposed provisions in plurilateral negotiations in the Joint Initiative on E-commerce at the World Trade Organization (WTO) related to cross-border data flows, data localisation and source code, and suspended digital trade talks in the Indo-Pacific Economic Framework for Prosperity (IPEF).[13] USTR Katherine Tai attributed the decision to the need for domestic policy space amid rapid technological advancements and ongoing debates on regulating "Big Tech." This decision has been criticised by some US lawmakers and industry groups, who fear it could increase Chinese influence over international e-commerce rules and harm US exports. USTR is currently re-evaluating its approach to data and source code, acknowledging the need for a balanced approach that protects both US interests and legitimate regulatory goals.

National Trade Estimate (NTE), USTR, in its report, identifies four categories of digital trade barriers (e.g., barriers to cross-border data flows, discriminatory practices affecting trade in digital products, restrictions on the provision of internet-enabled services and other restrictive technology requirements).[14]

Box 4: Joint Statement Initiative

[12] Joshua Levine, Tom Lee, and Nicolo Pastrone, "Non-tariff Digital Trade Barriers," American Action Forum, November 14, 2023, https://www.americanactionforum.org/insight/non-tariff-digital-trade-barriers/#ixzz8YP64MqbJ

[13] Office of the United States Trade Representative, "Indo-Pacific Economic Framework for Prosperity (IPEF)," accessed September 29, 2025, https://ustr.gov/trade-agreements/agreements-under-negotiation/indo-pacific-economic-framework-prosperity-ipef

[14] Office of the United States Trade Representative, 2025 National Trade Estimate Report on Foreign Trade Barriers, March 2025, https://ustr.gov/sites/default/files/files/Press/Reports/2025NTE.pdf

The Joint Statement Initiative (JSI)[15] is a negotiation tool initiated by a group of WTO members who seek to advance discussions on certain specific issues without adhering to WTO's rule of consensus decision-making.[16] The JSI also aims to produce a binding agreement for its members and was created for the following issues:

1. E-commerce
2. Investment facilitation for development
3. Micro, small and medium-sized enterprises (MSMEs)
4. Domestic regulation in services
5. Trade and women's economic empowerment
6. Environmental sustainability
7. Plastics pollution

On e-commerce, the JSI encompasses several digital policy issues such as cross-border data flows, data localisation, online consumer protection, privacy and network neutrality. Supporters of JSI consider it important as building consensus on these issues has been difficult in the traditional WTO consensus-building method. JSI members account for around 90 per cent of global trade and the US, EU and China are all supporters of the JSI.

India and South Africa have been the most vocal critics of the JSI. Their argument is that the JSI weakens the multilateralism of the WTO, which is achieved by consensus building. Over half the WTO members, mostly developing countries, has opted out of these negotiations as they believe they will be coerced into accepting global trading rules shaped by developed countries. China states that it believes in shaping the rules of the JSI with active participation from within rather than sitting on the sidelines.

The position of the US, EU and China in JSI on various issues are discussed later in this report.

[15] WTO, "Joint Statement Initiative on E-Commerce."
[16] At WTO, decisions are adopted only when no member objects to it. Members are not required to actively support any decision; they can choose to remain silent but as long as there is a formal objection to any decision, it will not be passed.

China's digital economy became the largest in the world, reaching USD 7.1 trillion in 2021, according to a white paper by the China Academy of Information and Communication Technology (CAICT);[17] it increased to USD 7.5 trillion in 2023. In terms of growth rates, Asia's overall economic performance stood out in 2022, with the region's economic growth rate being significantly higher than the global average and that of the developed economies in Europe and in the United States. China's digital economy is far ahead of that of its peers, such as Japan, India, South Korea and Singapore in the Asia region.

Figure A2.2 (Annexure II) illustrates the exponential growth of China's digital economy from 2005 to 2023. In 2005, its market size stood at USD 364 billion, surging to USD 7.5 trillion by 2023, reflecting a remarkable expansion. This growth trajectory outpaces that of the digital economies in the US, EU and India.

Total trade in digitally delivered services increased from USD 40 billion in 2005 to 385 billion in 2024. In 2024, exports were USD 220 billion and imports were USD 165 billion. China's share in exports also increased from about 1.4 per cent in 2005 to 4.62 per cent in 2024 (Table 1).

China's digital economy's growth is driven by rapid technological advancements, a vast consumer base and supportive government policies. Chinese companies operating within this sector are now among the largest globally, ranking second only to those in the United States.

Figure A2.3 (Annexure II) shows the market size of China's cross-border e-commerce exports and imports from 2013 to 2023. Over this period, exports grew from USD 378 billion in 2013 to USD 1,854 billion in 2023, while imports increased from USD 63 billion to USD 505 billion. This growth highlights China's increasing dominance in the digital economy, as it has become a net exporter mirroring, its earlier achievements in traditional manufacturing that earned it the title of the "World's Factory."

It is evident that digital trade has played an increasingly crucial role for the Chinese economy and hence, has become a central part of China's national strategy. With initiatives like the 14th

[17] China Academy of Information and Communications Technology, "China's Digital Economy Hits $7.1 Trillion: White Paper," *State Council Information Office of the People's Republic of China*, July 30, 2022, https://english.www.gov.cn/archive/statistics/202207/30/content_WS62e515e6c6d02e533532eb06.html

Five-Year Plan on Digital Economy[18] the Fintech Development Plan issued by the People's Bank of China (PBOC) and the "Eastern Data, Western Computing" plan, China developed a detailed roadmap and incentives to shore up its digital economy.

Under the 14th Five-Year Plan, China will enhance its capabilities in "strategic areas", such as sensors, quantum information, communications, integrated circuits and blockchain, as well as push for technologies like 6G. It will also facilitate the digital transformation of the supply chain to better utilise data resources and improve the governance of the digital economy. Further, PBOC's Fintech Development Plan for 2022-2025 aims to drive the digital transformation of finance in the country over the next four years.

Under its 'Eastern Data, Western Computing' initiative, China created four regional hubs to address the supply-demand imbalance in computing capacity and boost its overall computational resources in order to strengthen its digital sector. China also introduced the 'Measures for Data Export Security Assessment' focusing on cybersecurity and data security, which has led to stringent regulations[19] on cross-border data transfers, especially regarding personal and important data.

On March 22, 2024, the Cyberspace Administration of China ("CAC") officially issued Provisions on Promoting and Regulating Cross-border Flow of Data. The new provisions introduce significant changes to China's existing cross-border data transfer regime. According to it, transferring "1,00,000" individuals' personal information has become the new threshold to trigger the need for SCC-recorded or personal information protection certification. For data processors other than critical information infrastructure operators (CIIOs), a standard contract or a personal information protection certification is needed for the outbound transfer of any sensitive personal information unless the transfer falls under one of the enumerated exemptions. If data processors other than CIIOs transfer sensitive personal information of more than 10,000 people out of China, or a CIIO transfers any personal information (including sensitive personal information) out of China, a data security assessment is required.

[18]Yi Wu, "Understanding China's Digital Economy: Policies, Opportunities, and Challenges," *China Briefing*, August 11, 2022, https://www.china-briefing.com/news/understanding-chinas-digital-economy-policies-opportunities-and-challenges/

[19] Ropes & Gray LLP, "China's New Rules on Cross-Border Data Transfers: Key Highlights," *Ropes & Gray Insights*, April 5, 2024, https://www.ropesgray.com/en/insights/viewpoints/102j4i1/chinas-new-rules-on-cross-border-data-transfers-key-highlights

China's Cybersecurity Law, enacted in 2017, imposed significant compliance costs on multinational companies, giving the Chinese government broad access to their software source codes, thus exposing them to industrial espionage risks, giving some Chinese firms an unfair advantage and increasing the risk of theft of trade secrets.

The law also grants Beijing the right to request access to the software source code and national security reviews allow deeper access into companies' intellectual properties. This is in contrast to democracies, where laws regulate both corporate and government access to information; China's laws provide the government unrestricted access to personal and commercial data.[20]

EU's Philosophy on Digital Trade

The EU's digital economy is expected to reach USD 600 billion in 2025, up from USD 354 billion in 2019.[21] Digital trade has become a key element in the EU's trade policy. The EU, as the world's largest exporter and importer of digitally deliverable services, has a strong market position. EU's total trade in digitally delivered services increased from USD 818 billion in 2005 to USD 3.5 trillion in 2024. Its exports increased from USD 395 million in 2005 to USD 1872 million in 2024 with a global share of almost 40 per cent in 2024[22] (Table 1).

The increasing importance that the EU attaches to the digitalisation of the economy is reflected in its trade policy, in which the European Commission set out the objective of supporting the green and digital transformation of the EU economy. In order to ensure a leading position for the EU in digital trade, the EU is aiming to shape digital trade rules, in particular at the World Trade Organization (WTO), through its bilateral trade agreements and, most recently, in self-standing bilateral digital trade agreements.[23]

[20] Daniel Wagner, "The Global Implications of China's National and Cyber Security Laws," *Diplomatic Courier*, August 7, 2020, https://intpolicydigest.org/the-global-implications-of-china-s-national-and-cyber-security-laws/

[21] European Commission, *Building a Data Economy — Brochure*, Shaping Europe's Digital Future (Publication, 23 September 2019), https://digital-strategy.ec.europa.eu/en/library/building-data-economy-brochure

[22] WTO, Digitally Delivered Services Trade Dataset, available at https://www.wto.org/english/res_e/statis_e/gstdh_digital_services_e.htm?ref=digitalpolitics.co#:~:text=The%20dataset%20contains%20WTO%20estimates,for%20the%20period%202005%2D24.

[23] A self-standing bilateral digital trade agreement is a trade agreement signed between two countries that focuses specifically and exclusively on digital trade issues, rather than being part of a broader free trade agreement (FTA) or economic partnership agreement.

Figure A2.4 (Annexure II) illustrates the share of revenue generated by European companies through e-commerce. Ireland leads the region, with 33 per cent of its revenue derived from e-commerce activities.

Despite this strong performance in e-commerce revenue, European countries lack major players in the digital economy compared to the United States and China. The dominance of US companies with significant market shares in the European market highlights the region's reliance on foreign digital giants, underscoring a gap in homegrown global-scale digital enterprises within Europe.

Thus, it follows a rights-driven approach to digital trade, placing it somewhere between the US and China. This is partly because it relies on foreign companies having a large market share in their domestic market. The EU does not adopt policies that purposely puts restrictions on digital trade, nor does it compromise on the rights and privacy of its citizens to promote a more liberal market policy. It allows free market policies related to digital trade to operate as long as they align with its philosophy of protecting the privacy and rights of its citizens. If the EU feels that any segment of trade is harming the rights and privacy of its citizen, it intervenes and brings in laws to regulate it.

India's Digital Economy

India is also a rising power, along with the US, the EU and China; its digital economy is also increasingly becoming an important part of overall GDP. Digital trade is promising in terms of growth and productivity, relative to trade in goods. India digital economy was valued at USD 402 billion in 2023, accounting for 11.74 per cent of India's GDP.

Global trade patterns in the last decade indicate a rise in the services trade to gross domestic product (GDP) as against an overall decline in the global trade to gross domestic product. India has a strong position in services. Information technology and business process management (IT-BPM) are the largest exports for the country, accounting for almost half of total services exports in 2021-22. India ranked among the top ten largest exporters of digitally deliverable services in 2021. India's total trade in digitally delivered services increased from USD 47 billion in 2005 to USD 395 billion in 2024. Its exports increased from USD 30 billion in 2005 to 275 billion in 2024, increasing its share in global exports of digitally delivered services from

3 per cent to almost 6 per cent (Table 1). Both the OECD and WTO found that India's global share in digital exports has been rising whereas that of OECD countries has been falling.[24]

Figure A2.5: (Annexure II) illustrates the growth of India's e-commerce market from 2014 to 2024 Valued at approximately USD 14 billion in 2014, the market expanded significantly to reach USD 123 billion in 2024.

Digital trade has been immensely helpful for India's MSME sector. Digitalisation and flow of cross-border transmission has helped smaller firms to reach new customers through e-commerce, understand customers analytics and cost-efficient marketing, and promoted the use of social media. The increase in digital imports by MSMEs has also been helpful in increasing gross value added (GVA) and employment.[25]

Despite this notable growth, India's digital economy remains relatively underdeveloped compared to the US, China, and the EU. This lag can be attributed to insufficient infrastructure and limited government support. According to the OECD's Digital Services Trade Restrictiveness Index, India ranks as the second most restricted economy with a score of 0.31, with infrastructure and connectivity contributing the largest share of restrictions at 0.12. These challenges highlight the need for targeted reforms to unlock the full potential of India's digital economy.

Box 5: Digital trade provisions India has already agreed to
In various provisions in its FTAs, India has agreed on a number of digital trade related areas without any major issues or conflicts that would merit a deeper discussion. These include the following: 1. Domestic electronic transaction framework as per the UNCITRAL Model Law on Electronic Commerce (1996). 2. Hard obligation on authentication of e-contracts, e-signatures, e-authentication and electronic trust services to not deny the legal validity of a signature solely on the basis that the signature is in digital or electronic form.

[24] WTO, "Digitally Delivered Services Trade Dataset."
[25] Badri Narayanan Gopalakrishnan et al., *The Impact of Cross-Border Digital Transmissions on the MSME Sector in India and the Benefits of the WTO E-Commerce Moratorium* (IGPP, June 2023), https://igpp.in/wp-content/uploads/2023/06/The-Impact-of-Cross-Border-Digital-Transmissions-on-the-MSME-Sector-in-India-and-the-Benefits-of-the-WTO-E-Commerce-Moratorium-.pdf

3. Digital identities – A digital identity is an electronic representation of an individual's or entity's identity in the digital space. It consists of a set of data attributes that are used to uniquely identify and verify the identity of a person, organisation, or device during online interactions. Digital identities are crucial to enable secure access to online services, carry out electronic transactions and ensure trust in digital ecosystems.
4. Paperless trading and e-invoicing – Paperless trading refers to the use of electronic means to exchange trade-related information and documents such as invoices, bills of lading, certificates of origin and customs declarations between parties involved in a transaction. This process eliminates the need for paper-based documents, speeding up trade processes and reducing administrative burdens.
5. Open internet access – Open internet access refers to the principle that all individuals and organisations should have unrestricted, equal and non-discriminatory access to the internet. It supports the idea that users can freely access any lawful content, applications and services on the internet, without interference from internet service providers (ISPs) or governments. This concept is closely tied to net neutrality, which advocates open and fair treatment of all internet traffic.
6. Data innovation – Data innovation refers to the process of leveraging data, analytics and emerging technologies to create new products, services and business models, or processes that drive value, enhance decision-making and foster growth. It involves the creative use of data to solve problems, improve efficiency and generate insights that were previously unattainable. Examples include big data analytics, artificial intelligence (AI) and machine learning (ML), the Internet of Things (IoT), blockchain, etc.
7. Open government data – Open government data (OGD) is the practice of making government-held data freely available to the public in a structured, machine-readable format without any restrictions on its usage or redistribution. The goal of OGD is to increase transparency, improve public services, foster innovation and drive economic growth by leveraging data collected by public institutions. However, India has concerns regarding misuse of government data by countries India deems hostile to its interests such as Pakistan and China.
8. Online consumer protection – Online consumer protection refers to a set of laws, regulations and best practices designed to safeguard consumers' rights and interests

in the digital marketplace. Online consumer protection aims to ensure that consumers can engage confidently in digital transactions with a guarantee of fair treatment, privacy and security. Here also, India has concerns related to jurisdiction challenges in cross-country legal disputes.

A detailed explanation of these topics is presented in Annexure III.

Industry Comparison

Before delving into a comparison of the digital trade policies adopted by the four key regions within their respective free trade agreements (FTAs), it is important to first examine the industries operating in the digital space in these regions.

As illustrated in the figures (Annexure II), multinational corporations from the United States dominate a wide range of sectors, holding significant market shares both domestically and internationally. This extensive dominance underpins the US's advocacy for liberal digital trade policies and its push to make the moratorium on e-commerce duties permanent.

China, by contrast, has developed major corporations in the digital sector that have only recently begun to expand their influence in foreign markets. Historically, Chinese companies, supported by the government's "Great Firewall," enjoyed domestic dominance and even monopolistic control, effectively barring foreign firms from entering the Chinese market. This domestic-centric model explains China's preference for restrictive digital trade policies aimed at protecting its industries and limiting foreign competition.

In comparison, the EU has a smaller number of prominent digital players, while India lacks any major global corporations in the digital economy. Both regions see substantial market presence from foreign companies such as ByteDance, Apple, Microsoft, Amazon, Tencent and Meta. This scenario motivates the EU and India to adopt balanced digital trade policies that leverage the benefits of digital trade while safeguarding resident data and maintaining policy flexibility for regulation.

Financial Services

Figures A2.6, A2.7, A2.8, and A2.9 (Annexure II) present the market capitalisation (in USD billions) of listed financial services companies in India, China, the United States and the European Union.

In India, HDFC Bank leads the financial services sector with a market capitalisation of nearly USD 165 billion. While the bank has a significant footprint in traditional banking, digital-led financial services represent one of its fastest-growing areas. Collectively, the top 10 companies in this sector have a combined market capitalisation exceeding USD 570 billion.

In China, the Industrial and Commercial Bank of China (ICBC) holds the largest market capitalisation at USD 313 billion, more than half the size of India's top 10 financial services companies combined. The top 10 Chinese companies in this sector collectively account for almost USD 1.5 trillion in market capitalisation, showcasing the scale of the country's financial services industry.

In the United States, the largest players in financial services are traditional banks with market capitalisations reaching trillions of dollars. However, the US also has a significant number of companies operating exclusively in the digital financial services space with a global presence. Fiserv, with a market capitalisation of USD 118 billion, is the largest among them. The top 10 companies in this segment have a combined market capitalisation of approximately USD 500 billion. Notably, these US companies operate primarily in the digital domain, in contrast to Indian companies, which also engage heavily in traditional banking, but both have a similar combined market cap. This distinction highlights the dominance of US digital financial services companies.

In the European Union, Intesa Sanpaolo, an Italian bank, leads the sector with a market capitalisation of USD 72 billion. The combined market capitalisation of the top 10 financial services companies in the EU is approximately USD 550 billion, reflecting the region's relatively modest scale compared to China and the US

E-commerce

Figures A2.10, A2,11, A2.12 and A2.13 (Annexure II) display the market capitalisation (in billion USD) of listed e-commerce companies in India, China, the United States and the European Union.

In India, the major players in e-commerce include Amazon, Flipkart, Myntra, and Ajio. Flipkart, originally an Indian company, is now owned by US-based Walmart, and Myntra is a subsidiary of Flipkart. Ajio is not listed. Among the listed companies, Nykaa is the largest, with a market capitalisation of USD 5 billion. The combined market capitalisation of listed Indian e-commerce companies totals USD 8.3 billion. India's total domestic e-commerce market, measured by gross merchandise value (GMV), is valued at approximately USD 60 billion.

In China, Alibaba is the largest e-commerce company with a market capitalisation of USD 202.56 billion. This single company is more than three times the size of India's entire domestic e-commerce market. The combined market capitalisation of China's top 10 e-commerce companies is around USD 550 billion. Notably, all the top 10 companies are Chinese, indicating that the domestic e-commerce market in China is largely controlled by local players.

In the United States, Amazon leads the e-commerce sector with a market capitalisation of USD 2.35 trillion. Amazon is a global player with a presence in several countries, solidifying its position as a dominant force in global e-commerce. Other companies such as Walmart and BestBuy also operate in the e-commerce space, but their primary business models are still rooted in physical retail.

In the European Union, the largest domestic e-commerce company is Germany-based Zalando, with a market capitalisation of USD 9 billion. While Zalando leads the EU market, Amazon is the dominant e-commerce player overall. The combined market capitalisation of the top 10 domestic EU e-commerce companies totals USD 54 billion.

In the global e-commerce industry, it is evident that US companies dominate not only the US but also the Indian and European markets. In contrast, the Chinese e-commerce market remains overwhelmingly controlled by domestic companies, with limited foreign competition gaining a foothold.

Software and Technology

Figures A2.14 to A2.19 (Annexure II) illustrate the market capitalisation of companies in the software and technology domains.

In India, Coforge and TCS lead in the software and technology sectors, with market capitalisations of USD 7.4 billion and USD 177 billion respectively. The combined market capitalisation of the top 10 Indian software companies is approximately USD 25 billion, while the top 10 technology companies collectively reach USD 576 billion.

In China, Kingsoft and Xiaomi are the largest players in the software and technology domains, with market capitalisations of USD 5.87 billion and USD 108.78 billion respectively. The combined market capitalisation of China's top 10 software companies is around USD 16 billion, while that of the top 10 technology companies amounts to USD 316 billion.

In the United States, Apple, Microsoft, and Alphabet (Google) dominate both the software and technology sectors globally, with market capitalisations of USD 3.8 trillion, USD 3.2 trillion, and USD 2.3 trillion respectively. The combined market capitalisation of the top 10 US software companies exceeds USD 11 trillion, underscoring the dominance of Apple and Microsoft, which extend their influence beyond software into the broader technology space.

In the European Union, SAP, based in Germany, is the largest software company with a market capitalisation of USD 291 billion. The combined market capitalisation of the top 10 software companies in the EU is USD 542 billion.

Video Games

Figures A2.20 to A2.22 (Annexure II) represent companies in the video games domain. India does not have any company of significance in the video game industry.

In China, Tencent is the biggest video game company with a market cap of USD 490 billion. The combined market cap of the top 10 companies is USD 585 billion.

In USA, Microsoft is the biggest company in the video games domain. After Microsoft, Roblox is the second biggest with a market cap of USD 39.01 billion. The combined market cap of the top 10 companies is USD 136 billion.

In both China and the USA, one company has significant domination in the industry. A big reason behind this is that both Tencent and Microsoft buy other gaming companies and

incorporate them into their own business. Tencent also has a stake in various US-based gaming companies.

In EU, CD Project is the biggest gaming company with a market cap of USD 4.64 billion. The combined market cap of the top 10 companies is USD 11 billion.

Digital Trade and Artificial Intelligence

In the rapidly evolving global commerce landscape, digital trade has emerged as a critical driver of economic growth and innovation. The integration of artificial intelligence (AI) into digital trade represents a transformative shift that promises streamlined operations and enhanced efficiency and overcomes traditional barriers. AI technologies, like machine learning and natural language processing, transform digital trade as it assists in automating and optimising complex processes.[26]

Broadly, AI refers to "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy".[27] These systems use data to train algorithms and are embedded in hardware such as robots, autonomous cars and IoT devices. Common AI applications include smart assistants, translation, self-driving cars, medical diagnostics and robotics. AI is reshaping international trade, particularly through specific applications like data analytics and translation services, which reduce trade barriers.

Figures A2.23 and A2.24 (Annexure II) shows market the capitalisation of the top Chinese and US artificial intelligence companies. In China, Baidu, Tencent, Alibaba, SenseTime and Huawei are among the biggest AI companies but AI is a small part of their business model currently. Apart from these, Pony.AI is the biggest company that operates only in the AI sector with a market cap of 4.7 billion USD. US tech giants such as Apple, Nvidia, Microsoft, Alphabet (Google) and Meta are the biggest players in AI.

[26] Jennifer ThankGod, "Revolutionizing Digital Trade with Artificial Intelligence: Streamlining Processes and Breaking Barriers," SSRN Paper (March 1, 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4858782

[27] Organisation for Economic Co-operation and Development, *Recommendation of the OECD Council on Digital Security of Critical Activities (OECD-LEGAL-0449)*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

However, there are challenges in AI development that international trade rules could address, such as global access to data for training AI systems. Cross-border data flows are essential for the modern economy, enabling communication, financial transactions, access to a vast array of services, efficient manufacturing, medical research and many more.

Trade policy must evolve and keep pace with rapidly evolving AI systems. Regulating AI is challenging as countries need to ensure that regulations are sufficiently flexible to support and respond to technological innovation, while still addressing a range of public policy objectives from promoting innovation to ensuring fair competition, non-discrimination, privacy and security, which often involves trade-offs. Recent trade agreements like the United States-Mexico-Canada Agreement (USMCA), the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the emergence of digital-specific agreements reflect early efforts by major economies to establish comprehensive trade rules that address barriers to digital trade and cross-border data flows.

The current AI growth is driven by strong venture capital investments and the generation of large amounts of data because of rapidly expanding digital trade. The amount of big data being generated in today's increasingly digitised economy is growing at a rate of 40 per cent each year and is expected to reach 163 trillion gigabytes by 2025.[28]

AI encompasses the following four main components:

- Machine learning
- Robotics
- Artificial Neural Networks (ANNs) that mimic the human brain's neocortex to enable thinking-like processes in computers
- Generative AI that produces content like text, images and videos in response to prompts and improves with training

The application of AI-led technology is driving growth at the individual, business and economy levels. At the micro level, businesses are adopting AI to lower labour costs, increase productivity, enhance quality and minimise downtime. At the macro level, automation boosts productivity.

[28] Statista, *Artificial Intelligence: In-Depth Market Analysis*, Market Insights Report, released July 2024, https://www.statista.com/study/50485/in-depth-report-artificial-intelligence/

A September 2025 NITI Aayog report, *AI for Viksit Bharat: The Opportunity for Accelerated Economic Growth*, estimates AI could add **$500-$600 billion to India's GDP by 2035** through productivity gains.[29] According to a projection by the World Economic Forum, AI might generate 40 million new jobs in India by 2030.[30] According to these forecasts, AI is anticipated to have a considerable and favourable impact on India's GDP development in the years to come. By boosting productivity, facilitating the creation of new goods and services, and enhancing global competitiveness, AI is predicted to increase GDP growth.

According to the paper, "Artificial Intelligence and international trade: Some preliminary implications",[31] the implications of adopting AI are the following:

1. **<u>It can affect digital trade in the following manner:</u>**
    a. It can increase the productivity of adopters for sectors such as finance, insurance and on-line consumer platforms. However, some sceptics also argue that the perceived increase in productivity via AI is a paradox as there is lack of statistical evidence.
    b. It can reduce trade costs by improving logistical efficiency and removing language barriers (for example, the recently announced Samsung AI has AI assisted language translations on live calls.)
2. **<u>Trade also affects AI</u>**
    a. Access to hardware for the development of AI including high performance computing equipment, data sensors, communication units and adequate network equipment to ensure seamless information flow and interlinkages between units in the AI system.
    b. Trade data, especially in services, is very important in the development of AI and improving its accuracy, prediction capabilities and reliability.
    c. Restrictions on cross-border data flows can reduce AI's capabilities.
    d. Intellectual property rights (IPR) can affect what AI can access and train on.
3. **<u>Trade Measures affecting AI</u>**

[29] NITI Aayog, AI for Viksit Bharat: The Opportunity for Accelerated Economic Growth,
[30] Bhattacharya S, Ravindran A. The impact of artificial intelligence on the Indian economy: A review of the literature. J Econ Perspective. 2021;35(3):175-202.
[31] Janos Ferencz, Javier López González, and Irene Oliván García, "Artificial Intelligence and international trade: Some preliminary implications," OECD Trade Policy Papers No. 260 (Paris: OECD Publishing, 2022), https://www.oecd.org/en/publications/artificial-intelligence-and-international-trade_13212d3e-en.html

a. The development, deployment, and implementation of AI systems relies heavily on ICT related hardware. Barriers to trade on such hardware could negatively affect adoption of AI.
b. Services such as telecommunication services, computer services, transport, logistics, distribution and financial services play an important role in trade. The adoption of AI can improve efficiency in these areas. However, trade barriers could hinder progress. Trade regulations for digitally enabled services that are essential to digital transformation, especially in key sectors such as telecommunications, computer services, financial services and transport, have become more restrictive.
c. Movement of skilled personnel is a crucial part of the development and adoption of AI, especially cross-country movement. Restrictions on physical movement of professionals could also hinder the progress of AI.
d. Access to data is the most important aspect of development of AI and improving its efficiency, prediction capabilities and reliability. However, restrictions on cross-border data transfers could slow down the development of AI and reduce its efficiency. Access to data often does not simply mean access to large volumes of data. There are diminishing returns to scale on data, meaning that as more and more data is used, its usefulness declines. The variance or variety of data is also an important aspect. Access to a wide variety of data is necessary for the development of AI.

4. <u>Provisions in RTAs and emerging digital trade agreements relevant for AI systems</u>

a. RTAs are increasingly including provisions on data flows, which are essential for AI systems that rely on vast amounts of data. However, only a fraction of these agreements have binding commitments to enable data flows across borders.
b. Provisions related to the protection of personal information and privacy are common in RTAs, affecting the use of data in AI systems.
c. Some RTAs include commitments that prohibit forcing companies to locate computing facilities in the host country, which can reduce operational costs for AI systems that rely on centralised data processing.
d. RTAs are starting to include commitments to protect AI algorithms by prohibiting the requirement for source code transfers as a condition for market

access. This protects proprietary AI algorithms, although exceptions exist for regulatory or judicial needs.

e. Newer agreements like the Australia-Singapore Digital Economy Agreement and the Digital Economy Partnership Agreement (DEPA) include provisions for promoting AI and data-driven innovation. These agreements also focus on ethical governance frameworks for AI, ensuring safe and responsible use.

5. **Trade enhancing effects**

AI can enhance trade by

a. providing real-time data analysis and timely information
b. identifying emerging trade patterns
c. optimising supply chains
d. improving decision making
e. enabling real time monitoring of trade and economic indicators.

Each of these regulatory models has shaped the digital economy of the four players, influencing where innovation flourishes, where digital giants emerge and how businesses navigate cross-border operations.

Reasons for Regulating Digital Trade

Before conducting a detailed analysis of how varying national philosophies affect the approach to individual provisions in the digital trade chapter of FTAs, it would be instructive to examine the reasons a nation might have to regulate digital trade.

The authors posit that there are broadly four major purposes behind a nation regulating international digital trade.

1. Regulating for revenue – A nation might impose taxes and duties on digital products and services in order to raise revenue from firms benefiting from accessing the market of the country.
2. Regulating for competition – A nation might either wish to prevent anti-competitive practices in its market or support its domestic firms to increase their competitiveness in domestic or foreign markets.

3. Regulating for consumer welfare – Consumer protection, as well as the protection of the personal data of consumers, might be another set of reasons that would lead a nation to regulate digital trade.
4. Regulating for security – National security could be a strong driver behind a nation regulating digital trade in sensitive sectors and areas.

Every provision in the digital trade chapter of an FTA will likely interact with one or more of these purposes. And each kind of regulation will bring certain kinds of consequences, both positive and negative.

When trying to understand the best way forward for India in terms of building a digital economy and for positioning itself on critical digital trade issues in its FTAs, an examination of each digital trade provision in the light of the purposes mentioned above should prove beneficial. As such, the authors use the above categorisation as a tool to understand India's position on the digital trade issues discussed below, and to make recommendations on India's future approach on such issues.

Scope and General Provisions of Digital Trade Agreements

This section examines the scope and general provisions adopted by the United States, China, the European Union and India in their respective trade agreements, providing insights into their broader digital trade philosophies.

To further contextualise these commitments, information from the Digital Trade Integration Project is incorporated to assess whether the digital trade policies of these economies function as regulatory restrictions or enabling measures. By analysing their approaches to key digital trade provisions, this section highlights how these economies navigate market access, regulatory flexibility and policy autonomy in shaping the global digital economy.

The USA

Across its free trade agreements (FTAs),[32] the United States consistently acknowledges the economic growth and opportunities enabled by electronic commerce under the 'Scope and General' provisions of their respective digital trade or e-commerce chapters. These provisions emphasise the importance of avoiding barriers to the use and development of electronic

[32] Office of the United States Trade Representative, "Free Trade Agreements," USTR, https://ustr.gov/trade-agreements/free-trade-agreements

commerce and recognise the applicability of the WTO Agreement to measures affecting e-commerce, thereby grounding US commitments within the multilateral trade framework.

In several US FTAs such as the US-Chile FTA and US-Colombia FTA, the general provisions allow parties to impose internal taxes and charges on digital products, provided these are consistent with the provisions in the agreement. At the same time, measures affecting the supply of services through electronic means are subject to the obligations established under the chapters on cross-border trade in services, financial services and investment, while preserving exceptions for non-conforming measures.

Under more recent digital trade frameworks, such as the US-Mexico-Canada (USMCA) and the US-Japan Digital Trade Agreement,[33] the parties agreed that the e-commerce chapters do not apply to the following:

- government procurement
- services supplied in the exercise of governmental authority
- information held or processed by or on behalf of a party, including measures related to its collection or handling.

These carve-outs delineate the boundary between commercial digital activity and sovereign or governmental functions, preserving policy space for national governments in sensitive areas. The US has repeated this in its communication to the JSI on e-commerce.[34]

The US-Japan Digital Trade Agreement further introduces general and security exceptions under Articles 3 and 4, respectively. Article 3 incorporates, mutatis mutandis, the provisions of Article XIV (a–c) of the GATS and Article XX of the GATT 1994,[35] along with their

[33] United States Trade Representative, *Agreement between the United States of America and Japan concerning Digital Trade*, signed October 7, 2019, https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf

[34] World Trade Organization, *Notification under paragraph 2(a) of Article 31bis of the TRIPS Agreement or paragraph 2(a) of the 2003 Decision*, IP/N/9/ (WTO, [date]), https://docs.wto.org/dol2fe/Pages/FE_Browse/FE_B_009.aspx?TopLevel=10785

[35] Under Article XIV (a–c) of the General Agreement on Trade in Services (GATS) and Article XX of the General Agreement on Tariffs and Trade (GATT) 1994, WTO members are allowed to adopt certain measures that might otherwise breach their trade commitments, provided such measures are not applied in a discriminatory or protectionist manner. These include actions necessary to protect public morals or maintain public order, safeguard human, animal or plant life or health, and ensure compliance with laws and regulations such as those preventing fraud, deceptive practices or privacy violations. By applying these provisions mutatis mutandis, that is, with suitable adjustments, the digital trade agreement extends these well-established WTO exceptions to the digital domain, ensuring that both the United States and Japan retain the right to regulate digital trade for legitimate public policy, health or national security reasons within the same legal framework recognised by the WTO.

interpretative notes, thereby ensuring that established WTO exceptions such as those for the protection of public morals, health or national security are fully integrated into the agreement's framework. Article 4 reinforces national security protection by stipulating that no party is required to disclose information contrary to its essential security interests and that each party retains the right to apply any measures it deems necessary for the maintenance or restoration of international peace and security, or for the protection of its essential security interests.

The same approach is reflected in the United States' communication to the Joint Statement Initiative (JSI) on e-commerce,[36] wherein it proposed that any multilateral framework should also exclude government procurement, services supplied in the exercise of governmental authority and information held or processed by or on behalf of a government, including measures related to such information.

Collectively, these provisions reflect the US model of digital trade governance, which combines a pro-liberalisation stance promoting open digital markets and cross-border data flows with explicit safeguards for governmental functions, national security, and regulatory autonomy.

The European Union (EU)

Across its Free Trade Agreements (FTAs), the European Union (EU) has developed a coherent and legally consistent framework for digital trade and e-commerce, combining openness with strong regulatory safeguards. Several common elements recur across these agreements. First, the scope of e-commerce or digital trade chapters uniformly covers trade enabled by telecommunications or other information and communication technologies (ICT). The EU-Chile FTA (Article 19.1) excludes audio-visual services, while the EU-Mercosur FTA (Article 10.46, Sub-Section 6) and the EU-Japan FTA (Article 8.70, Sub-Section 5) extend this exclusion to include broadcasting, notarial or equivalent professions, and legal representation services. Further, both the FTAs recognise the principle of technological neutrality in e-commerce. It reflects the EU's consistent legal policy to preserve technological neutrality and cultural diversity, in line with its broader commitment to maintaining autonomy over cultural and public service sectors.

Second, across its FTAs, the EU reaffirms the applicability of WTO disciplines, particularly the GATS framework, by treating services supplied electronically as services for the purposes

[36] JSI on E-commerce, Communication from US, INF/ECOM/23, (2019). available at https://docs.wto.org/dol2fe/Pages/FE_Browse/FE_B_009.aspx?TopLevel=10785

of cross-border supply obligations. This principle is explicitly stated in the EU's agreements with Colombia, Peru and Ecuador, and CARIFORUM, where delivery by electronic means is treated as the provision of a service and exempted from customs duties, ensuring non-discrimination between digital and physical trade in services. Similarly, the EU-Canada Comprehensive Economic and Trade Agreement (CETA) and the EU-Singapore FTA reiterate that digital trade provisions are to be applied consistently with WTO rules to electronic commerce and emphasise regulatory co-operation to facilitate the development of e-commerce and, for that purpose. The EU recognised the benefits of having clear, transparent and predictable domestic regulatory frameworks, the importance of interoperability, innovation and competition, and the importance of facilitating the usage of e-commerce by SMEs.

Third, the EU consistently maintains public policy exceptions and regulatory autonomy within its digital trade chapters. Agreements such as EU-Japan[37] and EU-Vietnam explicitly preserve the right to regulate for legitimate public policy objectives, including the protection of public morals, health, safety, the environment, financial stability and cultural diversity. These provisions are modelled on WTO-style general exceptions under Article XIV of the GATS and Article XX of the GATT 1994, allowing measures that would otherwise breach trade obligations if necessary to pursue legitimate objectives and applied in a non-discriminatory manner. Additionally, across some of its FTAs, the EU clarifies that digital trade provisions do not require the privatisation of public undertakings, nor do they impose obligations regarding government procurement, subsidies or social security systems.[38]

Despite this common legal foundation, individual agreements differ in emphasis and depth. The EU-Chile Agreement narrowly defines scope and excludes audio-visual services to limit regulatory exposure, whereas the EU-Singapore FTA (Articles 8.57 and 8.59) adopts a flexible, co-operative approach, focusing on promoting e-commerce and avoiding unnecessary restrictions rather than imposing binding obligations. The EU-Mercosur and EU-Japan agreements add explicit exclusions and clauses ensuring that, in the event of inconsistency between the provisions of this section and the other provisions of the agreement, the latter shall prevail to the extent of the inconsistency. CETA (Article 16.5) places particular weight on regulatory predictability, transparency and SME participation while safeguarding the EU's right to exclude audio-visual subsidies and protect Canadian cultural industries (Article 7.7).

[37] Article 8.1, Section A, Chapter 8, EU-Japan FTA, Pg. 79.
[38] Article 107, Chapter 1, Title IV, EU-Columbia FTA, Pg. 31; Article 159, Chapter 1, Title III, EU-Central America FTA, Pg. 45; Article 7.1, Chapter 7, Section A, EU-Japan FTA, Pg. 26.

The EU-Vietnam FTA uniquely enumerates the right to regulate for environmental protection, public health, financial stability and social policy, explicitly linking digital trade to sustainable development goals.

Finally, the EU's position in the Joint Statement Initiative (JSI) on e-commerce extends these principles into the multilateral arena. The EU's JSI submissions emphasise technological neutrality, non-discrimination and transparency, while retaining the ability to define and implement cultural and audio-visual policies to maintain cultural diversity. The stabilised JSI text also mirrors EU FTA exclusions by omitting government procurement, services supplied in the exercise of governmental authority and government-held or -processed information, except where relevant to paperless trading, single-window data exchange, or open government data.[39]

In sum, the EU's digital trade architecture across its FTAs demonstrates a legally harmonised model: it promotes open and interoperable digital trade, anchored in WTO-consistent disciplines, while preserving regulatory sovereignty, cultural policy space, and the right to pursue legitimate public policy objectives.

The EU's digital trade architecture demonstrates a hybrid model – anchored in WTO principles, grounded in regulatory co-operation, and tempered by cultural and public policy exceptions. This approach ensures regulatory clarity and innovation while safeguarding sovereign regulatory autonomy and the integrity of international digital trade.

China

China's digital trade provisions in its free trade agreements (FTAs) generally adopt a soft-law and developmental approach, focusing on recognising the benefits of electronic commerce rather than establishing binding trade disciplines. Across its FTAs, China highlights the contribution of e-commerce to economic growth, opportunity creation and trade facilitation, while discouraging barriers to its use.

In the China-Singapore upgraded FTA, the applicability of the digital trade chapter is explicitly limited – where inconsistencies arise between the e-commerce chapter and other chapters of the agreement, other chapters shall prevail to the extent of the inconsistency. The agreement affirms the relevance of the WTO Agreement to electronic commerce measures and introduces

[39] JSI on E-commerce, Agreement on E-commerce, INF/ECOM/87, (2024), Pg. 4. available at https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/87.pdf&Open=True

a soft obligation to ensure that bilateral e-commerce trade is not more restrictive than comparable non-electronic trade.

Similar principles are reflected in the China-Cambodia FTA and the Regional Comprehensive Economic Partnership (RCEP), where the primary objective of the e-commerce chapter is framed as enhancing co-operation to build trust and confidence in e-commerce and promote its global expansion. Both agreements exclude government procurement (GP) and information held or processed by a party from their scope. Moreover, they, along with China's FTAs with Australia, Mauritius and Ecuador, agree in principle not to impose e-commerce restrictions that exceed those on traditional trade.

Under the RCEP, measures affecting the supply of services delivered electronically fall under existing obligations in Chapter 8 (Trade in Services) and Chapter 10 (Investment), as well as corresponding annexes outlining specific commitments, reservations and non-conforming measures, including exceptions that are applicable to those obligations, thereby ensuring consistency across sectors.

China's FTAs with Singapore and Korea reiterate that in case of conflict, non-digital trade provisions override digital trade chapters, reinforcing China's preference for a hierarchical and cautious integration of digital provisions within broader trade frameworks.

At the multilateral level, China's communication[40] to the WTO Work Programme on E-commerce acknowledges that digital trade reduces transaction costs, enhances integration into global value chains (GVCs), and benefits micro, small, and medium enterprises (MSMEs) by overcoming scale and distance barriers. China has emphasised inclusive participation in digital trade – especially for developing countries and least developed countries (LDCs) – and identified key discussion areas such as the following:

- Reducing digital trade barriers for MSMEs and underrepresented groups
- Sharing best practices for digital connectivity, inclusion and facilitation
- Building digital skills and capacity for trade integration

In its Joint Statement Initiative (JSI) on E-commerce, China underscored that WTO negotiations should leverage e-commerce's developmental potential, help developing members

[40] WTO General Council, Ideas to Reinvigorate the Work Programme on Electronic Commerce, WT/GC/W/855/Rev.2, (2023). available at: https://www.hketogeneva.gov.hk/doc/W855R2.pdf

integrate into GVCs, bridge the digital divide and promote inclusive participation in global digital trade.[41]

India

As of the publication of this report, India has incorporated digital trade chapters in two of its free trade agreements (FTAs): the India-UAE Comprehensive Economic Partnership Agreement (CEPA) and the India-UK FTA. Both chapters reflect a structure and scope closely aligned with the United States' Joint Statement Initiative (JSI) proposal and provisions found in various US FTAs.

Under Paragraph 1, both agreements establish a general scope clause applying to "measures adopted or maintained by the Parties that affect trade by electronic means."

In Paragraph 2, the India-UAE CEPA includes exceptions similar to those in the USMCA, excluding government procurement and information held or processed by or on behalf of a party, including measures related to its collection. The India-UK FTA, however, extends these exclusions further to cover both government procurement and audio-visual services.

A key distinction lies in Paragraph 3. The India-UAE CEPA adopts a broader and more integrative approach, explicitly linking measures affecting the electronic supply of goods and services to the obligations under the trade in goods, trade in services, and investment and trade chapters, along with any relevant annexes, exceptions, or limitations. In the event of any conflict, the provisions of these chapters prevail over the digital trade chapter.

By contrast, Paragraph 3 of the India-UK FTA specifies that measures affecting the electronic supply of services are subject to the relevant provisions of Chapter 8 (Trade in Services), Chapter 9 (Financial Services), and Chapter 11 (Telecommunications), including each party's schedules of specific commitments and exceptions.

Finally, Paragraph 4 of the India-UAE CEPA excludes the digital trade chapter from the FTA's dispute settlement mechanism, a provision is absent in the India-UK FTA. Unlike the USMCA or the US-Japan FTA, India's digital trade chapters do not incorporate the general exceptions of the GATS or GATT, nor do they include any security exception relating to the applicability of the chapter.

[41] JSI on E-commerce, Communication from China, INF/ECOM/19, (2019). available at: https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/19.pdf&Open=True

Since 1998, WTO members have regularly extended a moratorium on applying customs duties on electronic transmissions. The original ministerial declaration, which also saw the creation of the Work Programme on Electronic Commerce, contained a simple commitment which has come to be known as the e-commerce moratorium:[42]

"*Members will continue their current practice of not imposing customs duties on electronic transmissions*."

The World Trade Organization's ("WTO") 13th Ministerial Conference ("MC13") has extended the e-commerce customs duty moratorium for another two years, providing another short reprieve for digital trade companies from the imposition of tariffs.[43]

Various studies done on the impact of the moratorium give different numbers on the impact. For developed economies, the studies predict that the tariff loss could range between USD 20.45 million to USD 347 million. The overall tariff revenue loss will range from between 0.7 per cent to 2.7 per cent of total import duties and will range between 0.01 per cent to 0.04 per cent of total government revenue. For developing economies, the numbers lie between USD 613 million to USD 5,487 million, amounting to 0.8 per cent to 1.44 per cent of total import duties, and 0.064 per cent to 0.16 per cent of total government revenue.

Countries could make up for the lost revenue from VAT/GST applied domestically. In particular, there has been a significant increase in the import of new digital services, called 'Born Digital', across all income groups. Born Digital are services that cannot be delivered through physical carrier media, such as computing services, interactive online gaming services, or services provided through smartphone applications. These trade flows provide a new tax base for consumption taxes and can contribute to offsetting the fiscal implications arising from the dematerialisation of trade in digitizable goods. The growing imports of trade that is 'born digital' would generate new VAT/GST revenue, with the potential to offset foregone customs revenue. And most countries have an existing VAT/GST regime in place.

[42] World Trade Organization, *Joint Statement on Electronic Commerce*, https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?CatalogueIdList=4814,34856,20308&CurrentCatalogueIdIndex=1

[43] World Trade Organization, *Work Programme on Electronic Commerce: Ministerial Decision*, WT/MIN(24)/38, WT/L/1193, 2 March 2024, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/MIN24/38.pdf&Open=True

Collecting duties on electronic transmissions will be costly and technically complex. Currently, no customs infrastructures or processes exist to collect tariffs outside of traditional goods, or even correctly (and legally) attribute commercial value to electronic transmissions. Tariffs on electronic transmissions would impose an undue administrative burden on not just producers and consumers but also on tax authorities and carriers (electronic transmission service providers).[44]

The USA

The United States has consistently supported a permanent moratorium on customs duties on electronic transmissions, embedding this commitment as a core element across all its free trade agreements (FTAs). Each US FTA includes a dedicated article that permanently prohibits the imposition of customs duties on digital products transmitted electronically.

Under the United States-Mexico-Canada Agreement (USMCA), the parties explicitly agreed to maintain a permanent ban on customs duties related to the import or export of digital products transmitted electronically. Similar binding (hard) obligations appear across most US FTAs, typically expressed as follows:

"Neither Party may impose customs duties, fees, or other charges on or in connection with the importation or exportation of digital products by electronic transmission."

Although the provision uses the modal verb "may," it is interpreted as a mandatory obligation equivalent to "shall", reflecting a legal prohibition rather than discretion.

Most US FTAs, however, preserve the right to impose customs duties on imported physical carrier media (e.g., CDs, DVDs) containing digital products. In such cases, the customs value of the import is to be assessed solely on the value of the carrier medium, excluding the value of the digital content stored on it. This principle appears in agreements with Bahrain, Colombia, Morocco, Oman, Panama, Peru, and the Central America-Dominican Republic FTA (CAFTA-DR), which specify:

"The customs value of an imported carrier medium bearing a digital product of the other Party shall be based on the cost or value of the carrier medium alone, without regard to the cost or value of the digital product stored on the carrier medium."

[44] Hosuk-Lee Makiyama and Badri Narayanan, *The Economic Losses from Ending the WTO Moratorium on Electronic Transmissions*, ECIPE Policy Brief No. 3/2019 (European Centre for International Political Economy, August 2019), https://ecipe.org/wp-content/uploads/2019/08/ECI_19_PolicyBrief_3_2019_LY04.pdf

Some U.S. FTAs – notably those with Australia and Korea – go further, prohibiting customs duties irrespective of whether digital products are fixed on a carrier medium or transmitted electronically. Similarly, the US-Japan FTA prohibits customs duties on electronic transmissions and the content transmitted electronically.

While customs duties are restricted, many US FTAs permit internal taxation on the domestic sale of digital products, provided such taxes are applied in a manner consistent with the broader obligations of the agreement.

At the multilateral level, the United States has advanced this policy through the WTO Work Programme on Electronic Commerce (WPEC) and the Joint Statement Initiative (JSI). In multiple submissions and non-papers, the US has called for the permanent prohibition of customs duties on electronic transmissions on an MFN (most favoured nation) basis, emphasising that such duties could impede the free flow of digital content such as music, video, software and games. The US has argued that maintaining a complete ban ensures that creators, artists and entrepreneurs can participate in digital trade without artificial barriers. In its JSI communication, the US reiterated that binding trade rules should ensure that governments make permanent the practice of refraining from imposing customs duties on digital products.

Internal Taxation in US

The United States does not levy a value added tax (VAT) at either the federal or state level. Instead, sales and use taxes are administered independently by each of the 50 states and the District of Columbia[45], resulting in a decentralised and non-uniform framework for the taxation of goods and services, including those delivered digitally.

A significant shift in US state tax policy occurred following the US Supreme Court's decision in South Dakota v. Wayfair, Inc. (2018). The Court held that a seller with no physical presence in a state may nonetheless be required to collect and remit sales tax in that state if it conducts sufficient business there. This ruling effectively overturned the earlier Quill Corp. v. North Dakota (1992) physical presence standard and expanded states' taxing authority to include remote and online sellers.

The principle of "nexus" forms the constitutional and statutory basis for determining a state's authority to impose sales and use taxes. Nexus refers to the degree of business activity a seller

[45] Oldroyd Steve and Lipin Ilya, US-Sales Tax and Digital Goods, BDO Global, Issue 4-2019, (2019). available at: https://www.bdo.global/en-gb/microsites/tax-newsletters/indirect-tax-news/issue-4-2019/united-states-%C2%A0sales-tax-and-digital-goods

has within a state, which establishes a sufficient connection for tax purposes. Following the Wayfair decision, most states adopted economic nexus standards, typically requiring out-of-state or online sellers to collect and remit sales tax if they exceed specified thresholds — generally USD 100,000 in annual sales or 200 transactions with in-state consumers.

In practice, this means that remote sellers may now be obliged to collect state-level sales tax on the sale of tangible personal property, digital goods, and, in certain jurisdictions, services delivered electronically. While all US states impose sales tax on tangible computer-related property (e.g., hardware and peripherals), only a limited number of states extend this to computer-related or online services, such as streaming services, software-as-a-service (SaaS), and cloud computing.

This evolving approach demonstrates how state-level tax systems are adapting to digitalisation, even in the absence of a federal VAT, by redefining nexus and expanding the tax base to include digital trade and services.

The European Union (EU)

The European Union (EU) adopts a uniform approach across its FTAs by prohibiting customs duties on electronic transmissions. Agreements such as the EU-Chile (Article 19.7), EU-Singapore (Article 8.58), EU-Japan (Article 8.72), and EU-Vietnam (Article 8.51) FTAs explicitly state that "The Parties shall not impose customs duties on electronic transmissions." In its proposals to Korea, and in the EU-CARIFORUM (Article 119) and EU-UK (Article 203) FTAs, the EU classifies electronic transmissions as a supply of services, again prohibiting customs duties on such transmissions.

This interpretation is significant given the absence of an agreed definition of "electronic transmissions" and the uncertainty over the scope of the WTO moratorium.[46] Treating e-transmissions as services potentially extends GATS commitments to such flows and raises questions as to whether the moratorium covers both the means of transmission and the transmitted content.[47] Hence, while the EU's approach establishes a clear moratorium obligation, it does not resolve these definitional and jurisdictional ambiguities.

Later FTAs, including those with Mercosur (Article 44), Canada (Article 16.3), and New Zealand (Article 12.6), reaffirm a binding prohibition on customs duties but permit the

[46] https://www.iisd.org/articles/policy-analysis/wto-moratorium-customs-duties-electronic-transmission
[47] https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/03/understanding-the-scope-definition-and-impact-of-the-wto-e-commerce-moratorium-policy-brief_555f8509/4329569a-en.pdf

imposition of internal taxes or fees, provided they are consistent with the broader principles of the agreement. Overall, the EU framework reflects a commitment to facilitate cross-border digital trade through a permanent moratorium on customs duties, while preserving limited regulatory flexibility in domestic taxation.

Internal Taxation in the EU

Since July 1, 2021, the European Union (EU) has reformed its VAT regime for cross-border business-to-consumer (B2C) e-commerce. The previous member state-specific distance sales thresholds were abolished and replaced by a single EU-wide threshold of EUR 10,000. Below this threshold, supplies of telecommunications, broadcasting, and electronic (TBE) services and intra-EU distance sales of goods remain subject to VAT in the supplier's member state of establishment. The updated rules[48] apply to the following

- Distance sales of goods within the EU by suppliers or deemed suppliers (including electronic interfaces)
- Domestic sales of goods by deemed suppliers
- Supply of services by EU and non-EU sellers to EU consumers
- Distance sales of imported goods (excluding excise goods) from third territories or countries.

To simplify compliance, online sellers and marketplaces can register under a one-stop shop (OSS) system in a single EU member state for VAT declaration and payment across the Union, reducing administrative burdens by up to 95 per cent.[49]

Separately, about half of European OECD countries have introduced or proposed a digital services tax (DST) to tax revenues from digital activities. Countries that have implemented a DST include Austria, Denmark, France, Hungary, Italy, Poland, Portugal, Spain, Switzerland, Turkey, and the United Kingdom. Others – such as Belgium, the Czech Republic, Latvia, Norway, Slovakia, and Slovenia – have proposed or announced intentions to do so. These taxes vary in scope and tax base: Austria and Hungary limit taxation to online advertising, Denmark applies it to streaming services and France adopts a broader base, taxing revenues from digital interfaces, targeted advertising and data transmission.

[48] European Commission, VAT E-commerce – One Stop Shop, Pg. 2. available at https://vat-one-stop-shop.ec.europa.eu/index_en
[49] Id. at Pg. 3

The United States has criticised these unilateral DSTs as discriminatory toward US tech firms and has responded with threats of retaliatory tariffs, urging the withdrawal of such measures.

China

China's stance on the moratorium on customs duties on electronic transmissions aligns closely with that of India, characterised by a conditional commitment rather than a permanent prohibition. While China has agreed to maintain the current practice of not imposing customs duties on electronic transmissions, it expressly reserves the right to revise this approach in line with future WTO Ministerial decisions under the Work Programme on Electronic Commerce.

In both the upgraded China-New Zealand Free Trade Agreement and the Regional Comprehensive Economic Partnership (RCEP), China retains the right to impose taxes, fees or other charges on electronic transmissions, provided such measures are consistent with the terms of the respective agreements. Under the RCEP, parties are required to maintain their existing practice of not imposing customs duties on electronic transmissions, but the obligation is not permanent and remains subject to modification based on future WTO outcomes.

In its communications to the Joint Statement Initiative (JSI) on e-commerce and the WTO Work Programme on E-commerce, China reaffirmed its intention to continue the moratorium only until the next WTO Ministerial Conference, thereby preserving flexibility to alter its policy in the future.[50]

Internal Taxation in China

China enacted its value-added tax (VAT) law on December 25, 2024, which will take effect on January 1, 2026. The law retains the existing three-tier tax rate structure of 13 per cent, 9 per cent and 6 per cent, while introducing significant modernisations and international harmonisation measures.

Article 3 of the VAT law defines the scope of VAT liability, stipulating that entities and individuals (including sole proprietorships) engaged in the sale of goods, services, intangible assets or real estate within the People's Republic of China, or the importation of goods are VAT taxpayers required to remit tax in accordance with the law.

A key reform under the new framework is the clarification of the place of taxation for services and intangible assets. The law specifies that, except for transactions involving the sale or lease

[50] Supra note 43

of immovable property, the transfer of rights to natural resources and the sale of financial products, VAT liability arises where the consumption of services or intangible assets occurs domestically, or where the seller is a domestic entity or individual. This represents a shift from the previous business tax regime, which relied on criteria such as whether the service was provided within the territory or whether the seller or buyer was located domestically.

This transition to a "domestic consumption" principle aligns China's VAT system more closely with international best practices, particularly those applied in OECD jurisdictions, and provides clearer rules for taxing cross-border digital services and intangible transactions.[51]

India

India maintains a principled opposition to the extension of the WTO moratorium on customs duties on electronic transmissions, a position that contrasts with that of most developed economies. At the 13th WTO Ministerial Conference (MC13) on February 29, 2024, during the Working Session on the Work Programme on E-Commerce, India reiterated that with the ongoing digital transformation – driven by additive manufacturing, 3D printing, data analytics, artificial intelligence, and the Internet of Things – there is an urgent need to reassess the developmental implications of the moratorium, particularly for developing countries and least-developed countries (LDCs).

Under the India-UAE Comprehensive Economic Partnership Agreement (CEPA), India agreed to maintain its current practice of not imposing customs duties on electronic transmissions. The agreement, similar in structure to certain US FTA provisions, allows both parties to impose internal taxes, fees or other charges on digitally transmitted content, provided such measures are consistent with the broader obligations of the agreement.[52] However, these commitments are expressly contingent upon the outcomes of future WTO decisions under the Work Programme on Electronic Commerce.

Notably, the India-UK Free Trade Agreement (FTA) does not include an equivalent provision, indicating India's cautious and flexible stance on binding commitments related to the taxation of electronic transmissions.

[51] EY, China Officially enacts VAT law, (2025), Pg. 3. available at https://www.ey.com/en_gl/technical/tax-alerts/china-officially-enacts-vat-law-ushering-in-a-new-era-of-tax-governance
[52] Article 9.15, chapter 9 of India-UAE FTA.

Internal Taxation in India

In India, digital services delivered via the internet or an electronic network are classified as online information database access and retrieval (OIDAR) services under Section 2(17) of the IGST Act 2017 and are taxed at 18 per cent. Effective October 1, 2023, India withdrew the GST exemption previously available to foreign OIDAR service providers, thereby extending the 18 per cent IGST to all such supplies, including those to individuals and government entities.

Under Section 52(1) of the CGST Act, e-commerce operators must collect tax at source (TCS) at 1 per cent (0.5 per cent CGST + 0.5 per cent SGST) on the net value of taxable supplies facilitated through their platforms.[53]

In April 2020, India expanded its equalisation levy to cover e-commerce supplies of goods and services by non-resident operators at 2 per cent, applicable on receipts up to July 31, 2024. This measure aimed to address taxation of digital commerce by offshore entities. Subsequently, the 2024 Finance Bill abolished the 2 per cent levy on e-commerce sales, and the 2025 Finance Bill removed the 6 per cent levy on online advertising revenues – signalling a shift towards harmonising domestic indirect taxation of digital services under the GST framework.[54]

Personal Data Protection

As the digital economy continues to expand, personal data protection has emerged as a highly contested issue in global trade policy. Both governments and private corporations collect vast amounts of personal data, raising concerns over privacy, security and regulatory oversight.

With the increased prominence of digital trade, the risks associated with cyberattacks and data breaches have also intensified. In India, where digital literacy remains low and digital infrastructure faces persistent security challenges – the incidence of data leaks, financial frauds (UPI and card-related frauds), and identity theft have become increasingly common, the threat of cybercrime, including tactics like digital arrests and financial scams, underscores the need for robust data protection frameworks.

[53] CBEC, GST Sectoral Series-Electronic Commerce. available at: https://gstcouncil.gov.in/sites/default/files/2024-02/faq-e-commerc.pdf

[54] Asquith Richard, India scraps 2% equalisation levy on foreign digital service, VAT Calc, (2024). available at: https://www.vatcalc.com/india/india-2-equalisation-levy-extension-to-e-commerce-sellers-and-facilitating-marketplaces-apr-2020/

Given these challenges, it is essential to examine how different regions approach personal data protection within their free trade agreements (FTAs). Understanding the divergent regulatory models, whether market-driven, state-controlled or consumer-centric, offers insights into how nations balance economic interests with data privacy concerns in the evolving digital trade landscape.

The USA

The United States does not have a comprehensive federal data protection law, though proposals such as the American Privacy Rights Act have been debated in Congress. Federal initiatives currently focus on addressing national security and data brokerage risks rather than creating an omnibus privacy regime. A February 2024 Executive Order authorises restrictions on data brokerage activities and transactions involving "foreign adversaries" when deemed to pose national security risks, supported by a Justice Department Advanced Notice of Proposed Rulemaking (ANPRM). Related legislative efforts include the Protecting Americans' Data from Foreign Surveillance Act of 2023 and the Protecting Americans' Data from Foreign Adversaries Act (H.R. 7520).

The US has incorporated personal information protection provisions only in the USMCA and US-Japan FTA. Both agreements require parties to "adopt or maintain a legal framework" to protect the personal information of digital trade users, while allowing flexibility in domestic approaches. Under Article 19.8 of the USMCA, parties commit to principles such as limitation on collection, use limitation, purpose specification, transparency and accountability, and to ensuring that restrictions on cross-border data flows are necessary and proportionate. Under Article 19.8(4), the parties accept a "soft obligation" to adopt non-discriminatory practices that protect digital trade users from personal information violations. The United States additionally commits to publishing information about its protection framework – explaining both how individuals can seek remedies and how enterprises can meet legal requirements.

In its FTA with Japan, US agreed that parties may take different legal approaches to protecting personal information. Further, both the USMCA and US-Japan FTA encourage the development of interoperability and compatibility mechanisms between their privacy regimes. USMCA recognised the APEC Cross-Border Privacy Rules (CBPR) system as a valid framework for cross-border data transfers while ensuring privacy protection. In addition, parties under the USMCA committed to taking into account the principles and guidelines of relevant international bodies, such as the APEC Privacy Framework and the OECD

recommendation of the Council concerning guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013) while developing the personal information protection framework.

In the US proposal to the WTO Joint Statement Initiative (JSI) on E-Commerce,[55] provisions on personal information protection mirror those in the US-Japan FTA, including a hard obligation to maintain a protective legal framework and transparency commitments. The proposal preserves flexibility for parties to meet these obligations through comprehensive privacy or data protection laws, sectoral specific laws and laws that enforce voluntary commitments by enterprises. While it reaffirms that parties may choose different legal approaches, it also encourages interoperability and proportionate restrictions on cross-border data transfers. Finally, as in the USMCA and US-Japan FTA, the proposal requires parties to publish information on their personal information protection regulations, including how individuals can pursue remedies and how enterprises can comply with legal requirements.

US Personal Data Protection Laws

The United States does not have a comprehensive federal data privacy law but instead operates through a fragmented framework consisting of sector-specific statutes, executive action and – state-level initiatives. Two key federal initiatives have recently sought to establish broader protection standards.

The first bill is the American Data Privacy and Protection Act (ADPPA)[56], which – though pending Congressional approval – would create uniform requirements for how companies collect, process and transfer personal data. It mandates that entities limit data use to what is reasonably necessary to deliver requested services, grants consumers rights to access, correct and delete personal data, and provides an opt-out mechanism for targeted advertising.

The second is the Executive Order on Protecting Americans' Sensitive Personal Data[57] (E.O. 14117), implemented through a Department of Justice final rule on December 27, 2024. The rule authorises the Attorney General to restrict or prohibit large-scale transfers of sensitive data

[55] Supra note 37
[56] H.R.8152 – American Data Privacy and Protection Act, (2022). available at https://www.congress.gov/bill/117th-congress/house-bill/8152#:~:text=/30/2022)-,American%20Data%20Privacy%20and%20Protection%20Act,based%20on%20specified%20protected%20characteristics.
[57] National Security Division, Provisions Pertaining to Preventing Access to US Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, Department of Justice, Doc. No. NSD 104, (2024). available at: https://www.justice.gov/nsd/media/1382521/dl

– including genomic, biometric, financial, geolocation and personal health information – to "countries of concern." It establishes the Bulk Sensitive Data Regulatory Program, which identifies restricted transactions and entities, defines compliance and reporting obligations, and introduces a licensing mechanism for otherwise prohibited transactions. This framework primarily addresses national security and data sovereignty concerns rather than consumer privacy.

Alongside these developments, several longstanding federal laws provide sectoral protection:

- The Health Insurance Portability and Accountability Act (HIPAA) safeguards health data privacy and security.
- The Gramm-Leach-Bliley Act (GLBA) mandates confidentiality and disclosure practices in financial institutions.
- The Children's Online Privacy Protection Act (COPPA) governs data collection from children under 13.
- The E-Government Act of 2002 requires federal agencies to conduct privacy impact assessments for systems managing personal information.

At the state level, privacy governance expanded significantly following California's Consumer Privacy Act (CCPA) in 2019, which created a compliance model for businesses processing personal data of state residents. Since then, twenty US states have enacted comprehensive data privacy laws, filling the regulatory vacuum left by the absence of a national framework.[58]

Complementing these are laws and policies identified by the Digital Trade Integration Project as regulatory restrictions on digital trade, given their imposition of compliance, security, and access obligations on private entities. These include the following:

- Directive No. 3340-049a, granting US Customs and Border Protection authority to inspect electronic devices, even when containing sensitive data
- Network Security Agreements (NSAs), which compel foreign telecommunications providers to permit government access to communications data without judicial authorisation
- Sectoral mandates such as HIPAA and privacy impact assessments under the E-Government Act.

[58] Pittman F. Paul, Anderson Hope, Hafiz M. Abdul, US Data Privacy Guide, White & Case, (2025). available at: https://www.whitecase.com/insight-our-thinking/us-data-privacy-guide

In addition, the Consumer Online Privacy Rights Act (COPRA) bill, introduced in 2021, sought to provide comprehensive consumer rights and corporate obligations regarding data handling. It requires transparency through published privacy policies, enables individuals to access, correct, delete and export personal data, and obliges firms to maintain data security practices and designate privacy and data protection officers.[59]

Overall, the US framework remains fragmented and compliance-driven, prioritising oversight, security and national interest considerations over regulatory simplicity or innovation enablement. As such, these measures constitute restrictive or supervisory instruments rather than enabling frameworks for digital trade or cross-border data flows.

The European Union (EU)

The European Union (EU) consistently integrates the protection of personal data and privacy as a fundamental right in its free trade agreements (FTAs), framing it as essential to consumer trust, digital economy development and international trade facilitation. Across its agreements, this commitment manifests through both hard and soft obligations, granting flexibility while maintaining alignment with international standards.

The EU-Mercosur Agreement (Article 54(f)(ii)) highlights privacy and confidentiality of personal data and individual records but adopts a flexible, non-binding formulation. Similarly, the EU-New Zealand FTA (Article 12.5) recognises privacy as a fundamental right and underscores that high protection standards enhance consumer trust while allowing parties discretion to adopt appropriate measures.

By contrast, several FTAs impose hard obligations through enforceable provisions. The EU-South Korea FTA (Article 6) recognises privacy as a fundamental right and permits each party to "adopt and maintain safeguards" deemed necessary to ensure personal data protection. The EU-Singapore FTA (Articles 8.57, 8.62(e)(ii)) links electronic commerce development to compliance with international data protection standards and explicitly preserves parties' rights to enforce privacy laws that are not inconsistent with the provisions of this Chapter, including those relating to the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts" even where they may limit trade. The EU-Canada FTA (Article 16.6) embeds co-operation on e-commerce, including the protection of personal information and prevention of

[59] S.3195 Consumer Online Privacy Rights Act, (2022). available at https://www.congress.gov/bill/117th-congress/senate-bill/3195

deceptive practices. Likewise, the EU-Japan FTA emphasises co-operation on consumer protection in electronic commerce, including safeguarding personal data. Article 8.78 affirms "*the importance of adopting or maintaining measures to protect the personal data of electronic commerce users.*" and the EU-Ukraine FTA (Article 139) mandate adherence to the highest international data protection standards to preserve user confidence. The EU-UK Trade and Co-operation Agreement (Article 202) explicitly affirms personal data protection as a right integral to building trust in digital economies. It declares that "*individuals have a right to the protection of personal data and privacy".*

Collectively, these provisions form a coherent and rights-based digital trade framework, where privacy protection is elevated to a trade principle. The EU's approach provides regulatory flexibility – permitting each party to define implementation methods – while ensuring that domestic measures maintain compatibility with international norms.

The JSI (Joint Statement Initiative) draft on e-commerce, while not recognising privacy as a fundamental right, mirrors many EU principles. It obliges members to adopt and maintain non-discriminatory legal frameworks for personal data protection, encourages compatibility among different regimes of data protection and requires publication of information on national privacy protection. It further encourages parties to consider international standards in developing domestic frameworks.

According to the Digital Trade Integration Project (Annexure 1), EU policies operate simultaneously as regulatory restrictions and enabling measures for digital trade. The General Data Protection Regulation (GDPR) exemplifies this duality.

As a regulatory restriction, the GDPR imposes stringent compliance obligations on organisations, including the appointment of data protection officers (DPOs) and the conduct of data protection impact assessments (DPIAs) for activities involving large-scale monitoring or high-risk data processing. These measures heighten compliance costs and administrative burdens for firms engaging in digital trade.

Conversely, the GDPR also functions as an enabling measure by establishing a harmonised and extraterritorial framework for personal data protection, ensuring a consistent standard across all EU member states. This harmonisation facilitates the free flow of personal data within the single market, enhances interoperability with external regimes and strengthens trust and legal certainty in cross-border digital transactions.

Complementary legislation such as Directive (EU) 2016/680 governing personal data processing in criminal justice contexts further supports this framework by balancing security imperatives with individual privacy rights, thereby promoting regulatory coherence and inter-state co-operation.

In essence, the EU's trade policy operationalises its internal legal philosophy – that data protection is a fundamental right under Article 8 of the EU Charter of Fundamental Rights – into external agreements. This rights-based, high-standard model contrasts with the more flexible and market-driven approaches adopted by the United States and other trading partners, positioning the EU as the global standard-setter for data governance in trade.

China

In its FTAs with Mauritius and Australia, China commits to adopting or maintaining measures it deems appropriate and necessary to protect the personal information of users engaged in electronic commerce. In contrast, its FTAs with Korea, Singapore, Cambodia, New Zealand, and the RCEP Agreement impose a hard obligation to maintain a legal framework ensuring such protection. China's submission to the Joint Statement Initiative (JSI) on E-Commerce similarly proposes that all members adopt measures considered appropriate to safeguard personal data, while also emphasising that, in developing domestic legal frameworks, international standards and guidelines established by relevant organisations should be taken into account.

Further, under the RCEP and its upgraded FTA with New Zealand, China has agreed to publish information on its personal information protection framework, including available remedies for individuals and compliance mechanisms for businesses, and to encourage enterprises to disclose their privacy policies publicly.

According to the Digital Trade Integration Project (Annexure 1), most Chinese digital trade policies function as regulatory restrictions, with only one acting as an enabling measure. Regulatory instruments such as the Cybersecurity Law (2017), Data Security Law (2021), and State Security and Counterespionage Laws (1993, 2014) impose extensive monitoring, data localisation and disclosure obligations, requiring internet service providers (ISPs) and network operators to provide user data to authorities and to implement strict internal security mechanisms. Complementary measures such as the Provisions for Network Security Inspections (2018) and State Council Decree No. 292 (2000) further empower law enforcement

agencies to access, inspect and retain user information without judicial oversight, creating a significant compliance burden for private entities.

Conversely, the Personal Information Protection Law (PIPL) (2021) represents a major enabling measure, establishing a comprehensive and rules-based framework for personal data governance. It codifies data subject rights, defines cross-border data transfer mechanisms and introduces territorial applicability provisions (Article 53), thereby enhancing transparency and predictability for firms operating in China's digital economy.

Overall, while China's digital trade regime is predominantly security-oriented and compliance-heavy; the PIPL marks an important evolution toward a structured, trust-based model of personal data protection, balancing state control with the need for legal certainty in cross-border digital trade.

India

In its FTA with the United Arab Emirates (UAE), India has undertaken a soft obligation to adopt or maintain a legal framework that ensures the protection of personal data belonging to users of digital trade. Mirroring provisions found in the US-Japan Digital Trade Agreement, India's commitment allows flexibility in compliance – parties may fulfil the obligation through the adoption of comprehensive privacy laws or sector-specific regulations addressing personal data protection. Similarly, consistent with the USMCA framework, India has agreed to take into account the principles and guidelines developed by relevant international organisations when framing its domestic personal data protection laws.

India's FTAs also include commitments to transparency and co-operation. Under the India-UAE FTA, both parties have agreed to publish information on their respective data protection regimes, including available remedy mechanisms for individuals and compliance procedures for businesses, and to co-operate, where possible, on the protection of personal data transferred between the two countries. Moreover, in its FTA with the United Kingdom, India has agreed to establish a review mechanism to facilitate consultations on the adoption and maintenance of personal data protection frameworks, while explicitly excluding domestic laws affecting data protection from the scope of commitments.

Domestically, India has established a comprehensive legislative framework through the Digital Personal Data Protection (DPDP) Act, 2025, (notified on November 14, 2025) marking the country's first dedicated data privacy law. The Act governs the processing of digital personal

data, whether collected online or offline and subsequently digitised, and extends to extraterritorial processing connected with goods or services offered in India. It recognises an individual's right to protect their personal data and mandates that processing occur only for lawful purposes and with consent. To operationalise the Act, the Ministry of Electronics and Information Technology (MeitY) has drafted the Digital Personal Data Protection Rules, 2025, which establish a detailed framework for implementation, compliance and enforcement, including provisions on consent management, data fiduciaries and cross-border data transfer mechanisms.

Through this evolving regime, India seeks to balance its growing participation in cross-border digital trade with the need for data sovereignty and user privacy. While its international commitments reflect a co-operative and flexible approach, the DPDP Act signifies a shift toward a structured, rights-based framework for personal data protection, aligning India's digital trade policy with emerging global privacy norms.

According to the 'Digital Trade Integration Project' (ANNEXURE 1), several Indian policies function primarily as regulatory restrictions on digital trade, as they impose extensive obligations on private entities to comply with governmental directives, security mandates and data surveillance requirements.

- The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, empower the government to block public access to digital information transmitted or hosted on any computer resource through a designated officer, acting upon requests from authorised agencies or courts.
- The Indian Telegraph Act, 1885, and the corresponding Telegraph Rules confer broad powers on the government to intercept, disclose or possess communications, including through modern digital and telecommunication systems. These provisions permit interception without mandatory judicial oversight in all cases.
- The licence agreements for the provision of internet and telecommunication services require internet service providers (ISPs) and telecom operators to maintain extensive subscriber data, including call records and location information, and to grant law enforcement access for monitoring and investigative purposes.
- Under Section 69 of the Information Technology Act, 2000, the government is authorised to intercept, monitor or decrypt information for reasons of sovereignty,

public order or national security, and intermediaries are legally obligated to assist in such decryption processes.

- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, impose strict compliance duties on significant social media intermediaries, including the appointment of a chief compliance officer personally liable for ensuring adherence to government regulations on data, content moderation and platform accountability.

Collectively, these measures establish a highly securitised and compliance-intensive digital environment, prioritising national security, public order and state oversight over operational flexibility. While such frameworks are intended to protect public and national interests, they impose substantial compliance costs on digital service providers and restrict cross-border data flows.

India's sector-specific regulatory landscape – spanning telecommunications, banking and corporate data governance – remains fragmented in the absence of a comprehensive, unified data protection regime. Consequently, none of these measures explicitly function as enabling mechanisms for digital trade, as they neither facilitate innovation nor streamline regulatory compliance across sectors.

Cross-border Data Transfer

As digital trade expands, the movement of data across borders has become a critical issue, shaping the regulatory frameworks of major economies. Cross-border data transfers enable global commerce, supporting industries such as cloud computing, financial services and e-payments. However, concerns over data security, privacy, regulatory access and economic sovereignty have led governments to adopt varying degrees of data localisation measures ranging from mild storage requirements to strict flow prohibitions.

The rise in data localisation regulations has created significant trade-offs. While governments argue that restricting data transfers enhances privacy protection, regulatory oversight and national security, businesses contend that such measures increase compliance costs, reduce efficiency and stifle competition. International trade agreements now frequently address data localisation, with some agreements promoting unrestricted data flows while others permit regulatory exceptions.

Given the fragmented global approach, cross-border data governance remains one of the most debated issues in digital trade negotiations. Understanding how different economies balance data sovereignty with economic openness is essential to assessing the future of digital trade and global data flows.

The USA

Most US Free Trade Agreements (FTAs) do not contain explicit provisions on cross-border data transfers, and some merely recognise their importance as essential for a dynamic digital economy. The US-Korea FTA establishes a soft obligation, requiring parties to refrain from imposing unnecessary barriers to electronic information flows across borders. In contrast, the US-Mexico-Canada Agreement (USMCA) and the US-Japan Digital Trade Agreement introduce hard obligations, mandating that parties allow cross-border transfers of information, including personal data, when related to the business operations of a covered person. These obligations, however, are qualified: parties may adopt or maintain restrictions on data transfers to achieve legitimate public policy objectives, provided such measures are non-discriminatory, not a disguised restriction on trade and no more restrictive than necessary to achieve their intended purpose.

In its 2019 communication to the WTO, the US advocated for digital trade rules that promote the free flow of data across borders while maintaining reasonable safeguards for consumer data protection. Its proposals emphasised:

- Unrestricted cross-border data transfers, allowing data movement without arbitrary or discriminatory restrictions
- A ban on forced data localisation, preventing mandates for local digital infrastructure that increase costs and reduce efficiency
- Prohibitions on web blocking, ensuring open internet access by preventing arbitrary content filtering or blocking by governments.

The US draft proposal on e-commerce at the WTO mirrored the USMCA and US-Japan provisions, reaffirming a hard obligation to permit cross-border data transfers for business purposes, subject to narrowly tailored public policy exceptions.

However, in late 2023, the US Trade Representative (USTR) withdrew support for key digital trade disciplines – specifically those on cross-border data flows, data localisation and source code – in the Joint Statement Initiative (JSI) on E-commerce and Indo-Pacific Economic

Framework (IPEF) negotiations. USTR Katherine Tai cited the need to preserve domestic regulatory space amid evolving debates on privacy, competition and the regulation of large technology firms ("Big Tech"). This shift marked a significant recalibration of US digital trade policy, prioritising domestic policy autonomy over trade liberalisation commitments. The decision was met with criticism from US legislators and industry stakeholders, who warned that it could diminish US influence in shaping global digital trade norms and strengthen China's role in setting international standards.

United States Cross-Border Data Flow Regulation

The United States Executive Order (EO) 14117, titled "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern," prohibits and restricts specific data transactions involving designated countries or persons where such access may threaten US national security. While imposing these restrictions, the US government simultaneously reaffirms its commitment to open, global, interoperable, reliable, and secure cross-border data flows, recognising their importance to maintaining consumer, economic, scientific, and trade relations.

To operationalise this framework, the Department of Justice (DoJ) issued a final rule implementing EO 14117. The rule[60]identifies classes of prohibited and restricted transactions, designates countries of concern and categories of covered persons whose access to bulk sensitive personal data or government-related data is restricted, establishes a licensing mechanism to authorise, modify, or rescind otherwise prohibited transactions, provides for the issuance of advisory opinions and mandates recordkeeping and reporting to support investigative, enforcement and regulatory oversight.

In parallel, the EU-US Data Privacy Framework (EU-US DPF), the UK Extension to the EU-US DPF, and the Swiss-US DPF were introduced to facilitate transatlantic data flows by providing legally recognised mechanisms for the transfer of personal data from the EU/EEA, the United Kingdom (including Gibraltar) and Switzerland to the United States. These frameworks align with the respective jurisdictions' data protection laws and aim to ensure adequate safeguards for personal data.[61] The US Department of Commerce administers the

[60] Federal Register, National Security Division, Department of Justice, Final Rule – Preventing Access to US Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, (2025), Pg. 4. available at https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern

[61] Data Privacy Framework, Data Privacy Framework Overview. available at: https://www.dataprivacyframework.gov/Program-Overview

DPF programme, maintaining a public website that enables eligible US organisations to self-certify their compliance, thereby legitimising cross-border personal data transfers consistent with EU, UK, and Swiss privacy requirements.[62]

The United States adopts a dual approach to cross-border data governance, combining enabling measures that promote open digital trade with regulatory restrictions that safeguard national security and sensitive information.

Under the Digital Trade Integration Project (Annexure 1), the US facilitates data flows through binding international commitments such as the Agreement between the United States and Japan Concerning Digital Trade (2019) and the United States-Mexico-Canada Agreement (USMCA, 2020). Articles 11 and 19.11 of these agreements guarantee the free flow of data across borders, reduce barriers to digital trade and promote an integrated digital economy.

In contrast, several domestic regulatory frameworks impose targeted restrictions to protect sensitive government and defence data. The Code of Federal Regulations (2015, amended 2021) requires cloud service providers working with the Department of Defence (DoD) to store sensitive data within the United States unless explicitly authorised otherwise. Similarly, the Federal Risk and Authorization Management Program (FedRAMP) Control-Specific Contract Clauses (2017) permit federal agencies to specify contractual requirements regarding data storage locations. Furthermore, Network Security Agreements (1999) empower Team Telecom to mandate local data storage for telecommunications providers or mergers to ensure data accessibility for national security purposes.

Collectively, these measures illustrate the US model of maintaining openness in global digital trade while embedding regulatory safeguards for national and defence-related data, achieving a balance between trade facilitation and sovereign data protection.

The European Union (EU)

The European Union's Free Trade Agreements (FTAs) consistently prioritise cross-border data flows and personal data protection as central components of digital trade. Across its

[62] US Department of Commerce, Data Privacy Framework Programme Launches New Website Enabling US Companies to Participate in Cross-Border Data Transfers, (2023). available at: https://www.commerce.gov/news/press-releases/2023/07/data-privacy-framework-program-launches-new-website-enabling-us

agreements, the EU aims to ensure the unrestricted flow of data across borders while safeguarding public policy interests such as privacy, security and environmental protection.

Recent FTAs, including those with Chile (Chapter II, Article 19.4), New Zealand (Article 12.4), South Korea (Annex 7-D), the United Kingdom (Chapter II, Article 201) and the proposed EU-South Korea Digital Trade Agreement (Title II, Chapter I, Article 5), explicitly prohibit restrictions on cross-border data flows that could impede digital trade. For instance, the EU-Chile FTA provides that data transfers "shall not be restricted between the Parties" through requirements for local storage or processing, a principle reiterated in the EU-New Zealand FTA, which further bars mandates for data localisation, the use of domestic computing facilities or other measures limiting transfers.

In contrast, certain agreements such as the EU-Canada[63] and EU-Singapore[64] FTAs do not include a stand-alone article on data transfer but permit the transfer of information by financial service suppliers "in electronic or other form" for ordinary business data processing. These provisions are accompanied by general exceptions allowing measures to protect public security, morals, health or the environment, provided such measures are non-discriminatory and not disguised restrictions on digital trade.

In articles in other agreements, such as Article 8.45 of the EU-Viet Nam FTA, impose transitional obligations, requiring the parties to allow financial service suppliers to transfer data across borders within two years of the FTA's entry into force. Many EU FTAs also provide review mechanisms, typically within three years, enabling parties to assess and update data flow provisions in response to evolving technology and regulation. This is evident in the EU-South Korea, EU-UAE, EU-UK, and EU-Japan agreements, the EU-Japan requiring a reassessment of the inclusion of cross-border data flow provisions within three years of implementation.

The EU-New Zealand FTA (Article 12.4) represents a more advanced model by creating explicit and enforceable prohibitions on restrictions to cross-border data flows, thereby establishing binding obligations against data localisation.

[63] Article 13.15, Chapter 13, Pg. 101. available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2017:011:FULL
[64] Article 8.54, Sub-Section 6, Section E, Chapter 8, EU-Singapore FTA, Pg. 71. available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2020:186:FULL

In its submission to the WTO Work Programme on Electronic Commerce[65] (WPEC), the EU advocated embedding similar principles into bilateral and multilateral trade disciplines in a technologically neutral manner. It proposed that governments should not prevent service suppliers or their customers from transferring data electronically across borders or from accessing publicly available or self-stored information in other jurisdictions. Notably, however, the Joint Statement Initiative (JSI) stabilised draft does not currently include provisions on cross-border data transfers.

According to the Digital Trade Integration Project (ANNEXURE 1), the European Union's digital regulatory framework employs a dual approach that combines regulatory restrictions to safeguard data privacy with enabling measures to facilitate cross-border data flows under specific agreements.

Regulatory Restrictions

The General Data Protection Regulation (GDPR) (2018) forms the cornerstone of the EU's data protection regime. It applies extraterritorially to companies offering goods or services to, or monitoring the behaviour of, individuals within the EU (Article 3). Under Chapter 5, transfers of personal data outside the European Economic Area (EEA) are permitted only when one of the following conditions is met:

- The destination country ensures an adequate level of data protection, as determined by the European Commission.
- Appropriate safeguards, such as standard contractual clauses or binding corporate rules, are in place.
- The transfer is based on the explicit consent of the data subject or is necessary for contractual performance.

The EU has issued adequacy decisions for several jurisdictions, including Japan, New Zealand, and South Korea, while the EU-US Data Privacy Framework (2023) establishes a self-certification mechanism enabling US companies to lawfully receive personal data from the EU.

Enabling Measures

[65] WPEC (WTO), Communication from EU and US, S/C/W/338, (2011), Pg. 2. available at https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=Q:/S/C/W338.pdf&Open=True

The EU-UK Trade and Co-operation Agreement (2021) complements the GDPR framework by ensuring the free flow of data between the EU and the UK under Article 201, thereby preserving digital trade continuity post-Brexit.

This dual model reflects the EU's overarching policy objective: to uphold high data protection standards through stringent regulatory safeguards while enabling cross-border digital trade via mutually recognised international arrangements.

China

China's approach to cross-border data transfers reflects a cautious and security-oriented regulatory philosophy, balancing trade facilitation with strong state control over data flows. While most of China's Free Trade Agreements (FTAs) do not contain explicit provisions on cross-border data transfers, the country has taken incremental steps towards regulated openness within multilateral and bilateral frameworks.

Under the Regional Comprehensive Economic Partnership (RCEP), China has undertaken a hard obligation prohibiting parties from preventing cross-border transfers of information by electronic means where such transfers are conducted in the course of business by a covered person. However, the agreement allows parties to adopt or maintain restrictive measures when necessary to achieve legitimate public policy objectives, provided these measures are not applied in an arbitrary or discriminatory manner or serve as disguised trade restrictions. The RCEP further recognises the right of parties to restrict cross-border data flows to protect essential security interests, insulating such measures from external challenge.

In the China-Ecuador FTA, China acknowledges the role of digitalisation and data usage in fostering economic growth and commits to creating an enabling environment for cross-border information transfers and promoting data-driven innovation in support of its digital economy.[66]

In its submission to the Joint Statement Initiative (JSI) on E-Commerce at the World Trade Organization (WTO), China recognised the importance of cross-border data flows for trade development but underscored their sensitivity and complexity. It advocated a gradual and exploratory approach to negotiations to ensure members fully understand the policy, economic and security implications. China emphasised that data transfers should occur only under

[66] Article 10.13, Chapter 10, China-Ecuador FTA, Pg. 64. available at https://fta.mofcom.gov.cn/ecuador/xieyi/egde_xdzw_en.pdf

conditions of guaranteed security, must be orderly and remain subject to each member's domestic laws and regulations.

This framework illustrates China's effort to balance participation in global digital trade governance with the preservation of regulatory sovereignty and national security, reflecting its broader model of "orderly data flow under state supervision."

According to the Digital Trade Integration Project (Annexure 1), China's digital trade regulatory architecture is dominated by restrictive measures aimed at maintaining state control over data, with no enabling frameworks promoting cross-border data flows through binding international agreements. China's approach emphasises data localisation, national security and administrative oversight, reflecting its model of "cyber-sovereignty."

Regulatory Restrictions

1. Information Security Technology – Personal Information Security Specification (Amendment, 2020): Prohibits the sharing or transfer of biometric data unless essential for business operations. Transfers require explicit, informed consent, detailing the recipient's identity, purpose, data categories and security safeguards.
2. Lack of Participation in Binding Agreements: China has not entered into international trade agreements that create enforceable commitments facilitating free cross-border data flows.
3. Guidelines for Personal Information Protection within Public and Commercial Services Information Systems (2013): Forbids cross-border data transfers without prior consent, government approval or regulatory authorisation.
4. Personal Information Protection Law (PIPL, 2021): Mandates the domestic storage of personal information. Cross-border transfers require a security assessment, certification or contractual arrangement with strict consent and disclosure obligations.
    a. Article 3 of the draft measures defines "personal information protection certification" as a formal evaluation by bodies authorised by the State Administration for Market Regulation (SAMR).
5. Cybersecurity Law (2017) and Outbound Data Transfer Security Assessment Measures (2022): Require "key information infrastructure operators" to store critical data within China and undergo security assessments for overseas transfers involving sensitive or large-scale data.

a. Article 31 of the Data Security Law reiterates that data collected by such operators must be stored domestically and any transfer abroad requires a prior security review.
b. Article 36 imposes restrictions on providing data to foreign judicial or law enforcement authorities.

6. Telecommunications Regulations (2000, amended 2016): Mandate domestic storage of all data collected within China. Non-compliance has led to foreign firms being compelled to divest, although the precise article mandating localisation is not publicly traceable.
7. Administrative Measures for Population Health Information (2014): Require all population health data to be stored and processed within China, prohibiting any offshore storage.
8. Interim Measures for Online Taxi Booking Services (2016): Oblige online ride-hailing companies to store and process user and business data domestically, with additional requirements on server location and data retention.
9. Notice of the People's Bank of China on Protecting Personal Financial Information (2011) and Personal Financial Information Protection Technical Specification (2020): Require financial institutions to store, process and analyse personal financial data within China. Cross-border transfers are permitted only under stringent consent, security assessment and supervisory conditions.

India

India's approach to cross-border data transfers, both in its free trade agreements (FTAs) and domestic legislation, reflects a cautious and sovereignty-driven framework that recognises the importance of data flows for trade while retaining strong regulatory discretion over outbound data movement.

In its FTA with the United Arab Emirates (UAE), India incorporates a soft provision on cross-border data flows. The agreement recognises the importance of information flows in facilitating trade and the need to protect personal data, committing both parties to promote electronic information flows subject to their respective laws and regulatory frameworks.[67] This provision is largely declaratory and does not create binding obligations on unrestricted data transfers.

[67] Article 9.11, Chapter 11, India-UAE FTA, (2019), Pg. 5. available at https://commerce.gov.in/wp-content/uploads/2022/03/Chapter-9.pdf

Under the India-United Kingdom (UK) FTA, India agreed to establish a review mechanism to engage in consultations aimed at extending "appropriate equivalent disciplines" to those agreed with a third party (non-party) concerning the prohibition or restriction of cross-border information transfers for trade or investment purposes. This clause allows for future alignment but stops short of creating an enforceable obligation to permit unrestricted data flows.

Domestic Legal Framework

Domestically, Section 16 of the Digital Personal Data Protection Act, 2023 (DPDP Act) authorises the central government to restrict the transfer of personal data by a data fiduciary to specified countries or territories outside India by notification. This provision grants the government broad discretion to determine the jurisdictions to which data transfers may be prohibited or limited.

However, the Act also provides that any law prescribing a higher degree of protection or stricter restrictions on the transfer of personal data by a data fiduciary shall continue to remain in force, ensuring that sectoral or context-specific privacy protections are preserved even if they exceed the DPDP Act's general standards.

Further, Rule 14 of the draft Digital Personal Data Protection Rules, 2025, specifies that cross-border transfers of personal data shall be subject to any restrictions or requirements prescribed by the central government through general or special orders. Such orders may relate to the conditions under which personal data can be made available to foreign states, entities or agencies under their control.

According to the Digital Trade Integration Project (Annexure 1), India maintains a restrictive regulatory stance, characterised by data localisation mandates and stringent cross-border transfer conditions, with limited participation in enabling international frameworks. This reflects India's emphasis on data sovereignty and domestic regulatory control over digital trade liberalisation.

Regulatory Restrictions

1. Reserve Bank of India Directive[68] (2018): Mandates local storage of all payment data. For cross-border transactions, data may be processed abroad but must be transferred back to India and deleted from foreign systems within 24 hours.

[68] RBI, Storage of Payment System Data, RBI/2017-18/153, (2018). available at https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11244&Mode=0

2. Insurance Regulatory and Development Authority of India Regulations (2015, 2017): Regulation 3(9) of the 2015 regulation require insurance records related to Indian policies to be stored in India. Further, Regulation 18(ii) of the 2017 regulation laid down that if services are outsourced abroad, insurers must "*ensure that the terms of the agreement are in compliance with respective local regulations governing the outsourcing service provider and laws of the country concerned and such laws further all the original policyholder records continue to be maintained in India"*.
3. Cloud Services Guidelines and Master Service Agreement (2015): Government data handled by cloud service providers must reside on servers located in India. Data cannot be transferred abroad without explicit approval from the contracting authority.
4. Companies (Accounts) Rules, 2014: Rule 3(1) mandate that the electronic records and backups shall remain accessible in India; Further, the provision to Rule 3(5) mandates that even if company records are maintained abroad, their back-ups must be periodically stored on servers located in India.
5. Section 10 of National Data Sharing and Accessibility Policy (2012): Data collected by public authorities remains their property and must reside within their IT facilities, though controlled access and sharing are permitted.
6. Condition 39.23(viii) of Unified Licence Agreement (2016): Prohibits transfer of subscriber or network information outside India, except under specific conditions such as roaming or billing. Further Condition 39.23(iii) prohibits the transfer of domestic technical network details to any place outside India.
7. Public Records Act, 1993: Restricts the removal of public records from India without prior approval of the central government.
8. Digital Personal Data Protection Act, 2023 and Draft DPDP Rules, 2025:
    a. Section 16: The central government may restrict personal data transfers to specific countries.
    b. Rule 14: Data fiduciaries must comply with government-specified conditions for transferring personal data abroad, particularly concerning access by foreign states or entities.

Enabling Measure

IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011: Permits cross-border data transfer only if the recipient ensures

equivalent data protection standards, the transfer is necessary for a lawful contract and the data subject gives explicit consent.

Data Localisation

Data localisation refers to the more explicit requirement that data be stored and/or processed within the domestic territory. There are various reasons why governments legislate data localisation measures. Some of these are[69] the following:

1. They may require data to be stored domestically on domestic privacy and protection grounds.
2. They may mandate that data be stored locally with a view to ensuring access to information for regulatory purposes.
3. Data localisation might also be sought as a means of protecting information that may be deemed to be sensitive from a national security perspective.
4. Governments also promote local storage and processing to ensure data security on the ground that data security and integrity, and the continuity of critical systems can best be guaranteed when storage and processing is domestic.
5. Data localisation is increasingly being deployed in the context of industrial policies or digital protectionism, where countries believe that these measures can help develop domestic capacity in digitally intensive sectors.

Main approaches to Data Localisation:

Data localisation measures in place today vary widely, often in relation to their underlying policy objectives, the sectors or types of data targeted and the wider legal and policy environment. Even within a particular country, or across regions, different types of data localisation measures can apply to different types of data (e.g. personal data or non-personal, data pertaining to different sectors such as health data, telecommunication data, banking or payment processing data, insurance data, or satellite and mapping data to name a few). Overall, data localisation measures can be grouped into three broads, although not sharply delineated,

[69] Chiara Del Giovane, Janos Ferencz, and Javier López-González, *The Nature, Evolution and Potential Implications of Data Localisation Measures*, OECD Trade Policy Paper No. 278 (Paris: OECD Publishing, November 2023), https://www.oecd.org/en/publications/the-nature-evolution-and-potential-implications-of-data-localisation-measures_179f718a-en.html

categories. These reflect the fact that data localisation requirements are often paired with different types of processing and/or flow restrictions. These categories are the following:[70]

1. Category 1 – The first category of measures refers to those that require local storage of data without prohibiting storage or processing in other countries. These measures are often applied in the context of ensuring that regulators do not encounter issues related to jurisdictional reach. Approaches falling under this category tend to target business records (accounts), and telecommunications or financial data, including in the context of data retention policies.
2. Category 2 – The second category of measures are those that require local storage and processing but allow international access or transfers on the basis of clearly defined conditions.
3. Category 3 – The third category of measures refers to those that mandate local storage and processing of data while also prohibiting transfers and access to other countries (or only on the basis of ad hoc authorisations). These more sweeping restrictions can apply to a range of data, including banking, telecommunications or payment data, as well as to broader categories of information. Often, these approaches are less transparent and more ambiguous in terms of the scope of application.
4. Outside this typology, a new category of approaches about access rather than location is emerging (Say Category 0). These are measures where there is no requirement for data to be stored locally, but firms are required to guarantee access to data.

Regulation on data localisation measures has been increasing recently. Regulations in OECD countries are not prohibitive as regulations in OECD countries are mostly about storage requirements; non-OECD countries also put flow restrictions. By early 2023, there were 96 measures across 40 countries in place and four draft regulations (counting that three measures that were previously in place had been revoked). Nearly half the identified data localisation measures have emerged after 2015. Importantly, the measures themselves are becoming more restrictive; by early 2023, more than two-thirds of identified measures involved a storage requirement with a flow prohibition. Trade agreements now also include data localisation measures as a requirement to conduct business. International discussions on data localisation have largely taken place in the context of preferential trade agreements (PTAs). Data localisation also affects a diverse range of data:

[70] Id.

1. Thirty-two per cent of data localisation measures identified are cross-cutting, meaning that they have implications across all sectors of the economy.
2. Sixteen per cent of the measures identified apply to financial, banking or payments sectors.
3. Fourteen per cent are in the case of the public sector.
4. Eleven per cent apply to the telecommunications sector
5. The remaining 27 per cent of the measures apply to cloud computing, health, gambling, tech platforms and other sectors.

Businesses perceive that local storage measures with no flow restrictions can lead to increases in data management costs of around 16 per cent. If local storage is combined with flow restrictions, the impacts can be considerably higher at around 55 per cent. Importantly, 8 per cent of the respondents said that more prohibitive data localisation measures would stop their ability to operate internationally.

The USA

The United States does not include provisions mandating data localisation in any of its major FTAs. However, both the USMCA and the US-Japan Digital Trade Agreement contain commitments related to the location of computing facilities. These agreements provide that "No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory." The US-Japan agreement includes an exception for the "location of financial service computing facilities for covered financial service suppliers," recognising the specific regulatory sensitivities of the financial sector.

In its communication to the Joint Statement Initiative (JSI), the United States proposed similar provisions ensuring that businesses are not required to maintain local computing infrastructure as a condition for operation. Further, in its non-paper submitted to the WTO Work Programme on Electronic Commerce (WPEC), the United States emphasised that digital service providers and companies relying on cloud computing should not be compelled to build physical infrastructure or data centres in every market they serve. It argued that such localisation requirements create unnecessary costs and burdens for both providers and consumers, and that trade rules should promote efficient data processing and cross-border connectivity.

However, in October 2023, the United States Trade Representative (USTR) withdrew its support for certain digital trade negotiating objectives at the WTO, specifically those

concerning cross-border data flows, data localisation mandates and source code disclosure. This move reflects a recalibration of the United States' position in multilateral digital trade discussions, signalling greater caution in advancing binding international commitments on digital regulatory matters.

According to the Digital Trade Integration Project (ANNEXURE 1), the United States lacks a comprehensive, unified data protection framework but relies on a sectoral approach, with separate laws governing financial services, healthcare, telecommunications, and education. In addition, California's Consumer Privacy Act (2018) represents one of the most extensive state-level privacy laws, applying to all businesses operating within California and setting broad data protection obligations.

The United States also imposes certain regulatory restrictions through sector-specific measures and security agreements. Under the Network Security Agreements (in place since 1999, last reported in December 2021), foreign communications infrastructure providers are required to sign agreements with the US government to operate domestically. These agreements impose obligations such as local storage of certain customer data, minimum retention periods for billing records and access logs, and the establishment of internal corporate teams comprising US citizens with appropriate security clearances to ensure secure access by government agencies. These provisions are primarily targeted at the telecommunications sector and aim to strengthen national security and regulatory oversight.

Further, the Code of Federal Regulations (§239.7602-2, Title 48, Chapter 2, Part 239) authorises the US Department of Défense (DoD) to require cloud service providers handling DoD-related data to store such data within the United States, subject to case-by-case authorisation for storage abroad, depending on data sensitivity. Similarly, the Federal Risk and Authorization Management Program (FedRAMP) mandates that federal agencies include contractual clauses specifying data location requirements where applicable, identifying where "data-at-rest" must be stored.

Collectively, these measures illustrate that while the US maintains an open stance on cross-border data flows in trade agreements, it simultaneously enforces targeted localisation and security requirements in sensitive sectors for national security and regulatory compliance purposes.

The European Union (EU)

Across its Free Trade Agreements (FTAs), the European Union consistently promotes a policy framework opposing data localisation requirements, reinforcing its broader objective of facilitating unrestricted cross-border data flows while preserving regulatory autonomy for data protection.

The EU-Chile FTA explicitly prohibits data localisation measures that could impede digital trade. Article 19.4(b) prevents either party from requiring data to be stored or processed within its territory, while Article 19.4(c) prohibits restrictions on storage or processing in the other party's territory. The agreement further bars making cross-border data transfers conditional on the use of local computing facilities or network elements, including those certified or approved domestically. These provisions collectively ensure unhindered data movement between the EU and Chile.

The EU-Mercosur FTA adopts a more flexible approach, allowing exceptions to the prohibition on data localisation to ensure compliance with domestic laws. Article 54(1)(f)(ii) permits measures deemed necessary to uphold national regulations, particularly those protecting individual privacy and personal data. However, such measures must not constitute arbitrary or unjustifiable discrimination or disguised restrictions on trade, thereby maintaining the balance between regulatory flexibility and open digital trade.

The EU-New Zealand FTA similarly reinforces the EU's commitment to prohibiting localisation mandates. Articles 12.4(b) and (d) expressly forbid requiring data to be stored or processed within national borders, ensuring smooth digital trade and operational efficiency for businesses.

The EU-South Korea FTA echoes this principle in Article 5(1)(b) and (d), which prevents restrictions on cross-border data transfers based on the location of computing facilities or network elements within a party's territory.

Likewise, both the EU-Ukraine (Article 140) and EU-UK (Chapter II, Article 201) agreements uphold commitments to facilitate unrestricted cross-border data transfers without imposing localisation requirements. They also provide for periodic review mechanisms to ensure continued alignment with evolving data protection standards.

Collectively, these agreements reflect the EU's coherent trade policy stance against data localisation, aimed at fostering a predictable and open digital environment while safeguarding the right to regulate in the interest of privacy and data protection.

China

China's approach to data localisation in its free trade agreements (FTAs) is characterised by limited explicit commitments and a strong emphasis on preserving regulatory discretion. While most of China's FTAs omit direct provisions on cross-border data transfers and localisation, the Regional Comprehensive Economic Partnership (RCEP) introduces a nuanced framework balancing trade facilitation with domestic policy autonomy.

Under the RCEP, China agreed that each party may maintain its own measures concerning the use or location of computing facilities, including requirements designed to ensure the security and confidentiality of communications. At the same time, the agreement establishes a general obligation that no party shall require a covered person to use or locate computing facilities within its territory as a condition for conducting business, thereby discouraging mandatory data localisation.

However, Paragraph 3 of Article 12.14 provides broad exceptions, allowing parties to adopt or maintain localisation measures when deemed necessary to achieve legitimate public policy objectives, such as data protection or national security. These measures must not constitute arbitrary or unjustifiable discrimination or disguised restrictions on trade. Importantly, measures taken for the protection of essential security interests are explicitly non-justiciable and cannot be challenged by other parties.

This framework reflects China's cautious approach – formally recognising the principle against forced localisation while retaining expansive flexibility to impose localisation requirements on public policy or security grounds.

China's Legal and Policy Framework on Data Localisation and Cross-Border Data Transfers (as per the Digital Trade Integration Project, ANNEXURE 1)

China's regulatory environment is primarily restrictive, characterised by extensive localisation requirements, mandatory data retention and government access provisions across multiple sectors. While there are limited enabling measures permitting cross-border transfers under security-controlled conditions, the overall framework prioritises data sovereignty, national security and administrative control over digital trade liberalisation.

Regulatory Restrictions

1. Personal Information Protection Law (PIPL)
    a. Article 40: Requires critical information infrastructure (CII) operators and personal information processors to store all personal data collected within China domestically.
    b. Cross-border transfers may occur only after passing a security assessment conducted by the Cyberspace Administration of China (CAC).
2. Outbound Data Transfer Security Assessment Measures
    a. Based on Article 37 of the Cybersecurity Law, key information infrastructure operators must store personal and critical data within China.
    b. Transfers abroad are permitted only when business necessity exists and after a mandatory CAC-led security assessment in co-ordination with relevant ministries.
3. Provisions for the Administration of Internet Electronic Bulletin Boards (2000)
    a. Providers must retain user records (account details, IP addresses, access logs) for 60 days and make them available to authorities on request.
4. Administrative Measures for Population Health Information (Trial)
    a. Article 10 mandates domestic storage and processing of population health data; overseas storage is prohibited.
5. Internet Surfing Service Business Venue Management Rules (2001; amended 2011, 2016, 2019)
    a. Internet café operators must record and store user identity and browsing data for 60 days, sharing it with authorities upon request.
6. Information Security Technology – Personal Information Security Specification (GB/T 35273-2020)
    a. Section 9.2(i) prohibits transferring biometric data abroad unless strictly necessary for business.
    b. Requires explicit informed consent, disclosure of recipient identity, purpose, and security capabilities.
7. Provisions on the Management of Automotive Data Security (Trial)
    a. Articles 11–12: Automotive data deemed “important” must be stored domestically.

   b. Cross-border transfers are allowed only after a security assessment involving the CAC and other authorities.

8. Administrative Provisions on Mobile Internet Applications (2016)
   a. App providers must authenticate users' identities, retain logs for 60 days, and make them available to regulators.
9. Interim Regulations on Network-Appointed Taxi Service Operations (2016, amended 2020)
   a. Article 27: Online taxi operators must store user and operational data within China for at least two years.
   b. No cross-border transfers are allowed unless authorised by law and subject to security protocols.
10. Notice of the People's Bank of China (Yinfa No. 17/2011)
   a. Personal financial information collected by banks must be stored, processed, and analysed within China.
   b. Cross-border transfers are prohibited.
11. Guidelines for Personal Information Protection within Public and Commercial Services Information Systems (2013)
   a. Article 5.4.5: Forbids overseas data transfers without explicit consent, of the data subject, or clear provisions in laws or regulations, or without the agreement of the controlling departments.[71]
   b. Unauthorised transfers to foreign entities or individuals are strictly prohibited.
12. Regulation on Internet Information Services (2000) and Decision on Strengthening Network Information Protection (2012)
   a. Internet service providers (ISPs) must retain connection data (IP, duration, accounts) for 60 days and co-operate with investigations.
13. Online Publishing Service Management Rules (2016)
   a. Articles 8 and 9 require online publishers' servers and data storage to be located within China.
14. Map Management Regulations (2016)

[71] Creemers Rogier, Information Security Technology Guidelines for Personal Information Protection on Public and Commercial Service Information Systems, Digi China, Stanford University, (2013), pg. 9. available at https://digichina.stanford.edu/work/information-security-technology-guidelines-for-personal-information-protection-on-public-and-commercial-service-information-systems/

a. Mandates domestic hosting of servers and acquisition of an official operation certificate for online mapping services.

15. Telecommunications Regulations (2000, amended 2016)
    a. Require all data collected within China to be stored on Chinese servers.
    b. Enforcement has led to forced divestments by foreign firms (e.g., HP, Qualcomm, Uber) exceeding 50 per cent ownership to comply.
16. Administrative Provisions on Foreign-Funded Telecommunications Enterprises (2016 Revision)

    a. Foreign cloud and data centre operators must form joint ventures with Chinese partners and obtain internet data centre (IDC) licences.

Enabling Measures

1. Conditional Cross-Border Transfers
    a. Permitted only under strict conditions:
        i. Security assessments by CAC or other designated agencies
        ii. Explicit user consent and compliance with Chinese data protection standards
        iii. Demonstrated business necessity and government oversight
    b. Even where allowed, reciprocity and traceability mechanisms ensure Chinese jurisdictional control.

India

India's Free Trade Agreements (FTAs) concluded to date do not include provisions mandating data localisation or the localisation of computing facilities. However, according to the Digital Trade Integration Project (Annexure 1), India maintains a combination of regulatory restrictions that impose obligations for data storage, retention and localisation across multiple sectors.

Regulatory Restrictions

1. Prevention of Money-laundering (Maintenance of Records) Rules, 2005 – Rule 3 requires banking information to be stored for ten years from the cessation of transactions, applying to banks and financial institutions.
2. Reserve Bank of India (RBI) Directive, 2018 – Payment data must be stored in local facilities within six months; cross-border processing is permitted only if data are deleted

from foreign systems and brought back to India within 24 hours. Settlement data must also remain in India. Banks may store offshore banking data, but domestic payment data must remain in India.

3. SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 – Listed entities must preserve corporate and financial documents for specified durations ranging from five years to permanent retention, depending on classification under Schedules I–III.
4. IRDAI Regulations (2015 & 2017) – Insurers must store policy and claims data in data centres located in India. When outsourcing services abroad, original records must still be retained in India.
5. Licence Agreement for Internet Services (Amended 2022) – Internet service providers must retain call, exchange and IP records for at least two years for security purposes.
6. Unified Licence Agreement (Condition 39.23(viii)) – Telecommunications licensees are prohibited from transferring subscriber or user information abroad, except in limited cases related to roaming and international circuits.
7. National Data Sharing and Accessibility Policy – Requires that non-sensitive data generated using public funds be stored within India's borders.
8. Guidelines for Government Departments on Cloud Services (MeitY, 2015) – Empanelled cloud service providers must store all government data in India. The master service agreement further mandates that data stored abroad must not be removed without explicit approval by the government purchaser.
9. Companies (Accounts) Rules, 2014 – Books of account maintained electronically must be accessible in India; backup copies of data stored abroad must be periodically stored on servers located in India.
10. CERT-In Direction No. 20(3)/2022-CERT-In – Data centres, cloud services and VPN providers must retain subscriber and transaction data for at least five years, covering IPs, emails, contact details and financial information.

Protection and Non-Discriminatory treatment of ICT products that use cryptography

Information and Communication Technology (ICT) products such as smartphones, laptops, servers, cloud platforms, routers, messaging apps and banking systems play a central role in modern economies. These products often rely on cryptography, which means securing data and

making it unreadable to unauthorised parties using techniques like encryption, decryption, digital signatures and hashing.

Some examples of cryptography used in ICT products are:

1. Use of end-to-end encryption[72] in messaging platforms like WhatsApp and Signal.
2. Use of TLS/SSL encryption[73] for safe online transactions in web browsers.
3. Use of WPA3/WPA2 encryption[74] to secure wireless networks

Digital trade, whether it is cross-border e-commerce, cloud services, digital payments or data transfer, depends on trust. Thus, it becomes crucial that data maintains its integrity, transactions remain confidential and identities of buyers, sellers or platforms are authenticated.

Cryptographic security ensures that this data remains safe from espionage, cyberattacks or manipulation, making firms and governments more comfortable with allowing such flows. Without cryptographic protection, users and firms would be unwilling to engage in online trade due to the risks of fraud, hacking or data theft. Countries and companies that cannot guarantee secure ICT products risk losing trust in global digital markets.

For smooth cross-border function of digital products it is also important that countries do not discriminate against foreign service providers. Non-discrimination guarantees that all suppliers, domestic or foreign, compete under the same conditions, boosting innovation, competition and consumer choice. If countries discriminate against foreign ICT products with cryptography by using methods such as domestic certification, imposing unique technical standards or blocking imports from foreign firms it will be disadvantageous for corporations for the facilitation of digital trade in foreign countries. A good example of this is China where

[72] End-to-end encryption (E2EE) is a secure communication process that encrypts data before transferring it to another endpoint. Data stays encrypted in transit and is decrypted on the recipient's device. Messaging apps, SMS and other communications services rely on E2EE to protect messages from unauthorised access.
[73] TLS (Transport Layer Security) and its predecessor SSL (Secure Sockets Layer) are cryptographic protocols that secure communication over the internet. They encrypt the data exchanged between a user's browser and a server, ensuring that sensitive information like passwords, credit card details or personal data cannot be intercepted or altered by attackers. TLS/SSL also provides authentication (verifying the server's identity through digital certificates) and integrity (ensuring the data is not tampered with), making it the backbone of secure web browsing, often recognised by the "https://" prefix in website addresses.
[74] WPA2 (Wi-Fi Protected Access 2) and WPA3 are security protocols used to protect wireless networks. They encrypt the data transmitted between devices and a Wi-Fi router, preventing outsiders from eavesdropping or accessing the network. WPA2, introduced in 2004, uses AES (Advanced Encryption Standard) for strong protection but has known vulnerabilities. WPA3, introduced in 2018, improves on WPA2 by using stronger encryption (like SAE – Simultaneous Authentication of Equals), making it harder for attackers to guess passwords and providing better security even with weak passwords. In short, WPA3 is the newer, more secure standard for Wi-Fi encryption.

global services such as WhatsApp, Signal, etc., do not operate and domestic services such as WeChat have a monopoly in the domestic market.

Governments often cite security concerns to restrict encrypted products. However, if such restrictions are applied selectively, they can function as hidden trade barriers. A non-discrimination principle allows governments to address security risks (through standards or lawful access) while preventing protectionism disguised as security regulation. Besides, for digital trade to grow, users must trust that their communication, identity and transactions are protected.

We take a look at the policy stand of the USA, EU, China and India under their various FTAs regarding protection and non-discrimination of ICT products that use cryptography.

The USA

The United States places the principle of non-discrimination between domestic and foreign digital suppliers at the centre of its digital trade policy. In its communications to the WTO, the United States did not propose any provision concerning the protection of commercial ICT products that use cryptography. While multilateral trade rules under the WTO safeguard non-discrimination for goods, services and intellectual property, they do not explicitly cover digital products. To address this gap, the United States has consistently advanced the extension of the most favoured nation (MFN) and national treatment (NT) principles to digital trade. In its submissions to the Joint Statement Initiative (JSI) on e-commerce and to the WTO Work Programme on Electronic Commerce (WPEC), the US proposed binding obligations prohibiting members from according less favourable treatment to digital products of another party than to like domestic products, irrespective of the product's place of creation, publication, storage, transmission, contracting, commissioning, or first availability, or the nationality of its producer, author, performer, developer, or distributor.

This position is reflected across all US FTAs, which contain nearly identical provisions mandating equal treatment for digital products created or made available commercially outside a party's territory. The provisions also extend to non-party products, ensuring a broad scope of non-discrimination. However, these obligations are subject to specific exceptions, including the following:

1. Non-conforming measures maintained under the services, investment, or financial services chapters

2. Inconsistencies with the intellectual property rights chapter, as recognised in the US-Australia FTA
3. Audio-visual and broadcasting sectors, allowing domestic regulatory discretion
4. Subsidies or grants, including government-supported loans, guarantees and insurance, as clarified in the USMCA and the US-Japan Digital Trade Agreement.

Additionally, the US-Japan FTA permits limitations on foreign capital participation in broadcasting enterprises and preserves rights under bilateral or international intellectual property agreements. Collectively, these commitments reaffirm the US policy objective of embedding strong non-discrimination disciplines in digital trade while retaining flexibility in sensitive sectors.

United States cryptography legal framework

The United States cryptography legal framework primarily governs the export and lawful interception of encrypted communications through a combination of regulatory instruments and statutory provisions. The International Traffic in Arms Regulations[75] (ITAR) and the Export Administration Regulations[76] (EAR) both impose controls on the export of encryption technologies, particularly certain forms of encryption software and source code. The EAR regulates exports under Export Control Classification Number (ECCN) 5D002 on the Commerce Control List (Supplement No. 1 to part 774 of the EAR), covering encryption source code and object code software. These restrictions extend to making such software available for download outside the United States, including through online platforms or electronic transmissions. Section 740.13(e) provides notification requirements for the export or re-export of publicly available encryption source code, while Section 734.3 defines the scope of EAR, specifying that foreign-made goods or software containing controlled US-origin encryption are subject to regulation unless excluded Specifically, this applies to (i) any quantity, as described in §734.4(a) or (ii) quantities exceeding de minimis levels, as outlined in §734.4(c) or §734.4(d).[77]

[75] Sec. 120.1, International Traffic in Arms Regulations, Title 22, Chapter 1, Subchapter M, Part. 120. available at: https://www.pmddtc.state.gov/ddtc_public/ddtc_public?id=ddtc_kb_article_page&sys_id=%2024d528fddbfc930044f9ff621f961987
[76] Sec. 730.1, Export Administration Regulation, Subchapter C, Part. 730. available at: https://www.govinfo.gov/content/pkg/CFR-2012-title15-vol2/pdf/CFR-2012-title15-vol2-subtitleB-chapVII-subchapC.pdf
[77] Id. pg. 24

Domestically, there is no legislative authority mandating telecommunications or online service providers to facilitate government decryption of encrypted communications. However, the Communications Assistance for Law Enforcement Act (CALEA) of 1994 requires telecommunications carriers to ensure that their systems have the technical capability to intercept and deliver communications to the government when lawfully authorised. Importantly, CALEA does not require carriers to decrypt communications encrypted by users unless the encryption was provided by the carrier itself and it possesses the means to decrypt it.

The European Union

The European Union does not include an explicit provision on the non-discriminatory treatment of ICT products using cryptography in the digital trade chapters of its FTAs. However, the EU embeds the principle of non-discrimination across other chapters, particularly those related to customs, trade facilitation and telecommunications services, reflecting its broader commitment to fairness, transparency and equal market access.

While strongly committed to privacy and security (e.g., under GDPR), there are no explicit provisions on protecting ICT products using cryptography in its FTAs; instead, encryption is regulated through its internal dual-use export control framework. Under the EU Dual-Use Regulation, cryptographic products are treated as "dual-use" items technologies that can serve both civilian and military or security purposes. As a result, their export is subject to licensing and oversight to prevent misuse for surveillance, defence or cyber operations. This approach allows the EU to maintain strong security controls and adapt regulations to evolving risks, while keeping its FTAs focused on broader trade liberalisation rather than sensitive technology governance.

Under the EU-UK Trade and Co-operation Agreement, the EU obliges parties to ensure that any authorisations and applicable procedures are objective, transparent and non-discriminatory. Article 380 of the same agreement further reinforces this by committing both parties to non-discriminatory treatment and commercial consideration in the application of trade procedures.

Similarly, in its FTA with MERCOSUR, the EU undertakes to guarantee access to essential telecommunication facilities on reasonable and non-discriminatory terms, ensuring that suppliers of telecommunication services are provided interconnection on term, conditions and rates and of a quality no less favourable than those offered to domestic suppliers.

The EU-New Zealand FTA reiterates these principles under Article 10.50, requiring that authorisation criteria for providing telecommunication networks or services remain objective and non-discriminatory. It also mandates that enterprises or service suppliers from the other party enjoy access to and use of public telecommunication networks and services on reasonable and non-discriminatory terms and conditions.

Collectively, while the EU does not explicitly address cryptographic non-discrimination in ICT products, its broader treaty architecture upholds non-discriminatory access, transparency, and fairness as foundational principles in the regulation of digital and telecommunication services.

According to findings from the Digital Trade Integration Project (Annexure 1), several EU policies function as regulatory restrictions on foreign participation in IT services, internet access and digital content services, thereby conferring competitive advantages to domestic companies. These measures collectively reflect a protectionist dimension within the EU's otherwise liberal digital trade framework.

The International Procurement Instrument (IPI) imposes reciprocity-based limitations on the participation of non-EU firms in EU public procurement tenders. It restricts access for companies from countries that do not provide comparable opportunities for EU suppliers, applying to tenders valued at €15 million or more for works and concessions and €5 million or more for goods and services, including computers and related ICT products.

Furthermore, while the EU is a signatory to the WTO Government Procurement Agreement (GPA), its coverage schedules exclude telecommunications-related services (CPC 754), a core component of digital trade. This exclusion effectively narrows market access for foreign telecommunication and ICT service providers in the EU's procurement framework.

In addition, the European Standardisation Strategy (2022) introduced amendments to Regulation (EU) No 1025/2012 governing European standardisation organisations (ESOs). These amendments restrict the participation of non-EU stakeholders in the formulation of harmonised European standards applicable to ICT goods and online services. This limitation affects global interoperability and can indirectly hinder the ability of foreign companies to align with EU technical standards, thereby impacting market access and competitiveness.

China

China does not include provisions on non-discriminatory treatment of ICT products that use cryptography in its FTAs. However, its domestic legal framework introduces multiple

regulatory restrictions that collectively disadvantage foreign firms in the digital and ICT sectors. According to the Digital Trade Integration Project (Annexure 1), China's policies primarily serve as regulatory restrictions on IT services, internet access and digital content services provided by foreign multinationals, thereby favouring domestic enterprises. China also tightly controls cryptography under its 2020 Cryptography Law, requiring state approval and certification.

Foreign companies face complex compliance and licensing requirements, with numerous government bodies involved in accreditation and operational approvals. These overlapping procedures create significant barriers to market entry and operation. Domestic preferences are evident in government procurement, where Article 10 of the Government Procurement Law mandates the purchase of domestic goods and services except under limited circumstances, such as unavailability or overseas use.

In the area of encryption and ICT standards, the Regulation on Commercial Encryption requires prior certification from the National Commission on Encryption Code Regulations (NCECR) for any product using commercial encryption codes. Only Chinese or Chinese-owned firms can obtain such certification, effectively excluding foreign participants from the market. Similarly, the WAPI standard mandates the use of a domestically developed encryption protocol in all wireless equipment, superseding international norms like IEEE 802.11i.

Restrictions also extend to telecommunications and internet services. The Circular on Clearing up and Regulating the Internet Access Service Market (2017) prohibits telecom and internet service providers from establishing or renting VPNs without government approval. The Telecommunications Regulations (2000, amended 2016) and related licensing measures require ICP (internet content provision) licences for online services, with non-compliance leading to shutdowns or blacklisting. Foreign entities are barred from engaging in online publishing, and Article 8 of the Administrative Regulations for Online Publishing Services (2016) requires all servers and technical infrastructure to be located in China, with foreign co-operation subject to prior state approval.

Additionally, China maintains quantitative import restrictions on certain mechanical and electrical ICT products, as reflected in the MOFCOM Notice No. 106/2018 and related catalogues. Under the Cryptography Law, imports and exports of encryption products and technologies remain subject to government approval, with the definition of "commercial encryption for general consumption" left ambiguous.

Broad controls on digital content and information flows are further reinforced through content filtering and censorship mechanisms, including the Golden Shield Project, which blocks international websites, VPNs and social media platforms. Directives such as Directive No. 618 promote "indigenous innovation" by granting preferential treatment to products owned and developed by Chinese entities in government procurement.

Collectively, these measures reflect a highly restrictive digital governance model, wherein domestic industrial policy, encryption control and content regulation intertwine to safeguard national security and technological sovereignty, often at the expense of foreign market access and competition.

India

India's approach to non-discrimination and regulatory restrictions in digital trade reflects a blend of co-operative provisions in its FTAs and domestically protective measures aimed at security, localisation and domestic industry promotion. India allows encryption for commercial purposes but emphasises government access through sectoral regulations and oversight mechanisms.

In its FTA with the UAE, India has taken a positive and co-operative stance on digital products. Under Article 9.14 ("Co-operation on Digital Products"), both parties have agreed to mutually promote each other's digital products, provided these are created, produced, published and stored in the other's territory, and that the author or developer is a national of the other party. However, this co-operation does not extend to measures affecting the electronic transmission of scheduled audio-visual content where the consumer lacks control over scheduling.

Domestically, however, India's regulatory framework introduces several restrictions affecting digital trade and ICT-related services, primarily aimed at national security, consumer protection and domestic value addition.

According to the Digital Trade Integration Project, most of India's regulatory barriers are linked to internet shutdowns and domestic certification requirements.

Key measures include the following:

1. Information Technology Act, 2000 (Section 84A): Authorises government control over encryption standards for secure e-governance and e-commerce, though no implementing rules have been issued

2. Mandatory Testing and Certification for Telecom Equipment (MTCTE) and the Electronics and IT Goods (Compulsory Registration) Order, 2021: Impose local testing and certification requirements even on internationally certified equipment, covering over 175 telecom products
3. App bans under Section 69A of the IT Act (2020): Enabled blocking of 267 mobile apps on national security and public order grounds
4. National Security Directive on Telecommunication Sector: Mandates screening and security clearance for foreign telecom vendors, effectively restricting equipment from certain countries
5. Public Procurement Rules (General Financial Rules, 2017; DPIIT Orders):
    1. Prohibit global tender enquiries below INR 200 million
    2. Permit preferential treatment for locally manufactured goods and suppliers with ≥50 per cent local content ("Class-I Local Suppliers")
    3. Require joint ventures with Indian firms for large-scale procurements where domestic capacity is insufficient
6. Telegraph (Amendment) Rules, 2017: Impose domestic security testing and inspection of telecom hardware and software, adding compliance costs and risks of IP exposure

Together, these measures reveal India's dual-track digital trade policy – a co-operative and open stance in select FTAs like the India-UAE CEPA, contrasted by stringent domestic regulations that prioritise national security, data integrity and local industry protection over market openness.

Source Code Access and IPR Protection:

Source code forms the core of software development, serving as the underlying instructions that determine how a digital product operates. As software becomes an integral part of the global economy, the protection of source codes and algorithms has emerged as a critical issue in digital trade negotiations. Ensuring that source codes remain secure and proprietary is essential for intellectual property protection, cybersecurity and fostering innovation.

The protection of source codes is closely tied to intellectual property rights (IPR), as unauthorised access or forced disclosure can expose businesses to industrial espionage, unfair competition and loss of proprietary knowledge. Strong IPR frameworks safeguard software

ownership and innovation, preventing competitors from misusing trade secrets while ensuring a fair and competitive digital market.

However, approaches to source code regulation vary. While some frameworks emphasise strict protection, preventing mandatory disclosure of source codes to safeguard business interests and trade secrets, others incorporate exceptions that allow access under specific legal circumstances such as regulatory investigations or security concerns. Certain regulatory models permit voluntary disclosure through commercial agreements, balancing business flexibility with regulatory oversight.

The USA

The United States adopts a strong protective stance on source code and algorithm disclosure, complemented by enabling domestic and international frameworks that safeguard intellectual property rights (IPR) and promote digital trade.

Across its trade agreements, such as the USMCA, the US-Japan Digital Trade Agreement, and its communication to the WTO Joint Statement Initiative (JSI) on E-commerce, the US has established a hard legal obligation prohibiting either party from requiring the transfer of, or access to, source code or algorithms of software owned by persons of the other party as a condition for import, distribution, sale or use of that software or related products.

An exception to this rule applies where a regulatory or judicial authority may require a person to preserve or provide access to source code or algorithms for the purpose of specific investigations, inspections, enforcement actions or judicial proceedings, provided that safeguards against unauthorised disclosure are in place.

According to the Digital Trade Integration Project, the US supports digital trade through enabling legal and institutional measures that enhance innovation and IPR protection. These include the following:

1. Defend Trade Secrets Act (2016) which creates a federal cause of action against trade secret misappropriation, strengthening protection of proprietary digital information
2. WIPO Copyright Treaty (2002) that establishes standards for digital copyright and rights management.
3. WIPO Performances and Phonograms Treaty (2002) that protects digital rights of performers and producers, facilitating cross-border creative trade

4. Copyright Act (1976). which recognises source code as a “literary work” protected by copyright, while the Fair Use Doctrine (Section 107) enables educational, research, and innovation-related exceptions
5. Patent Cooperation Treaty (1978) that simplifies international patent filings, promoting global protection for digital innovations

Together, these instruments form a comprehensive and innovation-oriented framework, balancing commercial confidentiality with regulatory oversight and reinforcing the US position as a global leader in the protection and promotion of digital trade and intellectual property.

The European Union

The European Union (EU) has adopted a coherent and protective framework on source code access across its free trade agreements (FTAs) with partners such as Mercosur, New Zealand, South Korea, Japan, Chile and the United Kingdom. These agreements collectively establish the principle that no party shall require the transfer of, or access to, source code of software owned by a juridical or natural person of the other party, reflecting the EU’s commitment to safeguarding intellectual property rights and technological autonomy.

Key provisions, such as Article 12.11 (EU-New Zealand), Article 11 (EU-South Korea), Article 19.12 (EU-Chile), and Article 207 (EU-UK), set out this prohibition as a hard legal obligation, ensuring that software developers and firms retain exclusive control over their proprietary code.

These FTAs also introduce limited exceptions that allow access or transfer of source code under strictly defined circumstances. Permissible situations include voluntary transfers or commercial licensing arrangements, as well as requests by regulatory, conformity assessment, or judicial authorities for legitimate purposes such as investigation, inspection, or enforcement, subject to confidentiality safeguards to prevent unauthorised disclosure.

Furthermore, these agreements reaffirm the EU’s adherence to broader commitments in competition law, intellectual property protection and international obligations, including the WTO Government Procurement Agreement (GPA). This ensures that trade liberalisation does not compromise fundamental legal protections or market fairness.

In contrast, the EU-Japan Economic Partnership Agreement (Article 8.73) adopts a soft obligation, using the phrasing “a Party may not require,” which, while still prohibitor in intent, reflects a more flexible legal formulation. Nevertheless, it maintains the EU’s overarching

objective of preserving the confidentiality of source codes while supporting regulatory co-operation and commercial transparency.

Overall, the EU's approach balances IPR protection, regulatory discretion and commercial flexibility, creating a legally secure environment for cross-border digital trade and innovation.

According to the 'Digital Trade Integration Project' (ANNEXURE 1), the European Union has implemented significant policies and international agreements related to Source Code Access and IPR. These include the following.

Enabling Measures

1. Directive (EU) 2016/943 on the Protection of Trade Secrets (June 2016): Harmonises national laws on trade secret protection across the EU by providing a uniform definition and establishing measures against unlawful acquisition, use and disclosure. Exceptions allow disclosures in the public interest, including to expose misconduct or illegal activities.
2. WIPO Copyright Treaty (ratified 2009): Provides legal protection for copyright in the digital environment, facilitating the trade and protection of creative works. Under this treaty, authors are provided with the exclusive rights of distribution and rental, and with a broader right of communication to the public of their works in the digital environment. Computer programs are protected as literary works and the arrangement or selection of data or other material in databases is also protected. Specific protection is also provided for technological measures and electronic rights management information used to identify and manage works.

Regulatory Restrictions

1. EU Copyright Acquis (since 2001): Comprises 11 directives and two regulations that harmonise copyright laws. However, it lacks a unified copyright system. Exceptions to copyright are limited and controlled under the "three-step test" in line with the Berne Convention.
2. Digital Services Act (DSA) (since July 2022): Requires very large online platforms (defined as those with more than 45 million monthly users) to provide access to confidential data and algorithms to regulators and vetted researchers under strict conditions. This may raise concerns about trade secret protection.

3. Regulation EU 2019/1150 (Platform to Business Regulation) (since July 2019): Mandates transparency in algorithmic ranking for online intermediation services, potentially affecting trade secret protection. Service providers cannot refuse disclosure solely on the grounds of trade secrets.
4. Directive (EU) 2016/943 on Trade Secrets (The Trade Secrets Directive) (since 2016): Protects trade secrets while allowing their disclosure for public interest reasons, including regulatory compliance or reporting misconduct.

These measures collectively represent the EU's approach to balancing innovation, transparency and regulation in digital trade concerning source code access and IPR. While enabling measures foster growth and participation in global digital markets, regulatory restrictions impose conditions to ensure fairness, transparency and the protection of public interest.

China

China's Cybersecurity Law, enacted in 2017, imposed significant compliance costs on multinational companies, giving the Chinese government broad access to the software source code, thus exposing them to industrial espionage risks and the threat of trade secrets, and giving some Chinese firms an unfair advantage.

The law also grants Beijing the right to request access to the software source code and national security reviews allow deeper access into companies' intellectual properties. This is in contrast to democracies where laws regulate both corporate and government access to information, China's laws provide the government unrestricted access to personal and commercial data.

According to the 'Digital Trade Integration Project' (ANNEXURE 1), China's regulatory and institutional framework for digital trade reflects a mix of enabling measures and regulatory restrictions concerning source code access and IPR. The details are given below.

Enabling Measures:

1. Ratification of the WIPO Copyright Treaty: Facilitates the protection of copyright in the digital environment and supports international trade in creative industries
2. Ratification of the WIPO Performances and Phonograms Treaty: Provides protection for performers and producers of phonograms in the digital economy
3. Patent Co-operation Treaty (PCT) (since January 1994): Provides a framework for patent applications across multiple jurisdictions, supporting innovation and cross-border patent filings

Regulatory Restrictions:

1. Lack of Comprehensive Regulatory Framework Covering Trade Secrets: Limited measures under the Anti-Unfair Competition Law (2019), Civil Code (2021), and other laws provide partial protection for trade secrets. Stakeholders acknowledge progress, particularly under the revised criminal law, which offers stronger procedural protection and broader definitions of misappropriation.
2. Copyright Law of the People's Republic of China (Amended in 2020): Lacks fair use provisions comparable to other major jurisdictions, limiting lawful uses of copyrighted work. Exceptions under Article 22 remain specific and restrictive.
3. National Security Law (2015): Mandates all information systems in China to be "secure and controllable," requiring companies to grant the government access to sensitive information like the source code and encryption keys.
4. Lack of Adequate Enforcement of Copyright Online: High levels of piracy persist, and enforcement remains weak. China is a major origin economy for counterfeit goods, with significant economic impact.
5. Patent Law of the People's Republic of China (Amended in 2020): Introduces procedural challenges for non-resident patent applicants and places limits on compensation for damages. Recent amendments aim to address some enforcement difficulties but it remains a regulatory constraint.
6. The Medium- and Long-Term Plan for the Development of Science and Technology (2006-2020): Incentivises domestic innovation but restricts foreign participation by requiring Chinese ownership of intellectual property rights for product accreditation.

This framework illustrates the dual approach of encouraging innovation and protecting intellectual property while imposing conditions and constraints that limit the broader integration of China's digital economy into global systems.

India

Under its latest FTA with the United Kingdom, India adopted a hard obligation to restrict the requirement of transfer of, or access to, the source code of software owned by a person of the other party. This provision aligns India with global digital trade norms that safeguard proprietary technologies and intellectual property in the digital economy.

The Article 12.15 of the FTA, provides explicit exclusions, allowing regulatory bodies, judicial authorities, conformity assessment bodies and administrative tribunals to require access to

source code for legitimate purposes such as investigation, inspection, examination, enforcement action or judicial proceedings. It also clarifies that the voluntary transfer or granting of access to source code by a person of the other party remains outside the scope of this restriction, thus enabling commercial flexibility and contractual freedom.

According to the Digital Trade Integration Project (Annexure 1), India's regulatory and institutional framework concerning source code access and intellectual property rights (IPR) represents a balanced mix of enabling measures and regulatory restrictions that are summarised below.

Enabling Measures

1. Regulatory Framework Covering Trade Secrets
    - Although India lacks a dedicated trade secrets law, judicial precedents recognise trade secret protection through contract law, copyright law, principles of equity and the common law doctrine of breach of confidence.
    - The Information Technology Act, 2000, further strengthens protection for electronic records, providing an additional safeguard for digital assets.
2. Ratification of the WIPO Copyright Treaty (2018)
    - Aligns India's copyright protection with international digital standards, supporting digital trade, software innovation and creative industries.
3. Ratification of the WIPO Performances and Phonograms Treaty (2018)
    - Enhances protection for performers and producers of phonograms, promoting cross-border trade and co-operation in creative sectors.
4. The Copyright Act, 1957 (as amended in 2021)
    - Incorporates a fair dealing provision (Article 52(1)) that enables the lawful use of copyrighted materials for research, education and innovation, thereby supporting digital creativity and knowledge diffusion.
5. Patent Co-operation Treaty (PCT) (since December 1998)
    - Facilitates international patent filings, enabling innovators to secure protection across multiple jurisdictions, strengthening India's integration into the global IP ecosystem.

Regulatory Restrictions

1. Weak Enforcement of Copyright in the Digital Sphere

- Despite a robust legal framework, enforcement challenges persist due to limited technical capacity, absence of a centralised IP enforcement body, and co-ordination gaps among agencies, leading to high piracy rates.

2. Patents Act, 1970 (Foreign Filing Licence Requirement)
    - Inventors are required to first file patents in India or obtain prior permission to file abroad. While designed to safeguard domestic innovation, it imposes procedural burdens and carries criminal liability for non-compliance.
3. Practical Barriers in Patent Enforcement
    - Issues such as prolonged litigation, potential revocations, and lack of presumption of validity weaken patent enforcement. The Commercial Courts Act has been introduced to expedite IP disputes, but resource constraints limit its effectiveness.
4. Patents Rules, 2003 (Design Filing Procedures)
    - Although copyright, trademark and patent applications can be filed online, design filings still require in-person submission. Additionally, foreign applicants must engage local Indian agents, increasing compliance costs and procedural complexity.

Digital Services Trade Restrictiveness Index

Having taken a look at the various provisions in FTAs, we now take a look at where the US, EU, China and India stand on the OECD's Digital Services Trade Restrictiveness Index.

According to OECD, "*The rise of services in international trade is closely linked to rapid technological developments. Services that traditionally required close proximity to customers now can be traded at a distance, allowing firms to reach global markets at lower costs. The OECD Digital Services Trade Restrictiveness Index (DSTRI) measures cross-cutting barriers that inhibit or completely prohibit firms' ability to supply services using electronic networks, regardless of the sector in which they operate. It includes five measures: 1) infrastructure and connectivity, 2) electronic transactions, 3) e-payment systems, 4) intellectual property rights and 5) other barriers to trade in digitally enabled services. The DSTRI is a composite index that takes values between 0 and 1, where 0 indicates an open regulatory environment for digitally enabled trade and 1 indicates a completely closed regime.*"

The following table show the DSTRI scores of the US, EU, China and India (Table 2)

Table 2 – Digital Services Trade Restrictiveness Index Scores (2024)						
Country	**Overall Score**	**Infrastructure and Connectivity**	**Electronic Transactions**	**Payment Systems**	**Intellectual Property Rights**	**Other barriers affecting trade in digitally enabled services**
India	0.28	0.12	0.04	0.06	0	0.07
China	0.35	0.2	0.04	0.02	0	0.09
USA	0.06	0.04	0.0	0	0	0
Austria	0.16	0.12	0.02	0	0	0.02
Belgium	0.12	0.08	0.02	0	0	0.02
France	0.1	0	0.04	0.02	0	0.04
Germany	0.08	0.04	0.02	0	0	0.02
Ireland	0.08	0.04	0.02	0	0	0.02
Italy	0.09	0	0.04	0	0	0.04
Netherlands	0.06	0	0.04	0	0	0.02
Poland	0.26	0.2	0.02	0	0	0.04
Spain	0.18	0.16	0	0	0	0.02
Sweden	0.1	0.04	0.04	0	0	0.02
UK	0.02	0	0.02	0	0	0
Source: - OECD Digital Services Trade Restrictiveness Index | Market openness Indicators						

From the above table we can see that, China has the highest score followed by India. The scores of other countries are considerably less. However, a few years ago, India used to score more than China and had the highest score for all the 44 countries covered in this index, primarily because of infrastructure and connectivity limitations. Now, in the overall Index, India has improved its ranking from highest score to fourth highest with China being the most restrictive.

The primary challenge India faces lies in insufficient infrastructure and connectivity. In this area, India's score is now 0.12 whereas earlier it was at 0.20 (2021), which shows improvements made in this area.

India's policy space is also notably more open compared to China, a fact underscored by the earlier industry comparisons in this report.

In China, the digital economy is predominantly dominated by domestic giants, whereas India's market is significantly influenced by foreign companies across various sectors. Examples include video and music streaming (Netflix, Amazon Prime, Hotstar, YouTube, YouTube Music, Spotify), e-commerce (Amazon, Flipkart), eBooks (Amazon Kindle), and social media (Facebook, Instagram, WhatsApp). China's heavily regulated environment, coupled with government subsidies for domestic firms, creates an unequal playing field that limits the ability of foreign companies to compete and enabling domestic players to thrive. Conversely, India's relatively open approach fosters a more competitive environment for global firms.

Information gathered from both the 'Digital Trade Integration Project' (Annexure 1) and the OECD Digital Trade Restrictiveness Index show that both India and China impose restrictive policies on digital trade and cross-border data flows, but the extent and mechanisms of their restrictions differ. China enforces broad data localisation requirements through laws like the Cybersecurity Law (2017) and Outbound Data Transfer Security Assessment Measures (2022), while India has more sector-specific rules, such as those for payment data. Both countries refrain from joining binding international agreements on cross-border data flows, making them equally restrictive in this area. However, China is more restrictive regarding internet access, content control and the operation of foreign firms, with stringent regulations like the Telecommunications Regulations and the Golden Shield Project. India's restrictions are more focused on data residency for specific sectors and do not include such broad content controls. China's policies, such as mandatory source code access under the National Security Law (2015), are more restrictive than India's balanced approach to intellectual property.

While India's restrictions often stem from a lack of comprehensive policies and enforcement mechanisms, China's are driven by deliberate strategies to prioritise national security and domestic industry. China's measures are systematically enforced, using surveillance frameworks and strict content control, while India faces barriers due to weak enforcement and a focus on domestic sovereignty. Based on both policy restrictions and the OECD Digital Services Trade Restrictiveness Index data, China is more restrictive overall. While India's trade

environment is constrained by infrastructure issues in which it has made considerable improvements and where it now scores better than China, China's policies create a more controlled and isolated digital trade environment, limiting foreign participation and cross-border data flows.

Digital Trade Policy Spectrum

Having examined the various provisions adopted by different countries in their respective FTAs across key thematic areas, it is now possible to position the United States, the European Union, China, and India along a regulatory spectrum. This spectrum ranges from left to right, reflecting an increasing degree of restrictiveness and a progressively more closed market structure. The far left represents the most liberal and open approach to digital trade, while the far right signifies the most restrictive stance, characterised by greater regulatory control and limited market openness.

United States Most Liberal and Market-Oriented

The United States consistently occupies the far-left position across most regulatory dimensions, embodying a market-driven and innovation-oriented digital trade regime.

1. Customs Duties on E-Commerce: The US supports a permanent moratorium on customs duties for electronic transmissions, though its FTAs include softer, non-binding commitments compared to the EU's.
2. Personal Data Protection: The absence of a comprehensive federal data protection law creates a flexible environment for digital trade, though it leads to fragmented privacy regulations across states.
3. Cross-Border Data Transfer: The US advocates unrestricted cross-border data flows to promote innovation and global competitiveness, with recent scrutiny arising mainly from national security concerns.
4. Data Localisation: The US strongly opposes data localisation mandates, favouring free data flows while ensuring regulatory access through disclosure obligations rather than storage requirements.
5. Protection and Non-Discrimination of ICT Products: The US upholds strict non-discrimination principles in its trade agreements, ensuring open market access and equal treatment of foreign digital products.

6. Source Code and IPR: US trade agreements impose hard legal obligations prohibiting forced disclosure of source code, reinforcing strong intellectual property protection and safeguarding proprietary technology.

Collectively, these policies position the US as the most liberal and open digital economy, with an emphasis on innovation, private sector leadership and minimal regulatory interference.

European Union – Liberal but Regulation-Intensive

The European Union lies slightly right of the United States on the spectrum. It combines liberal digital trade principles with stringent data protection and regulatory oversight, seeking to balance open markets with consumer and privacy safeguards.

1. Customs Duties on E-Commerce: The EU advocates a permanent moratorium, enshrining duty-free digital trade as a legally binding obligation in its FTAs.
2. Personal Data Protection: The EU's General Data Protection Regulation (GDPR) represents one of the most comprehensive privacy regimes globally, prioritising data protection over commercial flexibility.
3. Cross-Border Data Transfer: The EU permits international data transfers only when adequate privacy standards are ensured, exemplified by mechanisms such as adequacy decisions and standard contractual clauses.
4. Data Localisation: The EU explicitly prohibits data localisation requirements in its trade agreements, maintaining free data movement within and outside the bloc, subject to privacy safeguards.
5. Protection and Non-Discrimination of ICT Products: The EU upholds non-discriminatory treatment of digital products, mirroring the US stance but accompanied by higher regulatory transparency obligations.
6. Source Code and IPR: While prohibiting mandatory source code disclosure, the EU allows limited exceptions for regulatory transparency and competition oversight, ensuring accountability for dominant digital platforms.

The EU's position reflects a regulatory equilibrium – liberal in trade orientation but interventionist in consumer protection and data governance.

India – Moderately Restrictive with Developmental Emphasis

India occupies a position between the centre and right of the spectrum. Its digital trade policy balances liberalisation with strategic regulatory control, driven by concerns over revenue loss, data sovereignty and cybersecurity.

1. Customs Duties on E-Commerce: India maintains only a temporary commitment to the WTO moratorium and has repeatedly opposed its extension, arguing for tariff flexibility to safeguard developing economies.
2. Personal Data Protection: India's data protection laws resemble the EUs in structure but suffer from weak enforcement, infrastructural challenges and fragmented regulatory capacity.
3. Cross-Border Data Transfer: India imposes increasing restrictions, particularly for sensitive sectors such as finance and payments, reflecting growing concerns over digital sovereignty and security.
4. Data Localisation: India's policy mandates local storage for critical and financial data, aiming to ensure regulatory oversight and security, though discussions on adopting flexible, partner-based exceptions continue.
5. Protection and Non-Discrimination of ICT Products: India adopts a relatively liberal approach in practice, allowing open competition, though its FTAs lack explicit non-discrimination clauses comparable to those of the US or the EU.
6. Source Code and IPR: While India recognises intellectual property protection, procedural inefficiencies and limited commitments in trade agreements weaken enforcement, creating uncertainty for digital firms.

Overall, India's regulatory approach reflects a development-oriented digital trade model – cautious liberalisation tempered by strong policy autonomy and an emphasis on national interest.

China – Most Restrictive and State-Controlled

China occupies the far-right end of the spectrum, reflecting the most restrictive and state-controlled approach to digital trade. Its policies are grounded in national security, state sovereignty and industrial policy objectives.

1. Customs Duties on E-Commerce: Although China adheres to the WTO moratorium, it preserves the right to impose tariffs under domestic and bilateral frameworks, ensuring full policy flexibility.

2. Personal Data Protection: China's data governance laws prioritise state access and control over privacy, effectively transforming data protection into a tool of state oversight.
3. Cross-Border Data Transfer: Among the strictest globally, China's laws require government approval for outbound data transfers and mandate extensive security reviews.
4. Data Localisation: China mandates local storage of critical data and ensures state access to both personal and corporate information, embedding localisation in its national cybersecurity framework.
5. Protection and Non-Discrimination of ICT Products: China enforces protectionist policies that privilege domestic firms through licensing requirements, censorship laws, and content restrictions.
6. Source Code and IPR: Chinese regulations require disclosure of proprietary software and grant extensive government access, undermining trade secret protection and creating barriers for foreign digital firms.

China's regulatory framework represents a state-centric model, where digital trade is subordinated to domestic industrial policy, cybersecurity imperatives and political control.

Reason to Regulate for India:

India's approach to regulating digital trade reflects a deliberate attempt to balance economic growth, consumer welfare, security imperatives and international competitiveness. Each area of regulation ranging from customs duties on e-commerce to data governance and intellectual property reveals the tension between liberalisation and the preservation of domestic policy space.

1. The debate over customs duties on electronic transmissions centres on two main objectives: revenue generation and domestic competitiveness. Imposing such duties could enable the government to tax foreign firms supplying digital products to Indian consumers, boosting fiscal revenues and granting domestic competitors a relative advantage. However, the drawbacks are significant. Many Indian firms rely on foreign digital tools (such as cloud computing or software) as essential inputs. Taxing these would raise production costs, reduce profitability and weaken their global competitiveness. Moreover, the risk of retaliatory tariffs from developed countries – particularly given recent trade conduct by the United States – could further harm Indian

exporters. In light of these potential downsides, continuing the current moratorium on e-commerce duties, without making it permanent, is considered the most prudent course. This approach preserves India's flexibility to reassess its tariff policy as the digital economy evolves.

2. Regulation of personal data serves two overarching goals: consumer welfare and national security. The European Union's adequacy framework underscores that only countries with strong privacy safeguards can freely exchange personal data with the EU. India's Digital Personal Data Protection Act, 2023, is an important step toward meeting these standards. Nevertheless, India's laws still allow government access to personal data for security purposes, an element that may hinder its recognition as "data adequate." The absence of such status imposes compliance burdens on Indian firms serving EU consumers, as they must store data within the EU or in an approved jurisdiction. Strengthening India's privacy protection and establishing transparent judicial oversight for government access could enhance India's global credibility, reduce compliance costs for firms and facilitate cross-border trade in digital services.
3. Restrictions on cross-border data transfers typically relate to security, consumer protection and competitive equity. Developed economies, such as the EU and the UK, advocate unrestricted data flows in their FTAs. However, India maintains reservations about binding commitments that could limit its regulatory autonomy. India's cautious stance reflects legitimate concerns about safeguarding sensitive data and protecting domestic businesses from data asymmetries with large multinational firms. The current policy of allowing cross-border data transfer without committing to its permanence in trade agreements offers India the flexibility to respond to evolving technological and geopolitical realities, ensuring both openness and policy sovereignty.
4. Data localisation policies are closely tied to data protection, consumer welfare and security. Mandatory localisation may enhance government oversight and protect citizens' data from foreign surveillance. However, it also imposes high compliance costs on both foreign and domestic firms, potentially deterring investment and innovation. The environmental consequences are equally noteworthy: local data centres require continuous energy supply, which, in India's current energy mix dominated by fossil fuels, could increase carbon emissions and jeopardise progress toward net-zero commitments by 2070. A hybrid model, therefore, is preferable, allowing companies operational flexibility to store data globally, subject to strong protection standards and conditional government access. India could adopt an FDI-style framework, requiring

prior approval only for data transfers involving firms from countries with strategic sensitivities.

5. Encryption and data security regulations intersect with consumer trust, competition and national security. Under India's telecom and IT laws, the government possesses powers to compel decryption for reasons of public order or security. However, unchecked use of such power's risks undermining privacy and eroding trust in digital services. Strong encryption safeguards are essential to ensure fair competition and maintain consumer confidence. Weakening encryption or mandating traceability could disadvantage smaller firms and impede digital adoption. A balanced regulatory framework, requiring judicial oversight or court authorisation for government access to encrypted communications, would align India's security imperatives with international norms while preserving user trust and market integrity.
6. Source code protection is fundamental to innovation, investment confidence and digital competitiveness. Compelling companies to disclose proprietary source code as a market access condition would discourage foreign participation, restrict technology transfer and dampen domestic innovation. Such policies could also lead to forgone tax revenues and reduced investor confidence. India has prudently refrained from imposing such disclosure mandates, reinforcing its reputation as a trustworthy trade partner. To consolidate this position, India should formally commit to source code protection in future trade agreements, ensuring predictability for investors while retaining the right to access software code in narrowly defined security-related circumstances.

Across all six domains, India's regulatory rationale reflects a balanced developmental approach – one that seeks to harmonise openness with control, innovation with sovereignty, and economic opportunity with strategic prudence.

Rather than aligning fully with the liberal regimes of the United States or the European Union, or the restrictive model of China, India's position is pragmatically centrist: it preserves policy flexibility to adapt to the fast-evolving digital landscape while incrementally aligning with international standards to strengthen its position in global digital trade.

Recommendations for India

India's approach to digital trade regulation has been a balancing act between openness and strategic protectionism. While it has allowed foreign firms to operate freely in many sectors, regulatory restrictions, data localisation mandates and enforcement gaps have created barriers

to digital trade and innovation. Given the global landscape, India must refine its policies to enhance competitiveness while safeguarding national security and economic interests.

1. **Strengthen Commitments to Non-Discriminatory Digital Trade**: Unlike China, which actively restricts foreign digital firms, India has maintained an open market for e-commerce, social media and streaming platforms. However, lack of clear commitments in trade agreements creates policy uncertainty. To foster greater investment and innovation, India should formalise its commitment to non-discriminatory treatment of digital products in trade agreements while ensuring fair competition and consumer protection.
2. **Reassess Data Localisation and Cross-Border Data Transfer Policies**: India's strict data localisation mandates, particularly in finance and payments, stem from concerns over cybersecurity and national security. However, these measures increase compliance costs and restrict global data flows, potentially hindering India's digital services exports and AI development. India should consider more flexible agreements with trusted partners, ensuring data mobility while maintaining security safeguards and jurisdictional access for cybercrime investigations.
3. **Maintain a Cautious Stance on Customs Duties on Electronic Transmissions**: While India has advocated ending the WTO moratorium on e-commerce tariffs, empirical studies suggest that the revenue potential is minimal and the complexity of distinguishing between digital carriers and content will impose high compliance costs. A data-driven approach, collecting accurate revenue estimates, and evaluating implementation feasibility would allow for a more informed decision in the future.
4. **Improve Intellectual Property and Source Code Protection**: India does not mandate government access to the source code, unlike China, but lack of strong enforcement mechanisms and procedural inefficiencies remain challenges for digital businesses. Strengthening trade secret protection, expediting patent approvals and ensuring fair regulatory treatment will enhance India's attractiveness as a global technology hub.
5. **Strengthen Enforcement and Digital Infrastructure**: India's biggest challenge is not necessarily overregulation, but rather weak enforcement and digital infrastructure limitations. To maximise the benefits of an open digital economy, India should focus on the following:
    - enhancing cybersecurity capacity to protect personal data and combat digital fraud

- investing in digital infrastructure to close connectivity gaps and improve service reliability
- ensuring regulatory consistency to reduce uncertainty for businesses and investors.

Conclusion

The digital trade policies adopted by the United States, the European Union, China, and India reflect distinct regulatory philosophies, each shaping the structure and competitiveness of their digital industries. The United States follows a market-driven, liberal approach, enabling its corporations to scale rapidly and dominate global markets across sectors such as e-commerce, software, financial services, AI and cloud computing. The absence of heavy regulatory constraints has fostered an environment where both established firms and start-ups can thrive, contributing to the dominance of American digital giants worldwide.

The European Union prioritises consumer protection, privacy and regulatory oversight, maintaining a balanced but restrictive framework for digital trade. While strong data protection laws and non-discriminatory principles have safeguarded consumer rights, they have also increased the compliance burden on businesses, limiting the emergence of large, globally dominant digital firms. As a result, the EU has fewer homegrown digital giants compared to the US and China, with its digital market significantly influenced by foreign corporations.

China, in contrast, has deliberately restricted foreign competition and heavily subsidised domestic firms, allowing Chinese digital companies to dominate their home market. This state-controlled approach, characterised by data localisation mandates, restrictions on content and government oversight has enabled the rise of tech giants in e-commerce, AI, gaming and social media. While initially focused on domestic growth, Chinese firms have increasingly expanded internationally, challenging US firms in areas such as AI and digital platforms.

India, while maintaining a largely open digital market, has faced challenges due to regulatory inconsistencies, weak enforcement and infrastructure limitations. Unlike China, India does not impose systematic barriers on foreign firms, allowing international platforms to dominate sectors like e-commerce, video streaming and social media. However, regulatory policies in certain areas such as data localisation and financial services have restricted foreign competition while fostering domestic innovation. Despite the absence of global-scale digital giants, India's

digital economy continues to grow, with opportunities in fintech, AI and cloud computing poised to shape its future role in global digital trade.

These varying policy choices illustrate the trade-offs between market openness, regulatory oversight and domestic industry growth. While the US champions unrestricted digital trade, the EU prioritises regulatory balance, China enforces strategic protectionism, and India navigates a hybrid approach. As digital trade expands, the ability of each economy to adapt its regulatory frameworks, foster innovation and integrate into global markets will determine its long-term success in the evolving digital economy.

References:

- International Monetary Fund, Organisation for Economic Co-operation and Development, United Nations Conference on Trade and Development, and World Trade Organization, Handbook on Measuring Digital Trade, 2nd ed. (Geneva: World Trade Organization, 2023), https://www.wto.org/english/res_e/booksp_e/digital_trade_2023_e.pdf
- Pritam Banerjee, Vartul, Saptarshee Mandal, and Divyansh Dua, "Negotiating for Digitally Delivered Services — Framework for a Comprehensive Approach," CRIT/CWS Working Paper No. 82 (Centre for WTO Studies, Centre for Research in International Trade, Indian Institute of Foreign Trade, March 26, 2025), https://wtocentre.iift.ac.in/workingpaper/CWS_WorkingPaper_82.pdf
- Organisation for Economic Co-operation and Development, Of Bytes and Trade: Quantifying the Impact of Digitalisation on Trade, OECD Digital Economy Papers (Paris: OECD Publishing, 2019), https://www.oecd.org/en/publications/of-bytes-and-trade-quantifying-the-impact-of-digitalisation-on-trade_11889f2a-en.html
- Digital Empires: The Globalization of New Worlds, 2023 ed. (Oxford: Oxford University Press), https://global.oup.com/academic/product/digital-empires-9780197649268?cc=&lang=en&
- Bureau of Economic Analysis, "U.S. Digital Economy: New and Revised Estimates, 2017–2022," Survey of Current Business, December 6, 2023, https://apps.bea.gov/scb/issues/2023/12-december/1223-digital-economy.htm
- World Trade Organization, "Joint Statement Initiative on E-Commerce," accessed September 29, 2025, https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm
- Congressional Research Service, Digital Trade and Data Policy: Key Issues Facing Congress, CRS Report IF12347 (Washington, DC: Congressional Research Service, 2023), https://crsreports.congress.gov/product/pdf/IF/IF12347
- Meghna Bal and Niharika, A Primer on India's Digital Trade Policy (New Delhi: Friedrich-Ebert-Stiftung India Office, April 2023), https://library.fes.de/pdf-files/bueros/indien/20262.pdf
- Joshua Levine, Tom Lee, and Nicolo Pastrone, "Non-tariff Digital Trade Barriers," American Action Forum, November 14, 2023,

https://www.americanactionforum.org/insight/non-tariff-digital-trade-barriers/#ixzz8YP64MqbJ

- Office of the United States Trade Representative, "Indo-Pacific Economic Framework for Prosperity (IPEF)," accessed September 29, 2025, https://ustr.gov/trade-agreements/agreements-under-negotiation/indo-pacific-economic-framework-prosperity-ipef
- Office of the United States Trade Representative, 2025 National Trade Estimate Report on Foreign Trade Barriers, March 2025, https://ustr.gov/sites/default/files/files/Press/Reports/2025NTE.pdf
- China Academy of Information and Communications Technology, "China's Digital Economy Hits $7.1 Trillion: White Paper," *State Council Information Office of the People's Republic of China*, July 30, 2022, https://english.www.gov.cn/archive/statistics/202207/30/content_WS62e515e6c6d02e533532eb06.html
- Yi Wu, "Understanding China's Digital Economy: Policies, Opportunities, and Challenges," *China Briefing*, August 11, 2022, https://www.china-briefing.com/news/understanding-chinas-digital-economy-policies-opportunities-and-challenges/
- Ropes & Gray LLP, "China's New Rules on Cross-Border Data Transfers: Key Highlights," *Ropes & Gray Insights*, April 5, 2024, https://www.ropesgray.com/en/insights/viewpoints/102j4i1/chinas-new-rules-on-cross-border-data-transfers-key-highlights
- Daniel Wagner, "The Global Implications of China's National and Cyber Security Laws," *Diplomatic Courier*, August 7, 2020, https://intpolicydigest.org/the-global-implications-of-china-s-national-and-cyber-security-laws/
- European Commission, *Building a Data Economy — Brochure*, Shaping Europe's Digital Future (Publication, 23 September 2019), https://digital-strategy.ec.europa.eu/en/library/building-data-economy-brochure
- Badri Narayanan Gopalakrishnan et al., *The Impact of Cross-Border Digital Transmissions on the MSME Sector in India and the Benefits of the WTO E-Commerce Moratorium* (IGPP, June 2023), https://igpp.in/wp-content/uploads/2023/06/The-Impact-of-Cross-Border-Digital-Transmissions-on-the-MSME-Sector-in-India-and-the-Benefits-of-the-WTO-E-Commerce-Moratorium-.pdf

- Jennifer ThankGod, "Revolutionizing Digital Trade with Artificial Intelligence: Streamlining Processes and Breaking Barriers," SSRN Paper (March 1, 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4858782
- Organisation for Economic Co-operation and Development, *Recommendation of the OECD Council on Digital Security of Critical Activities (OECD-LEGAL-0449)*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449
- NITI Aayog, AI for Viksit Bharat: The Opportunity for Accelerated Economic Growth
- Janos Ferencz, Javier López González, and Irene Oliván García, "Artificial Intelligence and international trade: Some preliminary implications," OECD Trade Policy Papers No. 260 (Paris: OECD Publishing, 2022), https://www.oecd.org/en/publications/artificial-intelligence-and-international-trade_13212d3e-en.html
- United States Trade Representative, *Agreement between the United States of America and Japan concerning Digital Trade*, signed October 7, 2019, https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf
- World Trade Organization, *Notification under paragraph 2(a) of Article 31bis of the TRIPS Agreement or paragraph 2(a) of the 2003 Decision*, IP/N/9/ (WTO, [date]), https://docs.wto.org/dol2fe/Pages/FE_Browse/FE_B_009.aspx?TopLevel=10785
- Hosuk-Lee Makiyama and Badri Narayanan, *The Economic Losses from Ending the WTO Moratorium on Electronic Transmissions*, ECIPE Policy Brief No. 3/2019 (European Centre for International Political Economy, August 2019), https://ecipe.org/wp-content/uploads/2019/08/ECI_19_PolicyBrief_3_2019_LY04.pdf
- Oldroyd Steve and Lipin Ilya, US-Sales Tax and Digital Goods, BDO Global, Issue 4-2019, (2019). available at: https://www.bdo.global/en-gb/microsites/tax-newsletters/indirect-tax-news/issue-4-2019/united-states-%C2%A0sales-tax-and-digital-goods
- Organisation for Economic Co-operation and Development. (2023). *Understanding the scope, definition and impact of the WTO e-commerce moratorium (Policy Brief No. 2023/01)*. OECD Publishing. https://doi.org/10.1787/4329569a-en
- European Commission, VAT E-commerce – One Stop Shop, Pg. 2. available at https://vat-one-stop-shop.ec.europa.eu/index_en

- EY, China Officially enacts VAT law, (2025), Pg. 3. available at https://www.ey.com/en_gl/technical/tax-alerts/china-officially-enacts-vat-law-ushering-in-a-new-era-of-tax-governance
- CBEC, GST Sectoral Series-Electronic Commerce. available at: https://gstcouncil.gov.in/sites/default/files/2024-02/faq-e-commerc.pdf
- Asquith Richard, India scraps 2% equalisation levy on foreign digital service, VAT Calc, (2024). available at: https://www.vatcalc.com/india/india-2-equalisation-levy-extension-to-e-commerce-sellers-and-facilitating-marketplaces-apr-2020/
- H.R.8152 – American Data Privacy and Protection Act, (2022). available at https://www.congress.gov/bill/117th-congress/house-bill/8152#:~:text=/30/2022)-,American%20Data%20Privacy%20and%20Protection%20Act,based%20on%20specified%20protected%20characteristics
- National Security Division, Provisions Pertaining to Preventing Access to US Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, Department of Justice, Doc. No. NSD 104, (2024). available at: https://www.justice.gov/nsd/media/1382521/dl
- Pittman F. Paul, Anderson Hope, Hafiz M. Abdul, US Data Privacy Guide, White & Case, (2025). available at: https://www.whitecase.com/insight-our-thinking/us-data-privacy-guide
- S.3195 Consumer Online Privacy Rights Act, (2022). available at https://www.congress.gov/bill/117th-congress/senate-bill/3195
- Federal Register, National Security Division, Department of Justice, Final Rule – Preventing Access to US Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, (2025), Pg. 4. available at https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern
- US Department of Commerce, Data Privacy Framework Programme Launches New Website Enabling US Companies to Participate in Cross-Border Data Transfers, (2023). available at: https://www.commerce.gov/news/press-releases/2023/07/data-privacy-framework-program-launches-new-website-enabling-us
- RBI, Storage of Payment System Data, RBI/2017-18/153, (2018). available at https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11244&Mode=0

- Chiara Del Giovane, Janos Ferencz, and Javier López-González, *The Nature, Evolution and Potential Implications of Data Localisation Measures*, OECD Trade Policy Paper No. 278 (Paris: OECD Publishing, November 2023), https://www.oecd.org/en/publications/the-nature-evolution-and-potential-implications-of-data-localisation-measures_179f718a-en.html
- Creemers Rogier, Information Security Technology Guidelines for Personal Information Protection on Public and Commercial Service Information Systems, Digi China, Stanford University, (2013), pg. 9. available at https://digichina.stanford.edu/work/information-security-technology-guidelines-for-personal-information-protection-on-public-and-commercial-service-information-systems/
- Sec. 120.1, International Traffic in Arms Regulations, Title 22, Chapter 1, Subchapter M, Part. 120. available at: https://www.pmddtc.state.gov/ddtc_public/ddtc_public?id=ddtc_kb_article_page&sys_id=%2024d528fddbfc930044f9ff621f961987
- Sec. 730.1, Export Administration Regulation, Subchapter C, Part. 730. available at: https://www.govinfo.gov/content/pkg/CFR-2012-title15-vol2/pdf/CFR-2012-title15-vol2-subtitleB-chapVII-subchapC.pdf

About the Authors

	**Mr. Shivang Mishra** is a Legal Research Fellow at the Centre for WTO Studies, where he focuses on Digital Trade aspect of international Trade. He has participated in negotiating Digital Trade chapters for several Free Trade Agreements, including the India-UK, India-EU, and India-Australia FTAs. He earned his Master of Law (LL.M) from NALSAR University of Law, Hyderabad and his undergraduate law degree (B.A. LL.B) from the National University of Study and Research in Law, Ranchi.
	**Mr. Vikas Verma** is a Young Professional (Economics Researcher) at Centre for WTO Studies. He has expertise in international trade including Trade in Services, and Digital Trade. He holds a Master's Degree in Economics from Gokhale Institute of Politics and Economics and BA (Hons) Economics from Vivekananda Institute of Professional Studies (VIPS), GGSIPU.
	**Mr. Vartul Srivastava** is a legal consultant at DPIIT, Ministry of Commerce & Industry. He has negotiated several trade agreements, including the IN-NZ FTA, IN-EU FTA, and IN-Chile FTA.
	**Dr. Pritam Banerjee** is the Head of the Centre for WTO Studies (CWS) at the Centre for Research in International Trade (CRIT), Indian Institute of Foreign Trade (IIFT), New Delhi, where he leads advisory efforts on trade remedies and policy space. With over 15 years of experience in economic policy and trade facilitation, he has previously served as a Consultant with the Asian Development Bank (ADB) and as Senior Director for Public Policy at Deutsche Post DHL Group, overseeing the South Asia region. He has also led Trade Policy at the Confederation of Indian Industry (CII) and worked with the World Bank. Dr. Banerjee has been a member of the National Council for Trade Facilitation (2016-2023) and a special invitee to the Committee on Ease of Doing Business Reforms under the Ministry of Commerce. He holds a PhD in Public Policy from George Mason University and a Master's in Economics from Jawaharlal Nehru University. He has published extensively on international trade, regional integration, and logistics.

Annexure I – Digital Trade Integration Project

Policy actions from the 'Digital Trade Integration Project' showing the various policies and laws adopted by the US, the EU, China and India for the countries under consideration.

The stance adopted by the four countries/region on different elements of the major aspects of digital trade are discussed below.

Personal Data Protection

USA

Sub Pillar	**Policies**
Requirement to allow the government to access personal data collected	Directive No. 3340-049a. Since January 2018 Under Directive No. 3340-049a of 2018, the US Customs and Border Protection (CBP) has broad powers to conduct device searches and requires travellers to provide their device passwords to CBP agents. Section 5.3.1 provides that "travellers are obligated to present electronic devices and the information contained therein in a condition that allows inspection of the device and its contents. If presented with an electronic device containing information that is protected by a passcode or encryption or other security mechanism, an officer may request the individual's assistance in presenting the electronic device and the information contained therein in a condition that allows inspection of the device and its contents." It is reported that CBP officers have compelled American citizens to unlock and hand over their phones, even after being told that the

	phone contained sensitive data. The directive also includes a provision that allows officers to examine a phone with external equipment if there is a "national security concern" (Section 5.1.4). It has horizontal coverage[78] and acts as a regulatory restriction
	Network Security Agreements. Since 1999, most recently in December 2021 Foreign communications infrastructure providers have been asked to sign network security agreements (NSAs) in order to operate in the US. These agreements ensure that US government agencies have the ability to access communication data when legally requested, often through a national security letter (NSL). NSLs do not require prior approval from a judge. The data in question can include call-identifying information, user location, call duration, start time, end time, IP addresses, location information, URLs, etc., and must be reported to the federal department in question within five business days following a request. It covers the telecommunication sector and acts as a regulatory restriction.
	Health Insurance Portability and Accountability Act (since August 1996)

[78] Horizontal coverage means the measure applies broadly across sectors or the entire economy. Vertical coverage means the measure applies only to specific sectors or services (for example, telecommunications or finance).

Requirement to perform an impact assessment (DPIA) or have a data protection officer (DPO)	The HIPAA of 2013 requires the designation of a privacy official for HIPAA-covered entities to develop and implement the policies and procedures of the entity (§ 164.530 on administrative requirements). It covers the health sector and acts as a regulatory restriction.
	E-Government Act of 2002. Since 2002 The E-Government Act of 2002, Section 208, requires agencies to conduct privacy impact assessments (PIAs) for any electronic collection and information technology (IT) systems that contain personally identifiable information (PII). It covers all federal agencies and acts as a regulatory restriction.
Framework for data protection	Lack of a comprehensive data protection law There is no comprehensive data protection law. However, there are sectoral laws, including those covering financial services, healthcare, telecommunications and education. It has horizontal coverage and acts as a regulatory restriction.
Source: Database - The Digital Trade Integration Project	

EU

Sub Pillar	Policies
Requirement to perform an impact assessment (DPIA) or have a data protection officer (DPO)	General Data Protection Regulation (Regulation 2016/679) (since April 2016, entry into force in May 2018) Since May 2018, the General Data Protection Regulation (GDPR) requires that organisations conducting "regular and systematic monitoring of data subjects on a large scale" or whose activities include the processing of sensitive personal data on a large scale must appoint a data protection officer (DPO). Previously, only European institutions and bodies were required to appoint a DPO, with some member states imposing such requirements on private companies too. In addition, under the GDPR, data protection impact assessments (DPIAs) are mandatory for data processing activities likely to generate high risk to the rights and freedoms of natural persons. It has horizontal coverage and acts as a regulatory restriction
Framework for data protection	General Data Protection Regulation (Regulation 2016/679) (since April 2016, entry into force in May 2018) The European Union General Data Protection Regulation (GDPR), which entered into force in 2018, considerably

	expands the scope of EU privacy rules. In addition to companies established in the EU, the regulation applies extraterritorially to companies offering goods or services to data subjects in the EU and companies that monitor the behaviour of EU citizens (Article 3). In addition, there is complementary legislation, Directive (EU) 2016/680, on the protection of natural persons regarding processing of personal data connected with criminal offences or the execution of criminal penalties, and on the free movement of such data. It has horizontal coverage and acts as an enabling measure
Source: Database - The Digital Trade Integration Project	

China

Sub Pillar	**Policies**
Requirement to allow the government to access personal data collected	People's Republic of China State Council Decree No. 292 – Internet Information Service Management Measures (since September 2000) According to Article 14 of Decree No. 292, ISPs are required to provide user information to the authorities upon request, without judicial oversight or transparency.

	It covers internet service providers and acts as a regulatory restriction
	Counterterrorism Law of the People's Republic of China (since December 2015, entry into force in January 2016) Article 18 of the Counterterrorism Law requires internet service providers and the telecommunication sector to "provide technical support and assistance, such as technical interface and decryption, to support the activities of the public security and state security authorities in preventing and investigating terrorist activities." It covers internet service providers and telecommunication sector and acts as a regulatory restriction
	Provisions for the Supervision and Inspection of Network Security by Public Security Agencies (since September 2018) The provisions authorise local law enforcement agencies to conduct remote or onsite inspections of the businesses under their supervision. Inspections must be aimed at ensuring compliance with general regulatory obligations on all businesses under the Cybersecurity Law or specific obligations applicable to internet service providers, including, but not limited to, the implementation of technical measures for network security and data protection that

	comply with national standards. During such an inspection, law enforcement agencies can physically enter business sites, machine rooms, review and copy relevant information, and assess the operational conditions and effectiveness of the technical measures taken by the company to safeguard the security of networks and information. It covers internet service providers and acts as a regulatory restriction.
	State Security Law (since February 1993) and Counterespionage Law (since November 2014) There are two articles in the State Security Law that permit state security organs to agree to demand, when necessary, to any information or data held by anyone in China. Article 11 stipulates that 'where state security requires, a state security organ may inspect electronic communication instruments and appliances and other similar equipment and installations belonging to any organisation or individual'. Article 18 states: 'When a State security organ investigates and finds any circumstances endangering State security and gathers related evidence, citizens and organisations concerned shall faithfully furnish it with relevant information and may not refuse to do so".

	The Counterespionage Law, which repealed the State Security Law, provides for state security organ personnel to gain entry to restricted regions, venues or units and to inspect, read or collect relevant archives, materials or items. Such access is permitted on the basis of relevant national regulations and upon approval and presentation of appropriate documents. Further, state security organ personnel can also check electronic communication tools, equipment and facilities in accordance with the regulations. It has horizontal coverage and acts as a regulatory restriction.
	Data Security Law of the People's Republic of China (since June 2021, entry into force in September 2021) Article 35 of the Data Security Law stipulates that where public security or national security authorities need to consult any data in order to safeguard national security or investigate a crime, the relevant organisations and individuals must provide such data. The same article stipulates that before getting access to the data held by private organisations, public security or national security authorities must go through strict approval formalities in advance. It has horizontal coverage and acts as a regulatory restriction.

Requirement to perform an impact assessment (DPIA) or have a data protection officer (DPO)	Cybersecurity Law (since June 2017)Article 21 of the Cybersecurity Law requires network operators to appoint persons in charge of cybersecurity. Critical information infrastructure operators (CIIO) are also required to set up specialised security management bodies and persons responsible for security management. Further, CIIOs must conduct security background checks on responsible persons and personnel in critical positions. It has horizontal coverage and acts as a regulatory restriction.
	Guidelines for Personal Information Protection within Public and Commercial Services Information Systems (since November 2012, entry into force in February 2013). The Personal Protection Law requires controllers to: - Notify data subjects that their legal representative or principal person bears overall responsibility for the security of personal data - Appoint a data security officer (this must a full-time position if the organisation deals with personal data as its main line of business and employs over 200 people, or processes personal data for more than 500,000 people) - Devise emergency plans to deal with security issues

	- Undertake security audits at least once a year - Provide training to relevant staff on data security at least once a year. It has horizontal coverage and acts as a regulatory restriction
	Amendment to the Information Security Technology – Personal Information Security Specification (GB/T 35273-2020) (since October 2020) The 2020 specification requires that personal information controllers appoint a person and a department responsible for personal information (PI) protection. The person responsible for PI protection must be someone who has relevant management experience and personal information protection expertise and is required to participate in important decisions on personal information processing activities and report directly to the principal of the organisation. It has horizontal coverage and acts as a regulatory restriction
Framework for data protection	Personal Information Protection Law (since August 2021, entry into force in November 2021) The Personal Information Protection Law (PIPL) is China's comprehensive data protection law and governs personal

	information processing activities carried out by entities or individuals within China. The PIPL introduces several important concepts, such as personal information, sensitive personal information and processing. It explicitly stipulates its extraterritorial jurisdiction and provides the traditional elements for data protection, such as principles of personal information processing, consent and non-consent grounds for processing, cross-border transfer mechanism, and rights of data subjects. It has horizontal coverage and acts as an enabling measure
Source: Database - The Digital Trade Integration Project	

India

Sub Pillar	**Policies**
Requirement to allow the government to access personal data collected	Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 The rules provide that an officer so designated by the central government under the rules (known as 'designated officer') can, on the receipt of request from any nodal officer of a government organisation or a competent court or by an order of any agency of the government, block access by the public to any information transmitted, received, stored or hosted in any computer resource. The request

	will be examined by a committee consisting of the designated officer and its chairperson and representatives, who will determine if the information must be blocked.
	Indian Telegraph Act, 1885, Telegraph Rules (since July 1885, last amended in December 2015) Pursuant to Section 5 of the Telegraph Act and the Telegraph Rules, the government has the power to temporarily possess licensed telegraphs and order the interception or disclosure of messages sent through such devices. The definition of a telegraph is fairly wide: it means any appliance, instrument, material or apparatus used (or that is capable of being used) for transmission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, visual, or other electromagnetic emissions, radio waves or Hertzian waves, or galvanic, electric, or magnetic means. It is not clear whether a court order is required to access the data. It has horizontal coverage and acts as a regulatory restriction
	Department of Telecommunications, Ministry of Communications & IT, Government of India, Licence Agreement for Provision of - internet services - unified access services after migration from CMTS - basic telephone services

	Under the Agreement for Provisions of internet services, ISP licence holders must maintain a log of all users connected to the service they are using and outward logins through an ISP's computer, which must be made available to the Telecom Authority at all times. ISP licence holders must also provide to authorised intelligence agencies at any time a complete list of subscribers on the ISP website with password-controlled access. A complete list of the records that must be maintained and provided for security purposes to authorities is set out in the link. ISPs are regulated and operate under a licence issued under the Telegraph Act, 1885. Under the Telegraph Act, any interception of messages may only be carried out pursuant to a written order by an officer specifically empowered for this purpose by the state or central government. The officer must be satisfied that it is necessary or expedient to do so in the interests of the security and sovereignty of India. However, such a requirement appears to be only for interception of messages and not for storage of subscriber related information. The CMTS and the BTS Licences identify several categories of records that must be made available and provided for security purposes to the Telecom Authority or authorised intelligence agencies. For example, under the BTS licence, a designated person from the central/state government has

	the right to monitor the telecommunication traffic in every switch and any other point in the network set up by the telecommunication service provider (TSP). Further, TSPs are required to make arrangement for monitoring and simultaneous calls by government security agencies at the location desired by the central/state government. Along with the monitored calls, the following records should be made available: (i) called/calling party numbers (ii) time/date and duration of interception (iii) precise location of target subscribers (iv) subscriber numbers, if any call-forwarding feature has been invoked by the target subscriber and (v) data records for even failed call attempts. Since the BTS is provided under the aegis of the Telegraph Act, any conditions related to interception pursuant to an order of an officer of the state/central government may apply here. It covers internet service providers and acts as a regulatory restriction
	Information Technology Act, 2000 Section 69 of the Information Technology Act 2000, as amended by the Information Technology (Amendment) Act, 2008, gives the central and state governments the power to direct any agency to intercept, monitor or decrypt, or cause to be intercepted, monitored or decrypted, any information transmitted, received or stored through any computer resource. The government must be satisfied

	that this is necessary in the interest of the sovereignty, security or defence of India. The government may require any subscriber or intermediary or any person in charge of the computer resource to extend all facilities and technical assistance necessary to decrypt the information. It has horizontal access and acts as a regulatory restriction.
Requirement to perform an impact assessment (DPIA) or have a data protection officer (DPO)	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 Under Rule 4 of the Information Technology Rules of 2021, a "significant" social media intermediary (defined as a social media intermediary with more than 5,00,000 registered users in India) must appoint a Chief Compliance Officer who must ensure compliance with the rules and will be liable in any proceedings relating to any relevant third-party information, data or communication link made available or hosted by that intermediary where he/she fails to ensure that such intermediary observes due diligence while discharging its duties under the rules. It covers significant social media intermediaries and acts as a regulatory restriction.
Framework for data protection	India does not have a comprehensive data protection law

	However, it has sectoral laws on data protection applicable to internet service providers, telecom service providers, banking information and certain corporate entities. For internet service and telecom service providers, the requirements are set out in the internet service provider licence and the unified access services licence respectively; for banking information, data protection requirements are set out in the Prevention of Money Laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005. It has horizontal coverage in certain service providers such as internet service providers, telecom service providers, certain corporate entities, banking information and banks acts as a regulatory restriction.
Source: Database - The Digital Trade Integration Project	

Cross-border Data Transfer

USA

Sub Pillar	Policies

Participation in trade agreements committing to open cross-border data flows	Agreement between the United States of America and Japan Concerning Digital Trade (since October 2019, entry into force in 2020) United States-Mexico-Canada Agreement (since November 2018, entry into force in July 2020) In both these agreements, the United States has binding commitments to open transfers of data across borders. This comes under Article 11 in the US-Japan agreement and in Article 19.11 in the US-Mexico-Canada agreement. It has horizontal coverage and acts as an enabling measure
Ban on transfer and local processing requirement	Code of Federal Regulations (since August 2015, last amended in October 2021) Federal Risk and Management Program Control Specific Contract Clauses (since December 2017) Pursuant to the Code of Federal Regulations (§239.7602-2 of Part 239 of Chapter 2 of Title 48), cloud computing service providers to the US Department of Défense (DoD) may be required to store data relating to the DoD within the US. The service provider's authorising official may authorise storage of such data outside the US, but this will ultimately depend on the sensitivity of the data in question. Similarly, Section 2.1 of the Federal Risk and Management Program (FedRAMP) Control Specific Contract

	Clauses require agencies with 'specific data location requirements' to include contractual obligations identifying where 'data-at-rest […] shall be stored'. It covers the public sector and acts as a regulatory restriction.
Local storage requirement	Network Security Agreements (since October 1999) The United States has not adopted laws or regulations requiring that data be stored locally in the United States. Nevertheless, in some cases Team Telecom – an informal grouping of the Departments of Defence, Homeland Security and Justice, and the Federal Bureau of Investigation – imposes requirements to store data locally in security agreements and assurances letters as a condition for the grant of a licence or consent for a merger or acquisition. In such cases, Team Telecom may require that such data be stored only in the United States, or that copies of such data be made available in the United States. It covers the telecommunications sector and acts as a regulatory restriction
Source: Database - The Digital Trade Integration Project	

EU

Sub Pillar	**Policies**

Conditional flow regime	General Data Protection Regulation (Regulation 2016/679) (since April 2016, entry into force in May 2018) "The EU's General Data Protection Regulation (GDPR) considerably expands the scope of EU privacy rules. In addition to companies established in the EU, the regulation applies extraterritorially to companies offering goods or services to data subjects in the EU and companies that monitor the behaviour of EU citizens (Art. 3). The regulation mandates that data be allowed to flow freely outside the European Economic Area (EEA) only in certain circumstances listed in Chapter 5 of the regulation. The main conditions for such a transfer are the following: the recipient jurisdiction has an adequate level of data protection; the controller ensures adequate safeguards (for instance, by using model contract clauses, binding corporate rules or other contractual arrangements); the data subject has given his/her consent explicitly and the transfer is necessary for the performance of a contract between the data subject and the controller. The GDPR allows for data transfers to countries whose legal regime is deemed by the European Commission to provide for an "adequate" level of personal data protection. The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands,

	Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, the Republic of Korea, Switzerland, the United Kingdom, and Uruguay as providing adequate protection. In addition, the EU-US Data Privacy Framework acts as a self-certification system open to certain US companies for data protection compliance since July 2023. It has horizontal coverage and acts as a regulatory restriction.
Participation in trade agreements committing to open cross-border data flows	The European Union has joined an agreement with binding commitments to open transfers of data across borders: the Trade and Co-operation Agreement between the European Union and the European Atomic Energy Community, of the One Part, and the United Kingdom of Great Britain and Northern Ireland, of the Other Part (Art. 201). It has horizontal coverage and acts as an enabling measure.
Source: Database - The Digital Trade Integration Project	

China

Sub Pillar	**Policies**

Cross-border data policies	Amendment to the Information Security Technology – Personal Information Security Specification (GB/T 35273-2020) (since October 2020) The 2020 Specification provides that personal biometric information must not be shared or transferred unless actually essential for business needs, in which case the personal information subject must be separately informed of the purpose, types of biometrics involved, identification of the recipient and the data security capacity of the service provider; the consent of the personal information subject must be explicitly obtained (9.2.i). It has horizontal coverage and acts as a regulatory restriction
Participation in trade agreements committing to open cross-border data flows	Lack of participation in agreements with binding commitments on data flows China has not joined any agreement with binding commitments on data flows. The lack of binding commitments on data flows acts as a regulatory restriction with horizontal coverage.
Conditional flow regime	Guidelines for Personal Information Protection within Public and Commercial Services Information Systems (since November 2012, entry into force in February 2013)

	Article 5.4.5. of the Guidelines for Personal Information Protection within Public and Commercial Services Information Systems - The provision prohibits the transfer of personal data outside the country unless the data subject has given express consent or the transfer is permitted under applicable law or authorised by the government or a competent regulatory authority., in the absence of which the express consent of the subject of the personal information, or explicit legal or regulatory permission, or the absence of consent from the competent authorities. If these conditions are not fulfilled, ""the administrator of personal information shall not transfer the personal information to any overseas receiver of personal information, including any individuals located overseas or any organizations and institutions registered overseas." Although the guidelines are a voluntary technical document, they might serve as a regulatory basis for judicial authorities and lawmakers. It covers public and commercial services information systems and acts as a regulatory restriction
	Personal Information Protection Law (since November 2021) The Personal Information Protection Law (Art. 40) provides that critical information

	infrastructure operators and personal information processors handling personal information must store personal information collected and produced within the borders of China. Where such information needs to be provided abroad, they shall pass a security assessment organised by the national cyberspace department. Besides, according to Article 38, the processors of personal information must apply one of the conditions to provide information outside the PRC: passing the security assessment organised by the national cyberspace department in accordance with Article 40 of this Law; obtaining personal information protection certification from the relevant specialised institution according to the provisions issued by the national cyberspace department; concluding a contract stipulating both parties' rights and obligations with the overseas recipient in accordance with the standard contract formulated by the national cyberspace department and meeting other conditions set forth by laws and administrative regulations and by the national cyberspace department. Where a processor of personal information provides personal information outside the People's Republic of China, it is required to inform the individual of the name or names of the overseas recipient, the contact information, the purpose of processing, the

	manner of processing, the type of personal information, as well as the manner and procedure for the individual to exercise his or her rights under this law with the overseas recipient, and obtain the individual's consent (Article 39). Personal information processors shall not provide personal information stored in the People's Republic of China to foreign judicial or law enforcement agencies without the approval of the competent authorities of the People's Republic of China (Art. 41). It has horizontal coverage and acts as a regulatory restriction
Ban on transferring data and local processing requirements	Cybersecurity Law (since November 2016, entry into force in June 2017) Outbound Data Transfer Security Assessment Measures (since July 2022, entry into force in September 2022) Article 37 of the Cybersecurity Law requires "key information infrastructure" operators to store personal information and critical data within China. Personal information and critical data can be stored outside China where there is a genuine need for business; in such a case, a ""security assessment"" needs to be conducted in accordance with procedures formulated by the Cyberspace Administration of China (CAC) in collaboration with other authorities. Article 4 of the Outbound Data Transfer Security Assessment Measures, promulgated

	by the CAC, outlines four situations in which a security assessment is necessary before an outbound transfer can take place: 1) in cases where the transfer concerns “important data”, which is broadly defined as data that could endanger national security, economic operation, social stability, public health and safety 2) in case the transfer concerns personal data by a critical information infrastructure operator or processor of personal information that processed data for one million or more individuals 3) in the case of transfers concerning personal data by a personal information processor that has made outbound transfers of personal information of 100,000 individuals or sensitive personal information of 10,000 persons in the preceding year and 4) in other situations that are not further defined. Article 8 of the measures covers the factors that the CAC will take into account when undertaking a security assessment. The assessment includes a wide range of aspects; for example: - The risks that the transfer may entail for national security or public interest, among other policy objectives - Legitimacy, necessity and method of transfer - Whether the level of data protection in the recipient country meets the requirements of laws in China

	- Sensitivity of the data and risks of data being tampered with abroad - Agreed safeguard measures between the data processor and data recipient - Any other matter that the CAC deems necessary. In the case of unfavourable outcomes, the data handler can ask the CAC for a re-assessment for a final decision. In the case of a positive decision, the permission to transfer data abroad is valid for two years but if substantial changes in risk factors arise, a new assessment might be needed. It covers key information infrastructure operators and acts as a regulatory restriction.
	Telecommunications Regulations of the People's Republic of China (since September 2000, last amended in February 2016) China's Telecommunications Regulations require all data collected inside China to be stored on Chinese servers. As a result of this regulation, Hewlett Packard, Qualcomm, and Uber were required to divest more than 50 per cent of their businesses in China to Chinese companies to avoid fines. It covers telecommunication services and cloud services and acts as a regulatory restriction.
	Map Management Regulations (since December 2015, in force since January 2016)

	Online maps are required to set up their server inside of the country (Article 34 of Map Management Regulations) and must acquire an official certificate. It covers maps services and acts as a regulatory restriction
	Administrative Measures for Population Health Information (for trial implementation; since May 2014) Population health information needs to be stored and processed within China. In addition, storage is not allowed overseas (Article 10). It covers the health sector and acts as a regulatory restriction
	Interim Measures for the Administration of Online Taxi Booking Business Operations and Services (since July 2016, in force since November 2016) China instituted a licensing system for online taxi companies which requires that personal information and business data should be stored and used in mainland China and must not be transferred outside China (Article 27 of the Interim Measures for the Administration of Online Taxi Booking Business Operations and Services). Such information should be retained for two years, except when otherwise required by other laws and regulations. The measure also mandates that servers of the taxi companies should be

	set up in mainland China with a network security management system and technical measures for security protection in compliance with regulations (Article 5.2). It covers the online taxi sector and acts as a regulatory restriction.
	Yinfa No. 17 [2011], Notice of the People's Bank of China on Protecting Personal Financial Information by Banking Financial Institutions (since January 2011, entry into force in May 2011) Personal Financial Information Protection Technical Specification (since February 2020) The "Notice of the People's Bank of China on Protecting Personal Financial Information by Banking Financial Institutions" states that the processing of personal information collected by commercial banks must be stored, handled and analysed within the territory of China and such personal information is not allowed to be transferred overseas (paragraph 6). The Personal Financial Information Protection Technical Specification (PFI Specification) regulates “any personal information collected, processed and stored by Financial Institutions during the provision of financial products and services"" (PFI). The PFI specification requires that PFI collected or generated in mainland China is stored, processed and analysed within the

	territory. Further, under the PFI Specification, where there is a business need for cross-border transfer of personal financial information (PFI), the financial institution has to obtain explicit consent to the transfer from the personal financial information subjects (i.e. the persons under the PFI Specification providing the data), conduct a security assessment and then supervise the offshore recipient to ensure responsible processing, storage and deletion of PFI (Section 7.1.3)." It covers the financial sector and acts as a regulatory restriction
	Personal Information Protection Law (since November 2021) The Personal Information Protection Law (Art. 40) provides that critical information infrastructure operators and personal information processors handling personal information must store personal information collected and produced within the borders of China. Where such information needs to be provided abroad, they have to pass a security assessment organised by the State cybersecurity and information department. It has horizontal coverage and acts as a regulatory restriction
Source: Database - The Digital Trade Integration Project	

India

Sub Pillar	Policies
Participation in trade agreements committing to open cross-border data flows	Lack of participation in agreements with binding commitments on data flows India has not joined any agreement with binding commitments to open transfers of data across borders. The lack of participation in agreements with binding commitments on open data transfers act as a regulatory restriction with horizontal coverage.
Conditional flow regime	Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 Rule 7 of Information Technology Rules, 2011, states that export of sensitive personal data or information within or outside India is permissible provided that the same standards of data protection required in India are adhered to, and that transfer is necessary for the performance of a lawful contract or has been consented to by the provider of the information. Sensitive personal information includes passwords, financial information such as bank account or credit/debit card details, sexual orientation, physical or mental health condition, biometric information, etc. It has horizontal coverage and acts as a regulatory restriction

Local storage requirement	Reserve Bank of India Directive (since April 2018) In April 2018, the Reserve Bank of India (RBI) issued a one-page directive stating that all payment data held by payment companies should be held in local facilities within six months of the directive. The directive noted that this would help the RBI gain ""unfettered supervisory access"" to transaction data, which it needs to ensure proper monitoring. Following a negative response from international payment companies such as MasterCard, Visa and American Express, the RBI has proposed (in ""Frequently Asked Questions"" of its website) to ease this restriction so as to allow payment firms to store data offshore as long as a copy was kept in India. The RBI has further clarified that for cross-border transaction data consisting of a foreign component and domestic component, a copy of the domestic component may be stored abroad, if required. With respect to processing of payment transactions outside India, the RBI requires that the data must be stored only in India after processing and should be deleted from systems abroad and brought back to India no later than 24 hours after processing. Any subsequent activity, such as settlement processing after payment processing done outside India, must be undertaken on a real time basis, pursuant to which the data must be stored only in India.

	The RBI has clarified that banks, especially foreign banks, can continue to store banking data abroad but in respect of domestic payment transactions, the data must be stored only in India. It covers the financial sector and acts as a regulatory restriction.
	Insurance Regulatory and Development Authority of India (Maintenance of Insurance Records) Regulations, 2015 Insurance Regulatory and Development Authority of India (Outsourcing of Activities by Indian Insurers) Regulations, 2017 According to the Insurance Regulatory and Development Authority of India (IRDAI) Maintenance of Insurance Records Regulations, 2015 (Regulation 3(9)), "Insurers are required that [...] (ii) the records pertaining to policies issued and claims made in India (including the records held in electronic form) are held in data centres located and maintained in India." In addition, the 2017 Regulations on Outsourcing of Activities by Indian Insurers provide that Indian insurer, even in cases where they outsource their services outside India, must retain all original records in India. It covers insurance services and acts as a regulatory restriction.
	Companies (Accounts) Rules, 2014

	Rule 3(5) of the Companies (Accounts) Rules 2014 provides that if a company's books and papers (or back-ups of them) are kept electronically at any location, they must also be periodically stored on a server physically located in India. It has horizontal coverage and acts as a regulatory restriction
Ban on transferring data and local processing requirements	Request for Proposal (RFP) for Provisional Empanelment of Cloud Service Offerings of Cloud Service Providers (CSPs) (since December 2015) Guidelines for Government Departments on Contractual Terms Related to Cloud Services (since March 2017) Master Service Agreement: Procurement of Cloud Services (since October 2019) In 2015, India's Ministry of Electronics and Information Technology (MeitY) issued guidelines for a cloud computing empanelment process under which cloud computing service providers may be provisionally accredited as eligible for government procurement of cloud services. The guidelines require such providers to store all data in India to qualify for the accreditation. In addition, Section 2.1.d of the Guidelines for Government Departments on Contractual Terms Related to Cloud Services requires that any government contracts contain a

	localisation clause mandating that all government data residing in cloud storage networks is located on servers in India. Furthermore, Section 1.17.4 of the Master Service Agreement: Procurement of Cloud Services states among other things that cloud service providers must offer cloud services to the purchaser from a MeitY-enrolled data centre that is located in India; the data must be stored within India and must not be taken out of India without the explicit approval by the purchaser. It covers cloud computing services and acts as a regulatory restriction
	National Data Sharing and Accessibility Policy (since March 2012) India's National Data Sharing and Accessibility Policy requires that "non-sensitive data available either in digital or analogue forms but generated using public funds" must be stored within the borders of India. The policy states that data belongs to the "agency/department/ministry/entity which collected them and reside in their IT-enabled facility" (Section 10). It has horizontal coverage and acts as a regulatory restriction.
	Licence Agreement for Unified Licence (since March 2016) Under Condition 39.23(viii) of the Unified Licence Agreement granted by the Department

	of Telecommunications, licensees are not permitted to transfer "subscriber accounting information" (except for roaming and related billing purposes) or "user information" (except if pertaining to foreign subscribers using an Indian operator's network while roaming, and international private leased circuit subscribers) to any person or place outside India. "User information" is not defined by Indian telecommunications law and the requirements do not restrict financial disclosures imposed by statute. Condition 39.23(iii) prohibits the transfer of domestic technical network details to any place outside India. It covers the telecommunications sector and acts as a regulatory restriction.
	Public Records Act 1993 (No. 69 of 1993) (since December 1993) Section 4 of the Public Records Act states that no person shall take or cause to be taken public records out of India without the prior approval of the central government, except for an official purpose. It covers the public sector and acts as a regulatory restriction.
Source: Database - The Digital Trade Integration Project	

Data Localisation

USA

Sub Pillar	Policies
Minimum period for data retention	Network Security Agreements (since 1999, last reported in December 2021) Laws passed by the US government such as Section 214 of the Communications Act of 1934, FISA (Foreign Intelligence Surveillance Act) and Executive orders passed by the president requires that foreign communications infrastructure providers sign network security agreements (NSAs) to operate in the US. The agreements impose local storage requirements for certain customer data as well as minimum periods of data retention for data such as billing records and access logs. The agreement requires companies to maintain what amounts to an "internal corporate cell of American citizens with government clearances", ensuring that "when US government agencies seek access to the massive amounts of data flowing through their networks, the companies have systems in place to provide it securely." It covers the telecommunications sector and acts as a regulatory restriction.
Source: Database - The Digital Trade Integration Project	

China

Sub Pillar	Policies

Minimum period for data retention	Provisions for the Administration of Internet Electronic Bulletin (since November 2000) These provisions apply to electronic bulletin services. Electronic bulletin services refer to electronic bulletin boards, electronic whiteboards, electronic forums, internet chat rooms, message boards and other forms of interactive behaviour characterised by the provision of information dissemination for online customers. The electronic bulletin service provider must record all information content published in the electronic bulletin service system as well as internet access time, user account, internet address or domain name, caller's phone number and other information. Such records must be kept for 60 days and provided to the relevant state authority when inquired in accordance with the law. It covers electronic bulletin services and acts as a regulatory restriction
	Internet Surfing Service Business Venue Management Rules (since April 2001, amended in 2011, 2016 and 2019) The Internet Surfing Service Business Venue Management Rules apply to commercial venues that provide internet surfing services to the public through computers connected to the internet. Internet surfing service businesses are required to record the users' authentic ID information, relevant surfing information, record back-ups, preserve such

	information for 60 days and provide the information to relevant governmental departments who make inquires according to the law. It covers internet surfing services and acts as a regulatory restriction
	Administrative Provisions on Information Services of Mobile Internet Application Programs (since June 2016 Entry into force in August 2016) Under the provisions, mobile internet application providers in accordance with the "background real name, the front voluntary" principle, register a user based on cell phone numbers and other real identity information authentication, record user log information, and save the information for 60 days (Article 7). It covers internet app providers and mobile internet app stores and acts as a regulatory restriction.
	Interim Regulations for the Management of Network Appointed Taxi Services Operations (since November 2016, amended in 2020) China instituted a licensing system for online taxi companies that requires them to host user data and business data generated by it on Chinese servers for at least two years; the information and data cannot be exported

	unless otherwise provided by laws and regulations. It covers online taxi companies and acts a regulatory restriction
	Regulation on Internet Information Services of the People's Republic of China (since September 2000) and the Decision on Strengthening Network Information Protection (since December 2012) The Regulation on Internet Information Services of the People's Republic of China requires that internet service providers (ISPs) keep records of the time spent on online by each service user, user account, IP address or domain name, phone number and other information for 60 days and provide that information to the authorised government authorities when required (Article 14.). In addition, the Decision on Strengthening Network Information Protection requires ISPs to co-operate with the government and provide technical support upon inquiry from the authorised government authorities (Article 10). It covers internet service providers and acts as a regulatory restriction.
Source: Database - The Digital Trade Integration Project	

As per the Digital Trade Integration Project under the pillar of 'Content Access', China has the following stance on the following sub-pillars:

Sub Pillar	**Policies**
Licensing schemes for digital services and applications	Interim Measures for the Administration of Online Taxi Booking Business Operations and Services (since November 2016) China instituted a licensing system for online taxi companies that requires that the personal information and business data should be stored and used in mainland China, and must not be transferred outside China. Such information should be retained for two years, except when otherwise required by other laws and regulations. The measure also requires that servers of taxi companies should be set up in Mainland China, with a network security management system and technical measures for security protection in compliance with regulations. It covers the online taxi sector and acts as a regulatory restriction.
	Map Management Regulations (since January 2016) According to the Map Management Regulations, service providers who provide online maps are required to set up their server inside the country and must acquire an official certificate. It covers maps service and acts as a regulatory restriction.

	Provisions on the Administration of Foreign-funded Telecommunications Enterprises (2016 Revision) China's telecom laws require all foreign firms that provide data centre or cloud computing services to enter into a joint venture with a Chinese firm and obtain an internet data centre licence. It covers data centres and cloud storage services and acts as a regulatory restriction.
Source: Database - The Digital Trade Integration Project	

India

As per the Digital Trade Integration Project under the pillar of 'Domestic Data Policies', India has the following stance on the following sub-pillars:

Sub Pillar	**Policies**
Minimum period for data retention	Prevention of Money-laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification, and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005 Banking information must be stored for 10 years "from the date of cessation of the transactions between the client and the banking company, financial institution or intermediary, as the case may be".

	It covers banking companies and financial institutions and acts as a regulatory restriction.
	Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 As per SEBI Listing Regulations, a listed entity (i.e., an entity which is listed on the stock market) is required to have a policy for the preservation of documents. SEBI's listing regulations require that the records, books, papers and documents of the company be preserved as per the following classification: - Schedule I - to be preserved permanently. Documents listed under these schedules include incorporation documents, share certificates, register of minutes of board meetings, register of members, etc. - Schedule II – to be preserved for eight years. Documents listed under this schedule include the books of accounts, attendance register of board meetings, register of debenture holders, etc. - Schedule III – to be preserved for a minimum period of five years or such higher period as may be determined by the board of directors of the company. Documents listed under this schedule include the register of stock options, register of directors and key managerial personnel, disclosures made under applicable company laws, etc. As per SEBI's listing regulations, documents set out in Schedule I and II can be kept in

	electronic mode. The complete list of documents under each schedule is set out in SEBI's listing regulations. It covers listed (public) companies and acts as a regulatory restriction.
	License Agreement for Provision of Internet Services, Amendment in Internet Service Provider (ISP) License Agreement guidelines for change in time period of storage of commercial records (since 2013, last amended in January 2022) According to the License Agreement Guidelines, the internet service provider licensee shall maintain all commercial records, call detail records, exchange detail records and IP detail records with regard to the communications exchanged on the network. Such records shall be archived for at least two years for scrutiny by the licensor for security reasons and may be destroyed thereafter unless directed otherwise by the licensor. Data retention requirements were previously in place under the "Licence Agreement for Provision of Internet Services" by the Department of Telecommunications, Ministry of Communications & IT, Government of India. It covers internet service providers and acts as a regulatory restriction.

	Indian Computer Emergency Response Team Direction No. 20(3)/2022-CERT-In (since April 2022) Direction 5 of Direction No. 20(3)/2022-CERT-In mandates data centres, virtual private server providers, cloud service providers and virtual private network service providers to mandatorily collect and retain certain subscriber related information in an accurate manner for a minimum period of five years after the subscriber is no longer availing the services. These data sets include subscriber names, period of hire including dates, IPs allocated and used, e-mail address along with IP and time stamp used at the time of registration, purpose of availing the services, verified address and contact numbers, and ownership pattern of subscribers. Virtual asset service providers, virtual asset exchange providers and custodian wallet providers must also maintain KYC information and records of financial transactions for a period of five years. Specifically in relations to transaction records, Direction No. 20(3)/2022-CERT-In state that the information must be maintained accurately in such a way that individual transactions can be reconstructed along with the relevant constituents such as IP addresses, time zones, transaction ID, public keys or equivalent identifiers, addresses or accounts involved, nature and date of transaction, amount transferred, etc.

	It covers data centres and virtual private servers, cloud service, virtual private network service, virtual asset service, virtual asset exchange and custodian wallet providers and acts as a regulatory restriction.
Source: Database - The Digital Trade Integration Project	

Non-Discriminatory Treatment of Digital Products

China

Sub Pillar	**Policies**
Licensing schemes for digital services and applications	Foreign investors have complained of the multitude of licensing and accreditation agencies they have to engage with to provide IT services, making the process problematic and time consuming. These licensing and accreditation requirements cover computer services, and act as regulatory restrictions.
	Circular on Clearing up and Regulating the Internet Access Service Market (since January 2017) The circular on Clearing up and Regulating the Internet Access Service Market barred telecommunication companies and internet access service providers from setting up or renting VPNs without government approval. More and more cases have been reported of VPNs being shut down; individuals who set

	up or use VPNs have been punished since 2017. It affects VPN services and acts as a regulatory restriction.
	State monopoly on imports and distribution of multimedia products (since 2000) China's General Administration of Press and Publications agency selects which publications and audio-visual products may enter China, while the state administration on radio, film and culture and the Ministry of Culture review various media. Additionally, China's Ministry of Culture selects which entities may import finished audio-visual products. This effective monopoly on the import and distribution of multimedia products means that China tightly restricts the import of cultural media into the country. These measures have been the focus of a WTO investigation launched by the United States in 2007 (DS363). The panel ruled in favour of the complainant, deeming that China had not adequately substantiated its defence, which concerned the need to protect public morals. In total, the panel found 29 WTO violations throughout various Chinese regulations, catalogues, rules, opinions and legal instruments. Rather than fully implementing the panel's recommendations, China and the US reached a memorandum of understanding via a negotiated settlement. Many of the associated laws remain in place,

	and their influence is amplified by provincial and local level regulations that cite them. It covers reading materials (e.g. newspapers, periodicals, electronic publications), audio-visual home entertainment products (e.g., video, compact discs, digital video discs), sound recordings (e.g., recorded audio tapes), and films for theatrical release and acts as a regulatory restriction.
	Interim Provisions of the People's Republic of China on the Management of International Networking of Computer Information Networks (since February 1996) Provisions on Administrative Law Enforcement Procedures for Internet Information Content Management (since December 1997, amended in 2011) According to Article 6 of the Interim Provisions, computer information networks for direct international networking must use the international channels provided by the national public telecommunications network of the Ministry of Posts and Telecommunications. No unit or individual may establish or use other channels for international networking on their own. The public security authorities may issue a warning and impose a fine of up to RMB 15,000 (USD 2200) on anyone who violates this provision. In addition, institutions or individuals are not allowed to use the

	international network to endanger national security, divulge state secrets, infringe upon national, social and collective interests, and the legitimate rights and interests of citizens, or engage in illegal and criminal activities. Institutions and individuals engaged in international networking services are required to file procedures in designated public security agencies within 30 days of the connection, and accept the security supervision, inspection and guidance of public security authorities; for those who violate the measures, individuals and institutions can be fined in serious cases and can be given six months to stop networking, shut down for rectification, etc. The Provisions on Administrative Law Enforcement Procedures for Internet Information Content Management set out the procedural and administrative processes for the Cyberspace Administration of China to enforce laws and regulations relating to internet content. It covers internet access and acts as a regulatory restriction.
	Telecommunications Regulations of the People's Republic of China (since September 2000, last amended in February 2016) According to Article 7 of the Telecom Regulations, a telecom operator must obtain a proper licence for its telecom business. In accordance with Article 8, the telecom

	business is divided into basic telecom business and value-added telecom business. The Classification Catalogue of Telecom Business, attached to these Regulations, further divides basic telecom business and VAT business into different sub-categories, each requiring a corresponding licence. One of the essential sub-categories of VAT business is called “Information Service”. The information service provided through the internet is called “Internet Information Service”, which is usually referred to as Internet Content Provision (ICP) service. This is a very broad category and covers a wide range of online services, such as instant messaging, app stores, search engines, online communities and online anti-virus services. An ICP licence is required for the ICP service. All websites with their own domain name that are hosted on Chinese mainland territory are required to obtain an ICP licence. Websites that are hosted outside the Chinese mainland territory do not need to obtain it. ICP filing is regulated by local regulations in each province. In general, requirements are similar in every province; for example, the core requirement fixed by the Beijing municipality is that the website abides by the content laws in China and "should not contain materials related to terrorism, explosives, drugs, jurisprudence, gambling, and other illegal acts”. In addition, the following

	requirements and documents have to be prepared and provided: - The domain name must be registered from a China-based domain name provider. - The ICP filing subject must be the domain name owner. - For a person, a scanned copy or photo of the front and back of the ID card is required. - For a company, a scanned copy or photo of the company's registration certificate, and scanned copies or photos of the front and back of the ID cards of the persons in charge of the ICP filing and the website is required. - Other documents required by the local communications administration, such as a domain name certificate. Websites are shut down and companies can be blacklisted by the Chinese Ministry of Industry and Information Technology if they do not comply with the ministry's requirements. It covers internet content provision services and acts as a regulatory restriction.
	Provisions on the Administration of Internet News Information Services and Provisions on Administrative Law Enforcement Procedures for Internet Information Content Management (since June 2017) According to Article 5 of the Provisions on the Administration of Internet News Information Services, internet news providers are required to obtain a permit to provide

	internet news information services to the public through internet websites, application software, forums, blogs, microblogs, public accounts, instant messaging tools, online live streaming and other such methods. In addition, pursuant to Article 6 of the law, the applicant's person-in-charge or chief editor must be a Chinese citizen and the applicant shall have a legal person legally established within the territory of the People's Republic of China. Furthermore, the applicant must separately obtain an internet content provider (ICP) licence or an ICP filing from telecom industry regulators. According to Article 16 of the law, without an ICP number, a website can be shut down by the hosting provider with no notice. Besides, all privately operated news services are obligated to have their operations overseen by personnel endorsed by the ruling party. Editorial staff working on these platforms need approval from national or local government internet and information offices, and their employees are required to undergo training and obtain reporting credentials from the central government. The Provisions on Administrative Law Enforcement Procedures for Internet Information Content Management set out the procedural and administrative processes for the Cyberspace Administration of China to enforce laws and regulations relating to internet content.

	It covers news providers and acts as a regulatory restriction.
	Administrative Regulations for Online Publishing Services (since March 2016) Strict guidelines on what can be published online and how the publisher should conduct business in China came into force in March 2016. According to Article 10 of the Administrative Regulations for Online Publishing Services, Chinese-foreign joint ventures, Chinese-foreign co-operative ventures and foreign-funded entities are not allowed to engage in online publishing services. Moreover, according to Article 7 of the law, any publisher of online content, including texts, pictures, maps, games, animations, audio and videos will be required to store their necessary technical equipment, related servers and storage devices in China. Online publication service units also need to get prior approval from the State Administration of Radio, Film, and Television (SARFT) if they want to co-operate on a project with any foreign company, joint venture or individual. This regulation covers online publishing services and acts as a regulatory restriction.
Blocking or filtering of commercial web content	Blocking of Foreign Cloud Services. Acts as a regulatory restriction
	Filtering of web content.

	Government-owned ISPs place filtering devices in the backbone IT equipment and in provincial level internal networks, a development that could potentially allow for interprovincial filtering. At least 14,000 search terms on search engines are filtered. It covers web content and acts as a regulatory restriction.
	Blocking of WhatsApp. It acts a regulatory restriction.
	Shutting down of social media account and multimedia streaming services Under the provisions of the Cybersecurity Law and as part of a social media crackdown on websites that disseminate "vulgar content" which "negatively impact society", China have shut down over 60 social media accounts that covered celebrity gossip. Additionally, China's media oversight body, the State Administration of Press, Publication, Radio Film and Television, ordered three major online companies (Weibo, fang, and ACFUN) to halt some of their multimedia streaming services, citing lack of adequate permits and contending that the sites hosted many politically-related programmes that do not conform with state rules. It covers web content and acts as a regulatory restriction.
	Blocking of web content

	In China, there is centralised control over international internet gateways, and occasional local shutdowns of internet access occur to suppress social unrest. This is facilitated through a nationwide system known as the Golden Shield, which involves blocking, filtering and monitoring access to international websites. Since 2012, even virtual private networks (VPNs) have been blocked by the Golden Shield. In addition, the government has previously completely cut off access to communication systems during specific events, as seen in the 10-month internet blackout in Xinjiang Uighur Autonomous Region in 2009. Furthermore, specific web applications are blocked and major platforms like YouTube, Facebook, Twitter, Google+, and foursquare remain consistently inaccessible. "Medium", an online website that allows users including news websites to publish sharable content has been blocked since April 2016. In addition, Reddit was blocked in 2018, and Wikipedia faced restrictions in 2019. Popular applications like Google Drive, Calendar, and Translate were also blocked. As of mid-2020, over 170 of the tops 1,000 globally visited websites and social media platforms were inaccessible in China. This includes prominent international news outlets and independent Chinese-language news services. Many websites of human rights organisations

	like Amnesty International, Human Rights Watch, and Freedom House are also blocked. It covers web content and acts as a regulatory restriction.
Source: Database - The Digital Trade Integration Project	

Source Code Access

USA

Sub Pillar	**Policies**
Effective protection covering trade secrets	The US has adopted the 'Defend Trade Secrets Act (DTSA)', which has horizontal coverage and acts as an enabling measure promoting digital trade.
The WIPO Copyright Treaty	Since March 2002, the US has been a signatory of the WIPO Copyright Treaty, which has horizontal coverage and acts as an enabling measure promoting digital trade.
The WIPO Performances and Phonogram Treaty	The US has been, since March 2002, a signatory of the WIPO Performances and Phonogram Treaty, which has horizontal coverage and acts as an enabling measure promoting digital trade.
Copyright act with clear exceptions	The US adopted the Copyright Act in 1976. Section 107 of the Act provides that fair use for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship and research is not an infringement of copyright. It has horizontal coverage and acts as an enabling measure promoting digital trade.

Patent Co-operation Treaty	The United States is a party to the Patent Co-operation Treaty (PCT) since 1978. It has horizontal coverage and acts as an enabling measure promoting digital trade.
Source: Database - The Digital Trade Integration Project	

EU

Sub-Pillar	**Policies**
Effective protection covering trade secrets	Act: The Directive (EU) 2016/943 of the European Parliament and of the Council of 8, June 2016, on the protection of undisclosed know-how and business information (trade secrets). Active since June 2016. The act is key to harmonising national laws concerning trade secrets by: - ensuring an equivalent level of protection of trade secrets throughout the union - introducing a uniform definition of the term ""trade secret"" - providing common measures against the unlawful acquisition, use and disclosure of trade secrets. At the same time, the Directive contains several exceptions to the protection of trade secrets, e.g., to the advantage of those who reveal misconduct, wrongdoing or illegal activity or if the disclosure of a trade secret serves the public interest.

	It has horizontal coverage and acts as an enabling measure.
The WIPO Copyright Treaty	Act: The EU signed the WIPO Copyright Treaty in 1996 and ratified the treaty in 2009. The treaty entered into force in 2010. It acts as an enabling measure
The WIPO Performances and Phonogram Treaty	Act: The EU signed the WIPO Performances and Phonograms Treaty in 1996 and ratified the treaty in 2009. The treaty entered into force in 2010. It acts as an enabling measure.
Copyright act with clear exceptions	Act: The EU copyright acquis (The European Union (EU) acquis is the collection of common rights and obligations that constitute the body of EU law, and is incorporated into the legal systems of EU Member States) consists of 11 directives and two regulations (since June 2001). Contrary to several intellectual property rights in existence (trademarks, design, new varieties of plants), copyright within the EU is still not a unitary right, but a bundle of national laws, though much harmonised by EU Directives. There is no general principle for the use of copyright protected material comparable to the fair use/fair dealing principle. Directive 2001/29/EC defines an exhaustive set of limitations on the author´s exclusive rights under the "three-step test"

	that is in line with the Berne Convention, which imposes three cumulative conditions to the limitations and exceptions of a copyright holder's rights. The Directive has been transposed by member states with some freedom left to them (means EU countries have incorporated an EU Directive into their own national laws, but they had flexibility in how they did it, choosing their own legal methods (like primary or secondary legislation) to achieve the Directive's goals, rather than being forced to follow a single strict EU law). The list of copyright exceptions and limitations provided by EU law is exhaustive. However, these may be optional for member states, as in the case of those provided by the Directive 2001/29/EC (the InfoSec Directive), or mandatory, as in the case of those provided by Directive 2019/790 on Copyright in the Digital Single Market (DSM Directive). It has horizontal coverage and acts as a regulatory restriction.
Patent Co-operation Treaty	
Mandatory disclosure of business trade secrets such as algorithms or source code	**Act**: The EU has adopted the "Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC"; the regulation has been in force since July 2022.

	The Digital Services Act (DSA) envisages research access to data under confidentiality obligations, as well as access to algorithms and explanations by regulators. Certain requirements in the DSA create uncertainty in relation to trade secret protection as very large online platforms can be under an obligation to open access to their (confidential) data. Article 31 of the DSA provides a framework for compelling access to competent national authorities (digital services co-ordinators) to monitor and assess compliance with the regulation. The digital services co-ordinator may also request large online platforms to provide access to data to vetted researchers for researching and identifying systemic risks as set out in Article 26(1). Such a requirement may include, for example, data on the accuracy, functioning and testing of algorithmic systems for content moderation. All requirements for access to data under the framework should be proportionate and appropriately protect rights and legitimate interests, including trade secrets and other confidential information. Moreover, according to Article 31(6) a platform may apply to amend the data request if it will lead to "significant vulnerabilities for the protection of confidential information."

	It mainly covers very large online firms (defined as firms with an average of monthly users equal to or more than 45 million) and acts as a regulatory restriction.
	Act: Regulation EU 2019/1150 on promoting fairness and transparency for business users of online intermediation services (the Platform to Business Regulation). It has been active since July 2019. Regulation EU 2019/1150 on promoting fairness and transparency for business users of online intermediation services (the Platform to Business Regulation) requires the disclosure of certain features of algorithms, which may constitute trade secrets. Article 5 stipulates that online intermediation services must disclose the main ranking parameters and their relative importance to business users through terms of service, while online search engines need to make similar disclosures publicly. The Commission's December 2020 guidance on ranking (§82) argues that providers cannot refuse to disclose the main parameters based on the sole argument that these constitute a trade secret. It covers online intermediation services and acts as a regulatory restriction.
	Act:

	Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (The Trade Secrets Directive). It has active since 2016. The Trade Secrets Directive (EU) 2016/943 protects trade secrets, while also allowing for disclosure of trade secrets for reasons of public interest, either to the public or to public authorities in the performance of their duties. Article 1.2 states that "this Directive shall not affect: [..] (b) the application of Union or national rules requiring trade secret holders to disclose, for reasons of public interest, information (including trade secrets), to the public or to administrative or judicial authorities for the performance of the duties of those authorities." Moreover, Article 5 stipulates that member states should ensure that an application for the measures, procedures and remedies provided for in this Directive is dismissed where the alleged acquisition, use or disclosure of the trade secret was carried out in any of the following cases for revealing misconduct, wrongdoing or illegal activity, provided that the respondent acted for the purpose of protecting the general public interest.

	It has horizontal coverage and acts as a regulatory restriction.
Source: Database - The Digital Trade Integration Project	

China

Sub Pillar	**Policies**
Effective protection covering trade secrets	Does not have a comprehensive regulatory framework covering trade secrets. China lacks a comprehensive framework in place that provides effective protection of trade secrets, but there are limited measures addressing some issues related to them, namely, Anti-Unfair Competition Law (revised in 2019), the Civil Code (effective since 2021), the Civil Procedure Law (revised in 2017), Labour Law (revised in 2018) and Criminal Law (revised in 2015). According to the Anti-Unfair Competition Law, trade secrets refer to any technical information, operational information or commercial information that is not known to the public and has commercial value, and for which its infringer adopted measures to ensure its confidentiality. In addition, stakeholders have welcomed the latest revision of the Criminal Law and the continuing implementation of previously issued judicial interpretations as positive developments. In particular, stakeholders noted stronger procedural protections for

	right holders and broader definitions of misappropriation. It acts as a regulatory restriction
The WIPO Copyright Treaty	China has ratified the World Intellectual Property Organization (WIPO) Copyright Treaty. It acts as an enabling measure
The WIPO Performances and Phonogram Treaty	China has ratified the World Intellectual Property Organization (WIPO) Performances and Phonograms Treaty. It acts as an enabling measure.
Copyright act with clear exceptions	Copyright Law of the People's Republic of China (since 1991, amended in 2020) China has a copyright regime under the Copyright Law of the People's Republic of China. However, the exceptions do not follow the fair use or fair dealing model, thus limiting lawful use of copyrighted work by others. Article 22 lists exceptions, which include use of a published work for the purposes of the user's own private study, research or self-entertainment, use of a published work, within proper scope, by a state organ for the purpose of fulfilling its official duties, etc. The act has horizontal coverage and acts as a regulatory restriction.
Patent Cooperation Treaty	China has been a party to the Patent Co-operation Treaty (PCT) since January 1994. It has horizontal coverage and acts as an enabling measure

Mandatory disclosure of business trade secrets such as algorithms or source code	National Security Law of the People's Republic of China (active since July 2015) According to Article 25 of the Chinese government's 2015 National Security Law, all information systems in China must be "secure and controllable". Every company operating in China – whether domestic or foreign – is required to provide the Chinese government with access to its source code, encryption keys and backdoor access to their computer networks in China. It has horizontal coverage and acts as a regulatory restriction.
Enforcement of copyright online	Lack of adequate enforcement of copyright online China has high levels of online piracy and lacks effective enforcement. Moreover, China continues to be the largest origin economy for counterfeit and pirated goods, between 2017 and 2019, it accounted (together with Hong Kong) for more than 85 per cent of global seizures of counterfeit goods. In addition, the rate of unlicensed software installation in the country was 66 per cent in 2017 (above the 57 per cent rate of the Asia-Pacific countries), with an estimated commercial value of USD 6,842 million. It has Horizontal coverage and acts as a Restriction on Digital Trade.

Practical or legal restrictions related to the application process for patents	Patent Law of the People's Republic of China (amended in 2020) Article 18 of the amended Chinese Patent Law provides that non-resident foreigners or organisations without business establishments in China have to entrust the patent agency established by law to handle patent applications or other patent-related matters in China. Moreover, according to Article 19, any entity or individual intending to file a patent application in a foreign country for an invention or utility model completed in China has to submit a request for confidential examination to the patent administration department under the State Council in advance. The patent administration department of the State Council will handle international patent applications in accordance with the relevant international treaties to which the People's Republic of China is a party, this Law and the relevant provisions of the State Council. It has horizontal coverage and acts as a regulatory restriction
	Patent Law of the People's Republic of China (amended in 2020) In China, it is often difficult to provide evidence to support a specific claim for damage compensation in a patent enforcement action. The amount of damages was capped between a minimum of RMB10,000 (USD 1,450) to RMB 1,000,000

	(about USD 145,000), which is not considered to be adequate. The first draft of the amendment to the Patent Law proposed an increase in the range between RMB 100,000 and RMB 5,000,000 (USD 15,000 - USD 750,000) However, the second reading of the draft amendments under scrutiny has changed this, setting only an upper ceiling of RMB 5,000,000 (USD 750,000) and eliminating the minimum amount. The amendment also introduces certain changes regarding evidence of illicit profit of a defendant, The new draft amendment provides that in order to determine the amount for compensation, where the right holder has endeavoured to present evidence and the related account books or materials are mainly in the control of the accused infringer, the People's Court may order the defendant to provide those books and materials relating to the infringing conduct. If the defendant does not provide or provides false account books or materials, the People's Court may refer to the right holder's claims and evidence to rule on the amount of compensation. This will aid foreign right holders in patent enforcement actions. It has horizontal coverage and acts as a regulatory restriction
	The Medium- and Long-Term Plan for the Development of Science and Technology (2006–2020)

	China's indigenous innovation practices are a web of policies, regulations and strategies that create incentives for Chinese enterprises to create advanced technologies. Only enterprises with Chinese legal person status can apply for product accreditation. Moreover, to be accredited, a product must have been manufactured by an entity with full ownership of intellectual property rights in China, either by creating the rights or by acquiring them. These policies, which are contained in the Medium- and Long-Term Plan for the Development of Science and Technology (2006–2020), aim to encourage domestic innovation and build and support "national champions" by providing financial incentives that favour domestic innovation. It has horizontal coverage and acts as a regulatory restriction
Source: Database - The Digital Trade Integration Project	

India

Sub Pillar	**Policies**
Effective protection covering trade secrets	India does not have a comprehensive regulatory framework covering trade secrets but there are limited measures addressing some issues related to them. As per the decision of the Delhi High Court in 1995, a trade secret is defined as any information with commercial value, which is not

	available in the public domain and the disclosure of which would cause significant harm to the owner. Moreover, Indian courts and tribunals have upheld the protection of trade secrets under other laws such as contract law, copyright law, principles of equity and common law action of breach of confidence (which is basically the breach of an obligation to keep a piece information secret). In addition to the above, the Information Technology Law of 2000 also sets legal means of protection to confidential information in the form of electronic records. These have horizontal coverage and act as enabling measures.
The WIPO Copyright Treaty	India has ratified the World Intellectual Property Organization (WIPO) Copyright Treaty (since September 2018, entry into force in December 2018) It has horizontal coverage and acts as an enabling measure
The WIPO Performances and Phonogram Treaty	India has ratified the World Intellectual Property Organization (WIPO) Performances and Phonograms Treaty (since September 2018, entry into force in December 2018) It has horizontal coverage and acts as an enabling measure.
Copyright act with clear exceptions	The Copyright Act, 1957 (Act No. 14 of 1957, as amended up to Act No. 33 of 2021) The Copyright Act, 1957 provides a clear regime of copyright exceptions that follows

	the fair dealing model, which enable the lawful use of copyrighted work by others without obtaining permission. According to Article 52(1), a fair dealing with any work (not being a computer program) for the purposes of private or personal use, criticism or review and the reporting of current events and current affairs does not constitute an infringement of copyright. It covers internet intermediaries and acts as an enabling measure.
Patent Co-operation Treaty	India has been a party to the Patent Co-operation Treaty (PCT), since December 1998. It has horizontal coverage and acts as an enabling measure
Enforcement of copyright online	Lack of adequate enforcement of copyright online Copyright is not adequately enforced online in India. Although the country has taken steps against websites with pirated content, there is weak enforcement of IP by courts and police officers, lack of familiarity with investigation techniques, and the continued absence of a centralised IP enforcement agency; these, combined with a failure to co-ordinate actions at both the national and state level, threaten to undercut the progress made. In 2017, the reported rate of unlicensed software installation in the country was 56 per cent in 2017 (below the 57 per cent rate

	the Asia-Pacific countries), with an estimated commercial value of USD 2,474 million. The value of losses from the piracy of music and movies in 2020 was reported to be about USD 4 billion per year while the commercial value of unlicensed software used in India was approximately USD 3 billion. It has horizontal coverage and acts as a Regulatory Restriction
Practical or legal restrictions related to the application process for patents	Patents Act, 1970 (Act No. 39 of 1970, as amended up to Act No. 15 of 2005) Patents Rules, 2003 (as amended in 2012) In 2002, the foreign filing licence requirement was introduced in the Indian Patents Act of 1970. This requirement provides that any inventor who is a resident of India should file a patent application for his/her own invention first in India. The filing can be extended internationally only after a period of six weeks after the date of filing the domestic patent application. Alternatively, the inventor is required to obtain the controller's permission for filing the patent application outside India. However, given that the process is burdensome, filing an application first in India is the preferred way of complying with these provisions. The violation of such rule results in criminal liability under Section 118 of the Indian Patent Act, 1970, with consequent monetary fine or imprisonment

	up to two years, in addition to the impossibility to proceed with the patent application, thus resulting in rejection It has horizontal coverage and acts as a regulatory restriction
	Practical restrictions related to the enforcement of patents The potential threat of patent revocations, lack of presumption of patent validity and the narrow patentability criteria under the India Patents Act impact companies across different sectors. In addition, courts take a significant amount of time to make a final decision in a patent case. A patent lawsuit ordinarily takes approximately five to seven years to be finally decided after trial, if contested by the other party. The Commercial Courts Act helps speed up the process with case management hearings and time-bound trials. However, the backlog of cases at the court and the shortage of judicial officers has an impact on the time it takes for a final decision on a case. The restrictions have horizontal coverage and acts as a regulatory restriction.
	"Patents Act, 1970 (Act No. 39 of 1970, as amended up to Act No. 15 in 2005) Patents Rules, 2003 (as amended in Patents (Amendment) Rules, 2012)"

	According to the Patent Act, 1970 (Act No. 39 of 1970, as amended in Act No. 15 of 2005) and the Patents Rules, 2003 (as amended in Patents (Amendment) Rules, 2012), applications for copyright, trademark and patents can be filed online; however, design applications can only be filed in person. Moreover, applicants who do not have a registered place of business in India are required to file applications through an Indian attorney or agent. It has horizontal coverage and acts as a regulatory restriction.
Source: Database - The Digital Trade Integration Project	

According to the Digital Trade Integration Project (Annexure 1), India and China both exhibit restrictive policies regarding digital trade and cross-border data flows, but the extent and mechanisms of their restrictions vary. In terms of data localisation, China enforces broader and more stringent requirements through laws like the Cybersecurity Law (2017) and Outbound Data Transfer Security Assessment Measures (2022), which mandate local storage for various sectors, including financial and health data. India's localisation rules, such as those for payment data and insurance records, are more sector-specific and less extensive. Both countries refrain from joining binding international agreements on cross-border data flows, making them equally restrictive in this area. However, China is far more restrictive when it comes to internet access, content control and the operation of foreign firms. Policies like the Telecommunications Regulations and the Golden Shield Project heavily restrict foreign access, with stringent requirements for Chinese partnerships and government oversight. In contrast, India focuses mainly on data residency for specific sectors and does not impose such broad content controls. Regarding intellectual property rights, China is more restrictive due to its mandatory source code access requirements under the National Security Law (2015), while India's approach is more balanced, focusing on legal mechanisms like the Copyright Act (1957) and offering fair dealing provisions. Overall, China's policies are driven by a deep focus on domestic economic

control, innovation and security, making it more restrictive than India's. India has a more gradual approach to modernising its digital trade framework while aligning with international standards in certain areas. Thus, while India imposes significant restrictions, they are narrower in scope compared to China's comprehensive and systemic control over digital trade.

India's restrictions on digital trade often stem from a lack of comprehensive policies and enforcement frameworks, whereas China implements deliberate policies to make digital trade more restrictive. In India, the absence of enabling laws, such as robust trade secret protection or centralised IP enforcement mechanisms, create unintentional barriers to trade. These restrictions often arise from internal challenges, such as weak enforcement capacity and a focus on domestic sovereignty over global integration rather than deliberate obstruction. By contrast, China's approach is characterised by explicit regulatory measures aimed at controlling digital trade, such as mandatory data localisation, government access to source codes and approval requirements for cross-border data transfers. These policies, reflected in laws like the Cybersecurity Law and Personal Information Protection Law, are strategically designed to prioritise national security, promote domestic industry and maintain tight governmental oversight. Furthermore, China actively enforces its restrictive measures, leveraging surveillance frameworks and stringent content control mechanisms to safeguard its digital ecosystem, even at the cost of limiting integration with global markets. Thus, while India's restrictions are often unintentional and rooted in capacity limitations, China's are deliberate and systematically enforced to achieve strategic objectives.

Taking into account both the policy-driven restrictions and the OECD Digital Services Trade Restrictiveness Index data, it can be concluded that **China is generally more restrictive** than India in terms of digital trade, but for different reasons. China's policies are intentionally designed to impose barriers and control the flow of digital services and data. These policies create a highly controlled environment that limits foreign participation and cross-border data flows, making China's digital trade environment more restrictive at a regulatory level. India's higher overall score on the OECD Digital Services Trade Index primarily reflects its infrastructure challenges, particularly in rural areas, rather than regulatory hurdles as extensive as those seen in China.

Figure A2.1: Gross Output of the Digital Economy in the USA (in trillion USD)

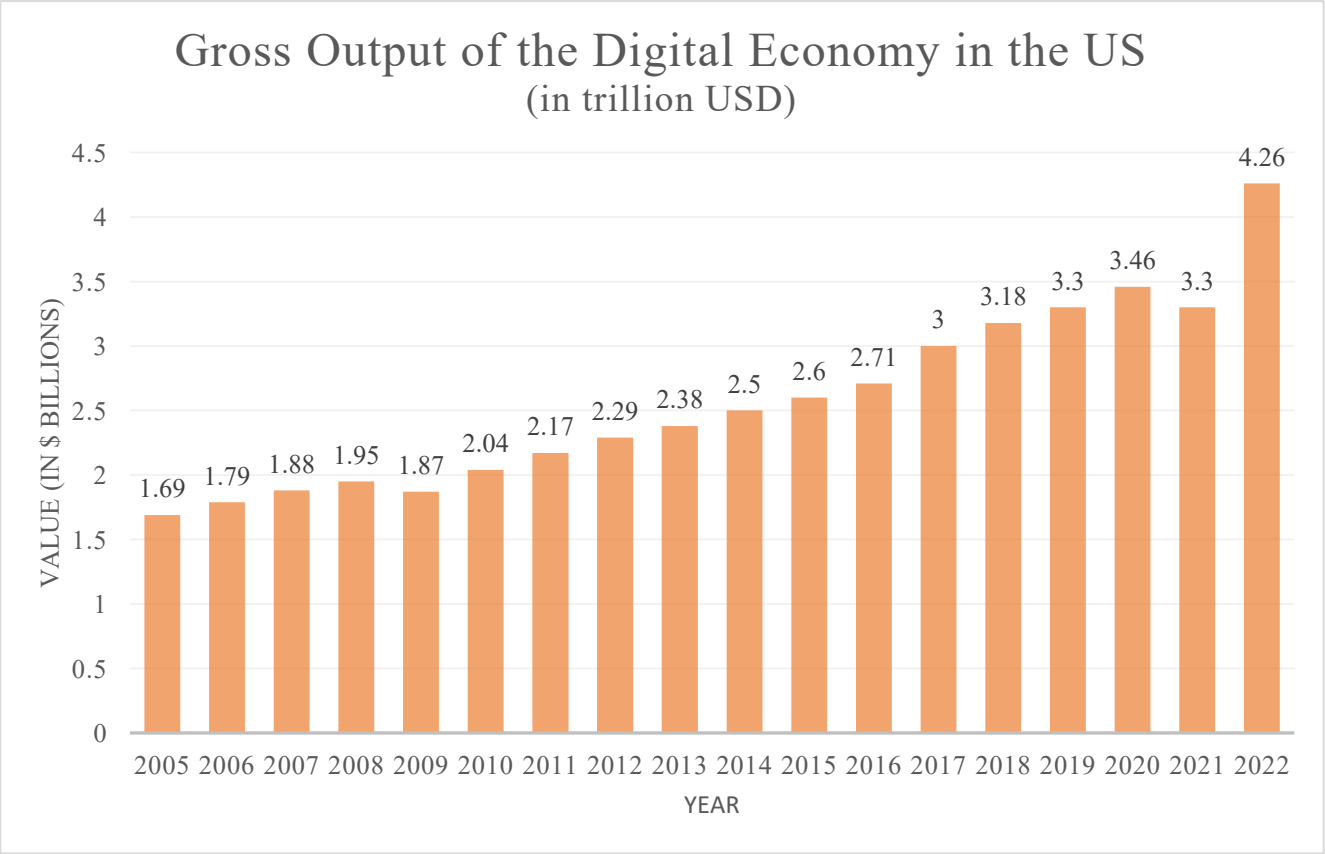


Figure A2.1

Source: Bureau of Economic Analysis (BEA)

Figure A2.2: Market Size of China's Digital Economy from 2005 to 2023. (in trillions USD)

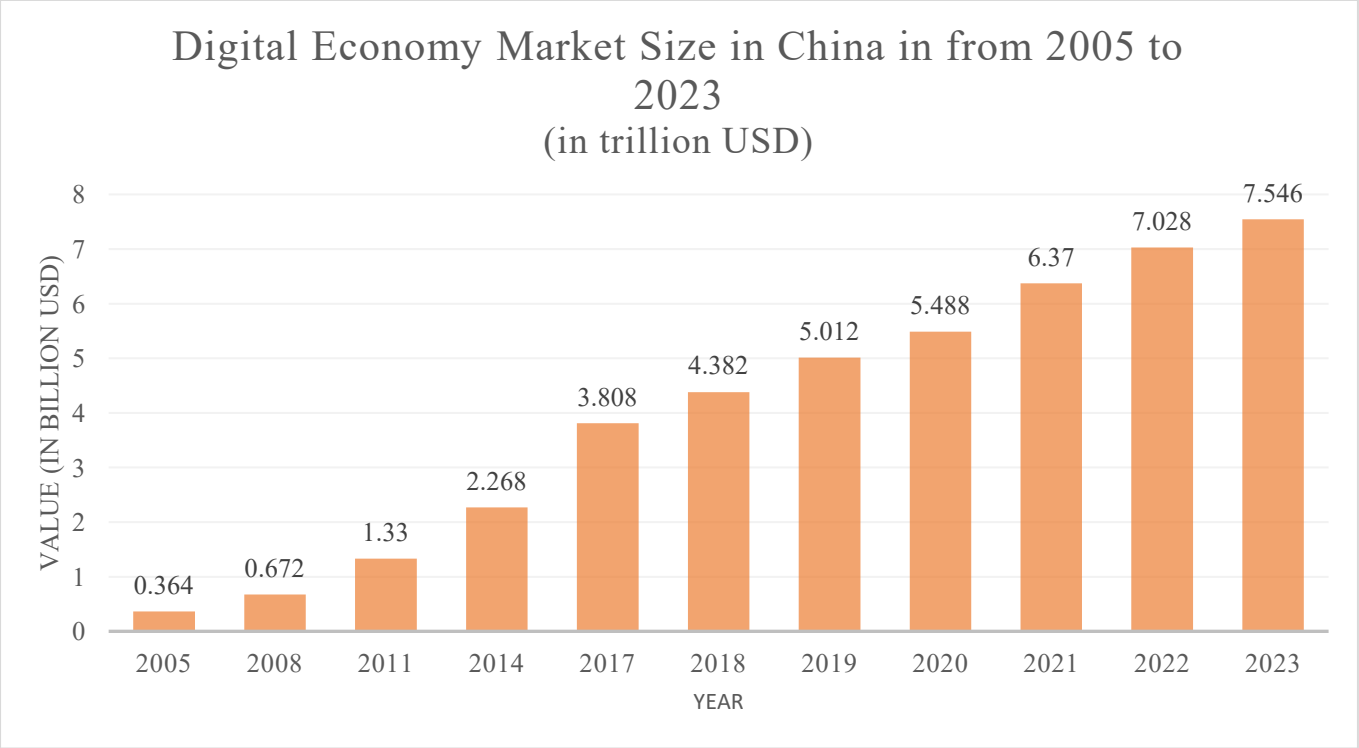
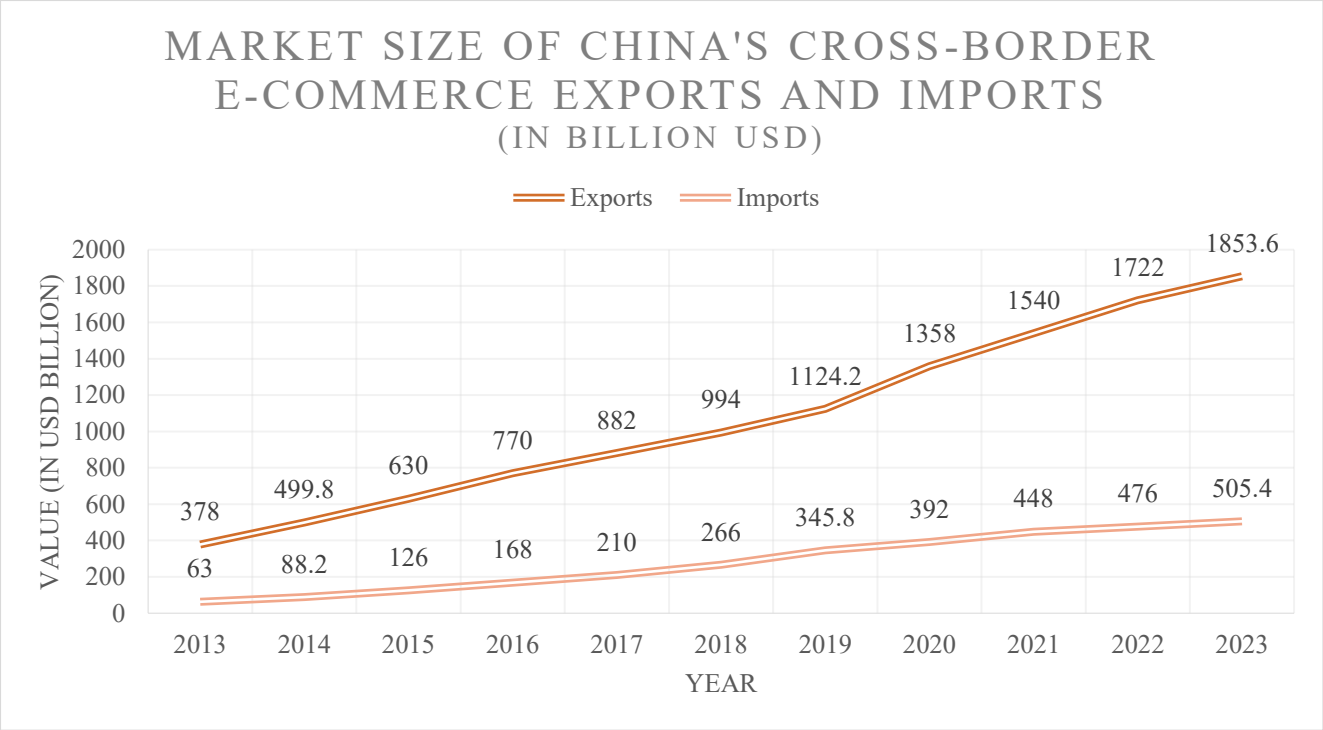


Figure A2.2: Source: CAICT

Figure A2.3: Market Size of China's Cross-Border E-commerce Exports and Imports (in billion USD)

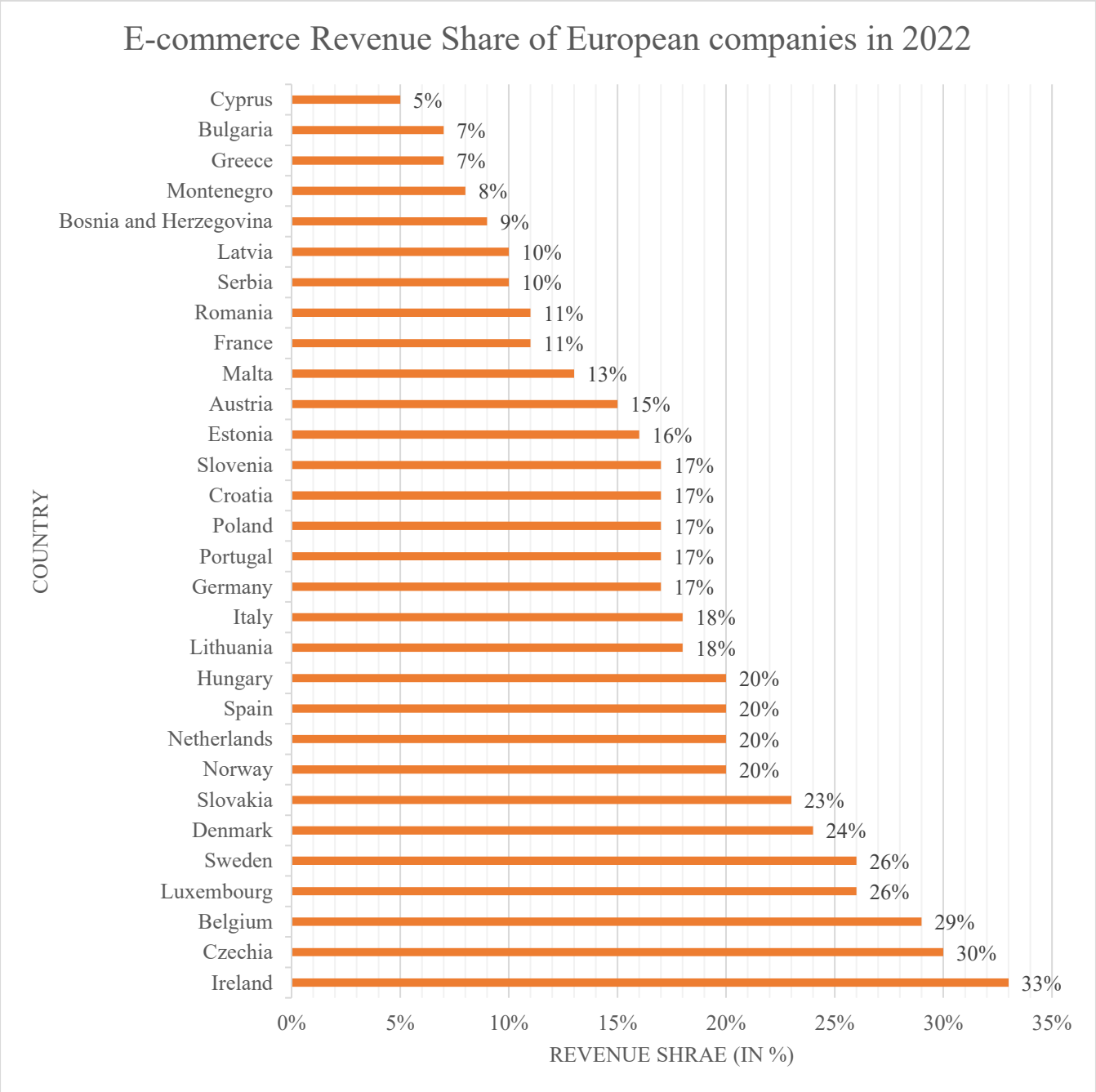
Figure A2.3



Source: 100ec.cn

Figure A2.4: E-commerce Revenue Share of European companies in 2022

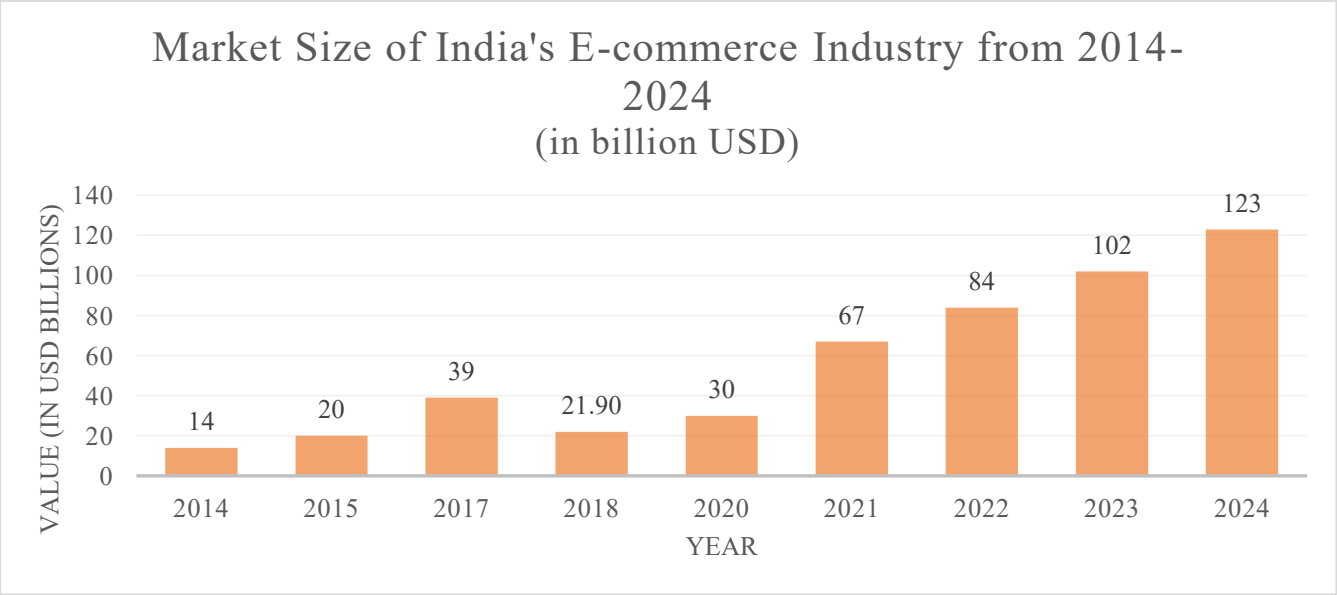
Figure A2.4



Source: Eurostat

Figure A2.5: Market Size of India's E-commerce Industry from 2014-2024 (in billion USD)

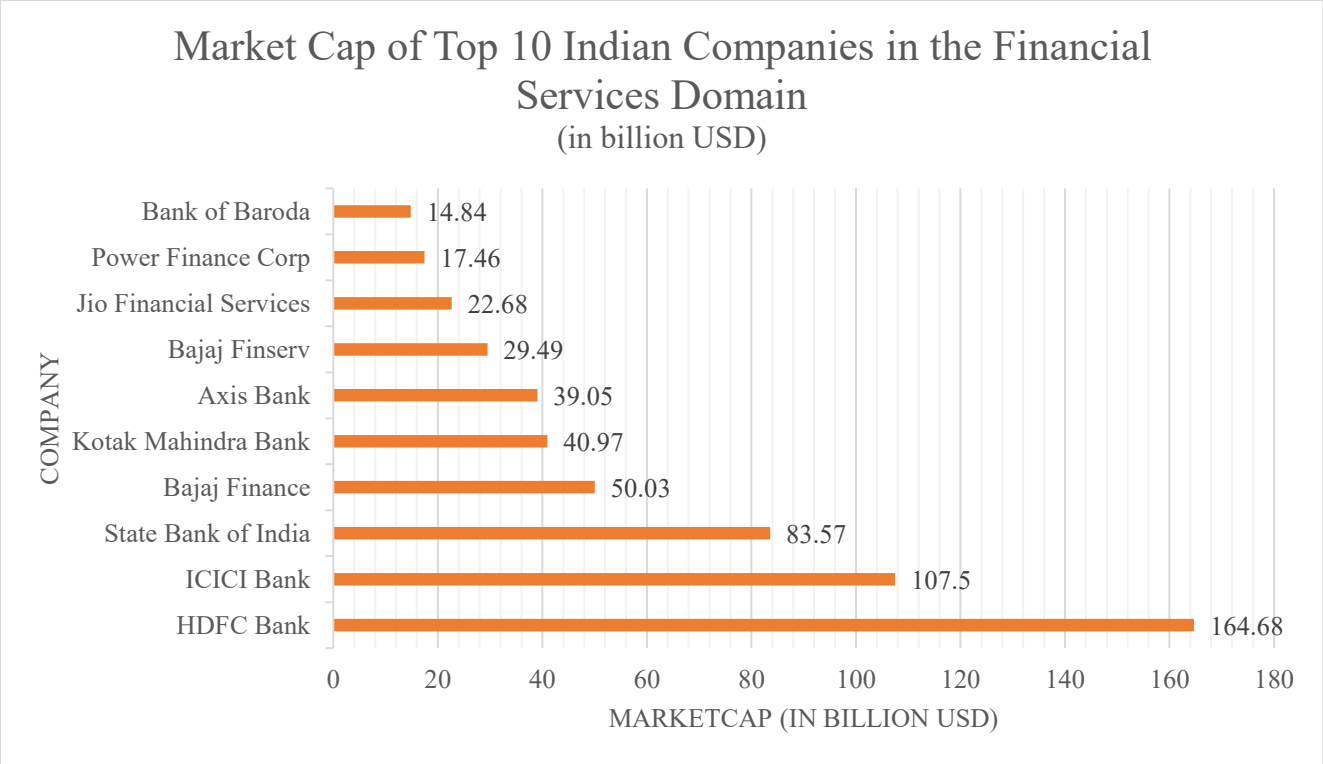
Figure A2.5



Source: India Brand Equity Foundation

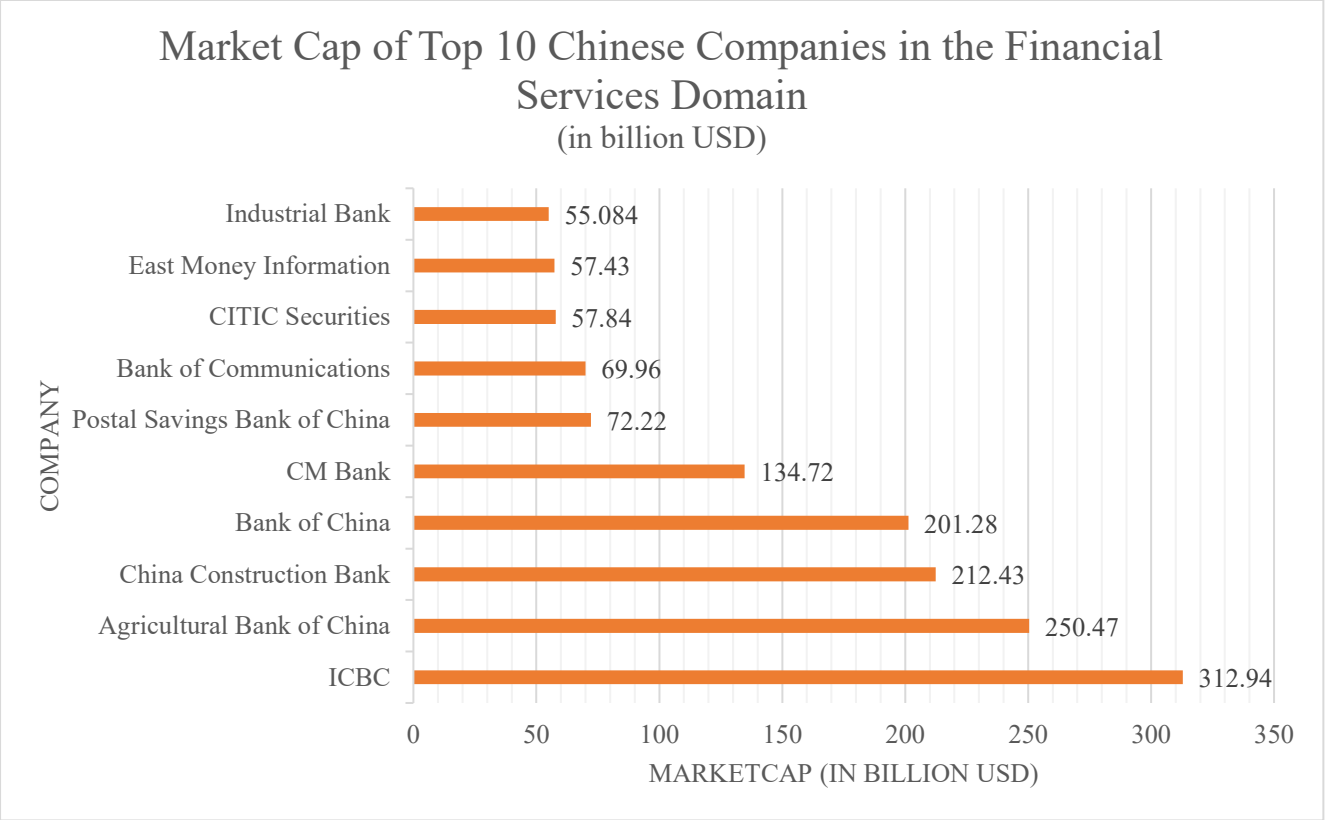
Figure A2.6 to A2.9 – Market Cap Comparison of Companies in the Financial Services Domain (in USD Billions)

Figure A2.6



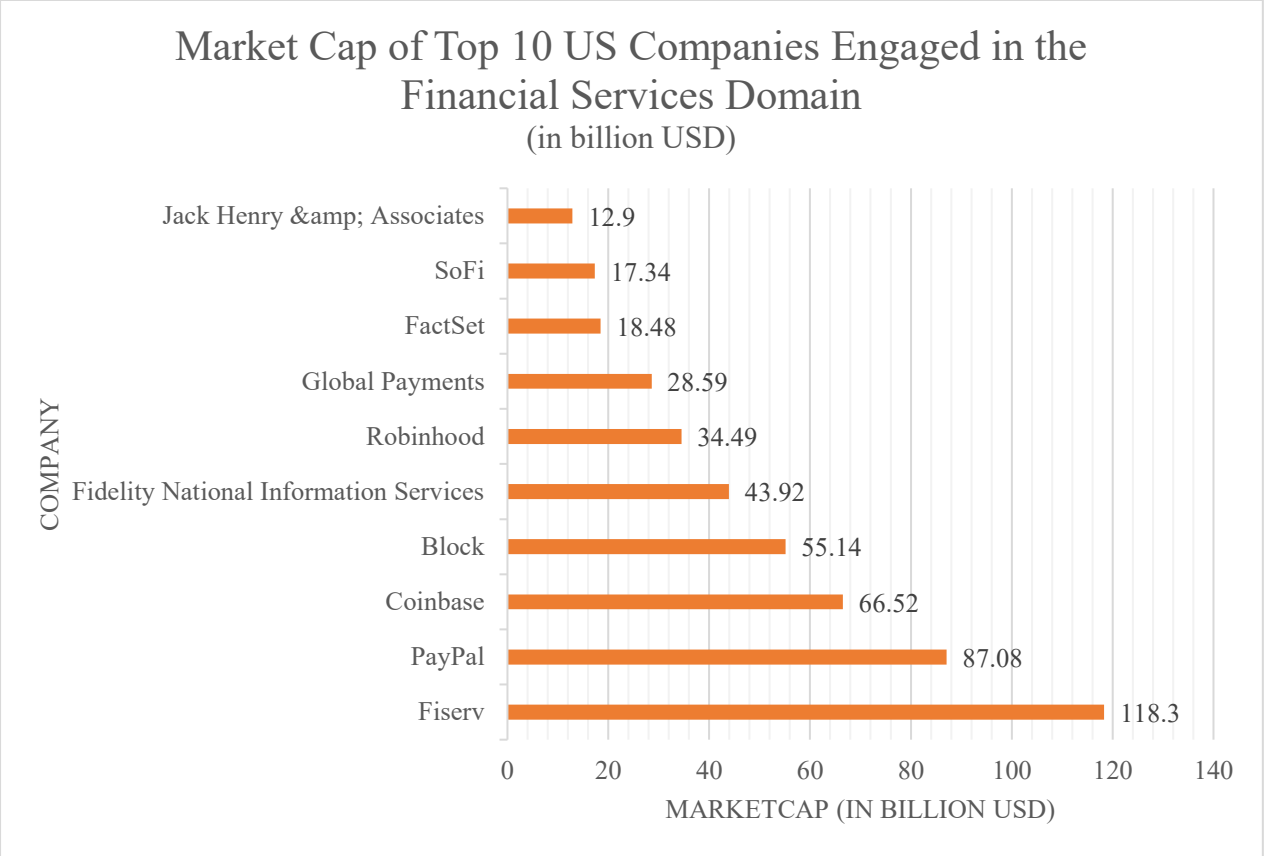
Source: Companies' market cap

Figure A2.7



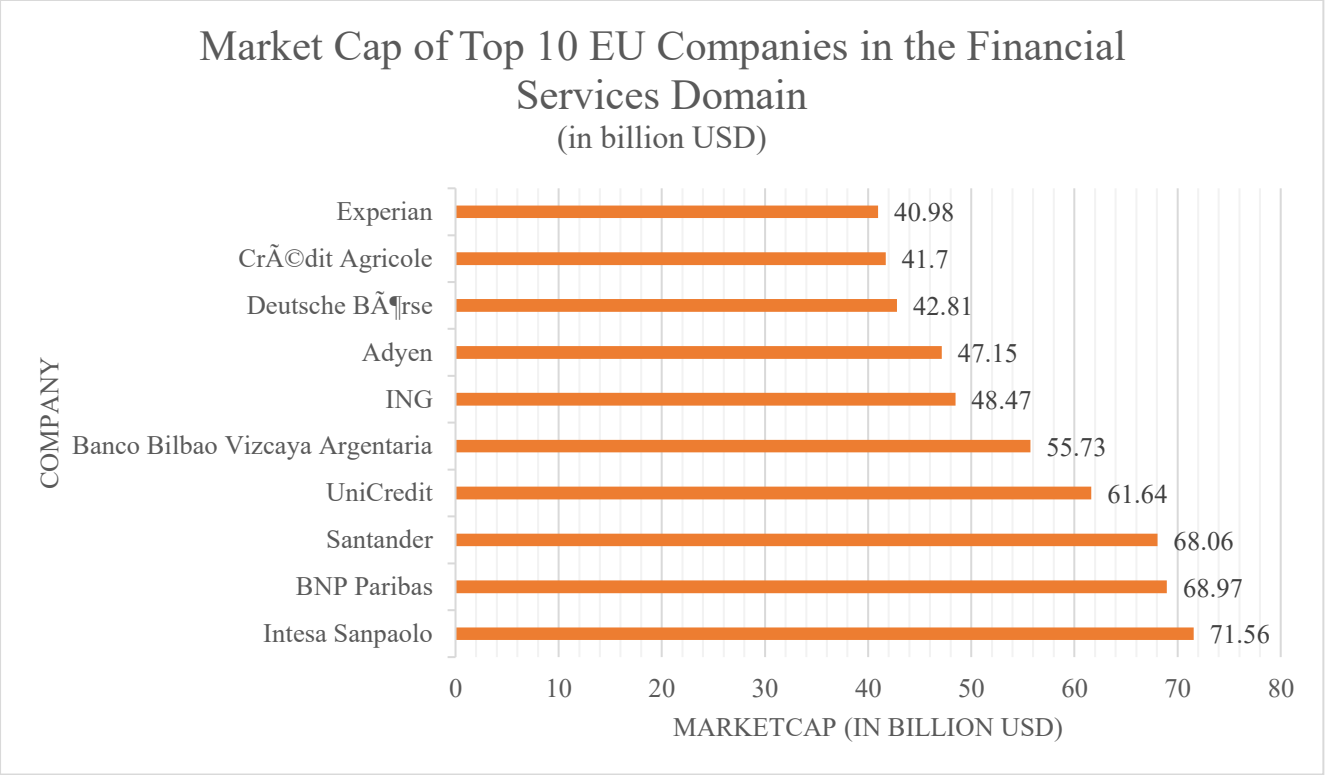
Source: [Companies' market cap]

Figure A2.8



Source: [Companies' market cap]

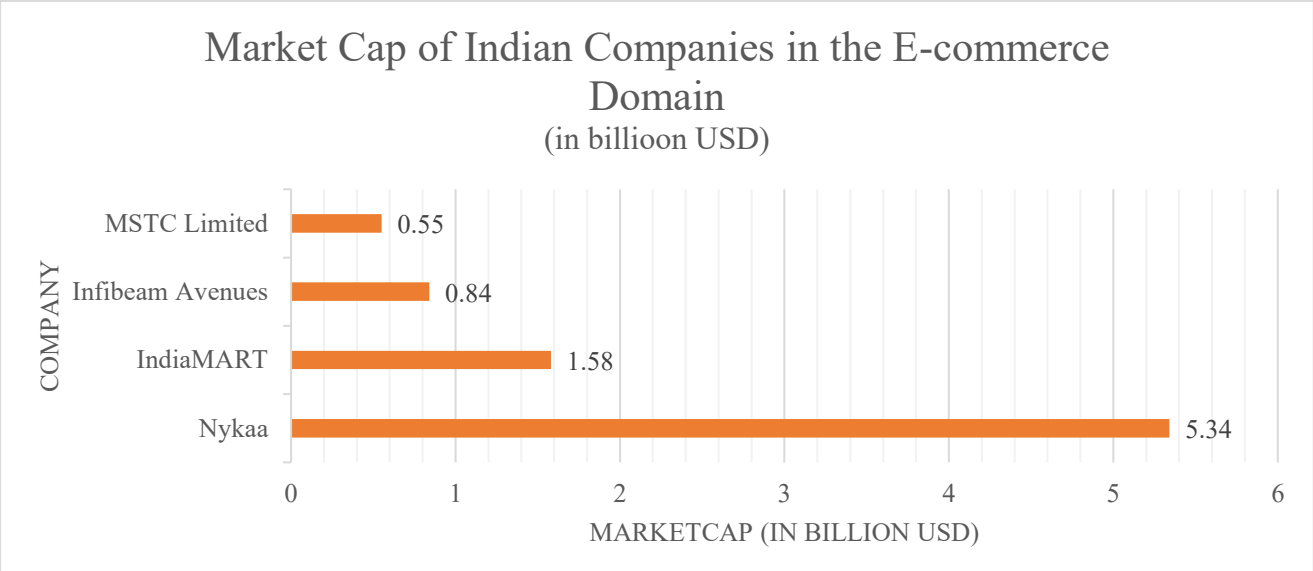
Figure A2.9



Source: Companies' market cap

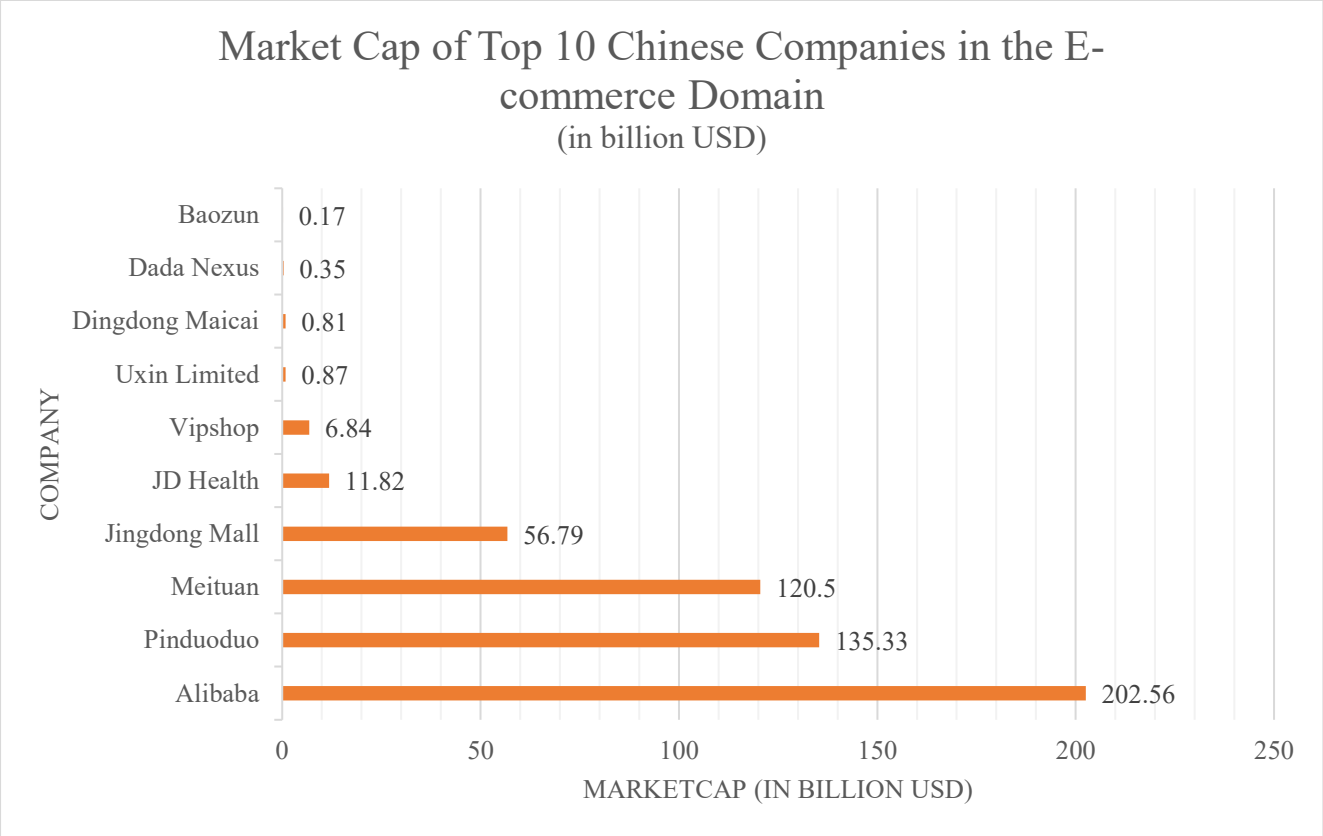
Figure A2.10 – A2.13: – Market Cap comparison of Indian companies in the E-commerce Domain

Figure A2.10



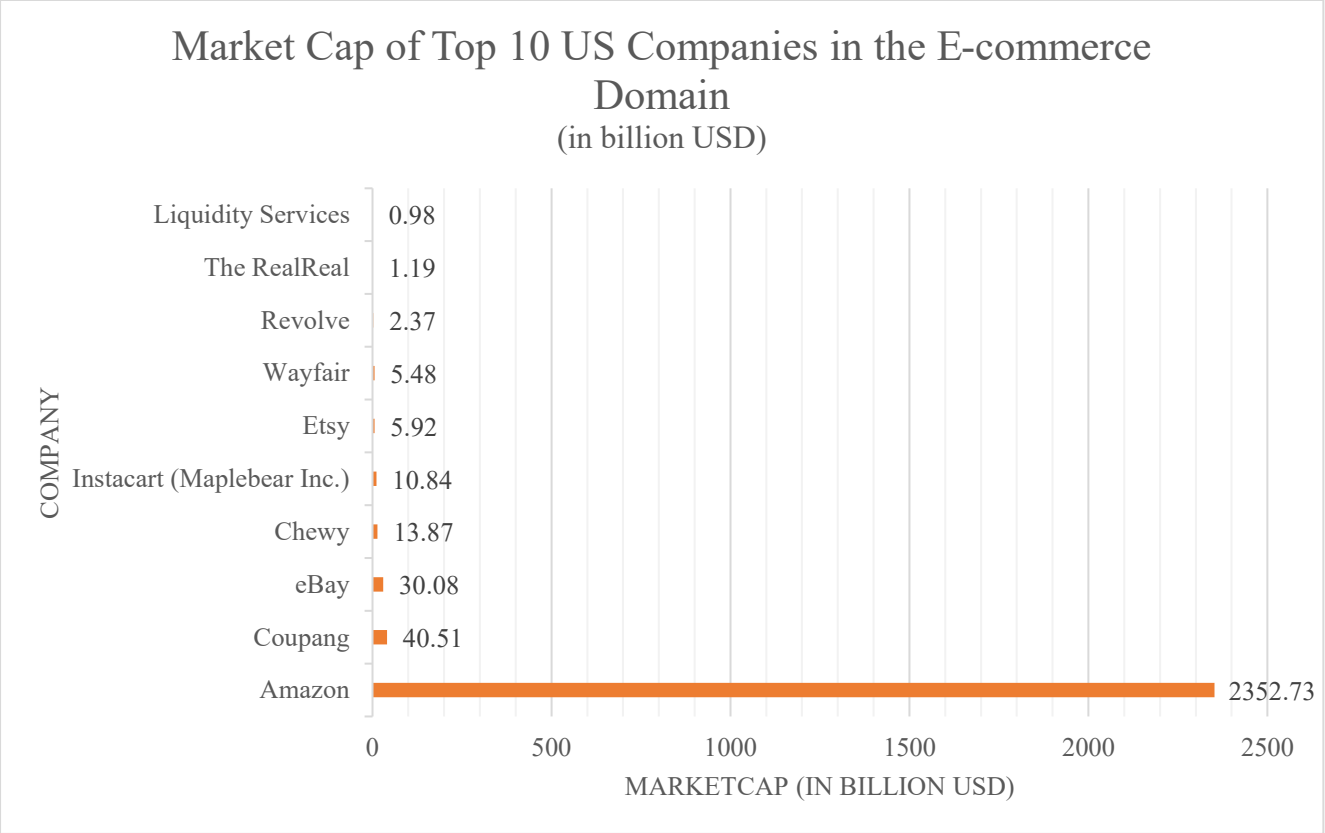
Source: Companies' market cap

Figure A2.11



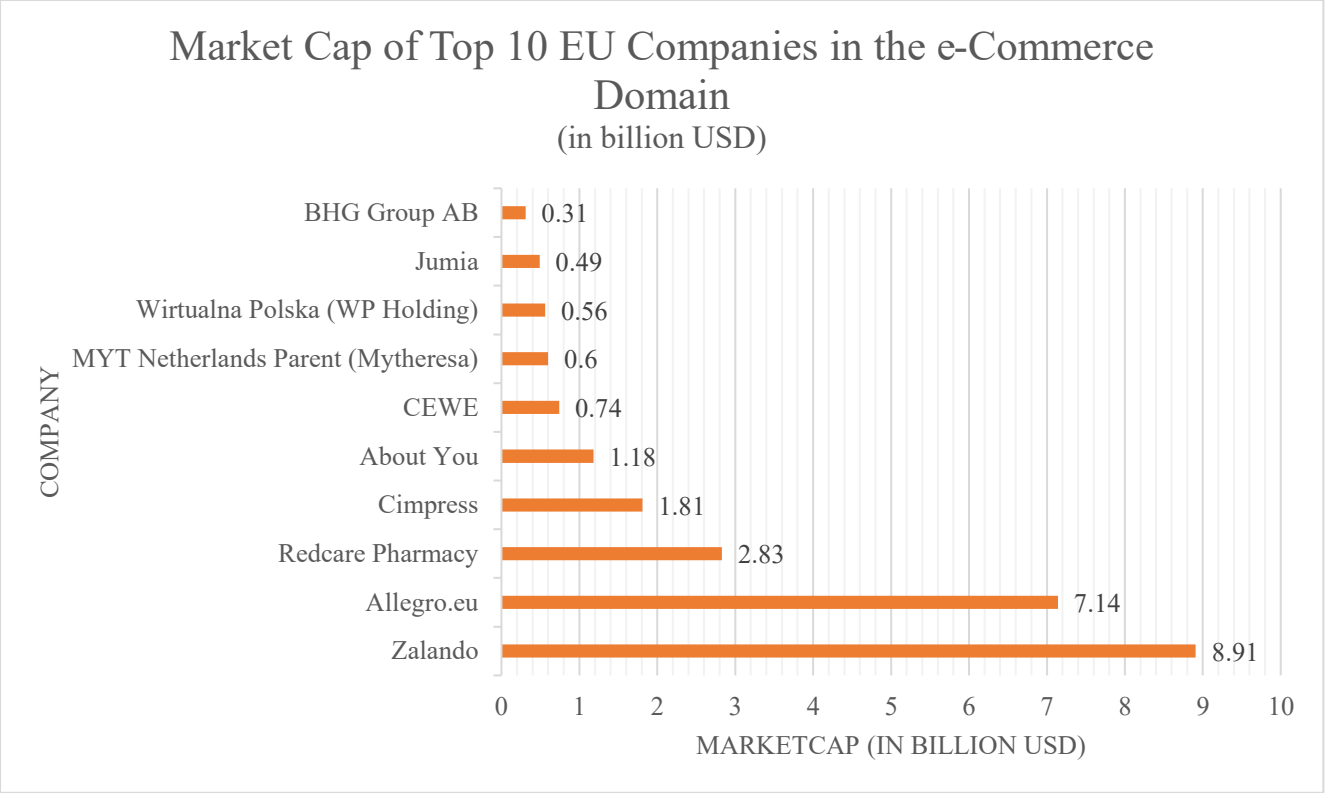
Source: [Companies' market cap]

Figure A2.12



Source: [Companies' market cap]

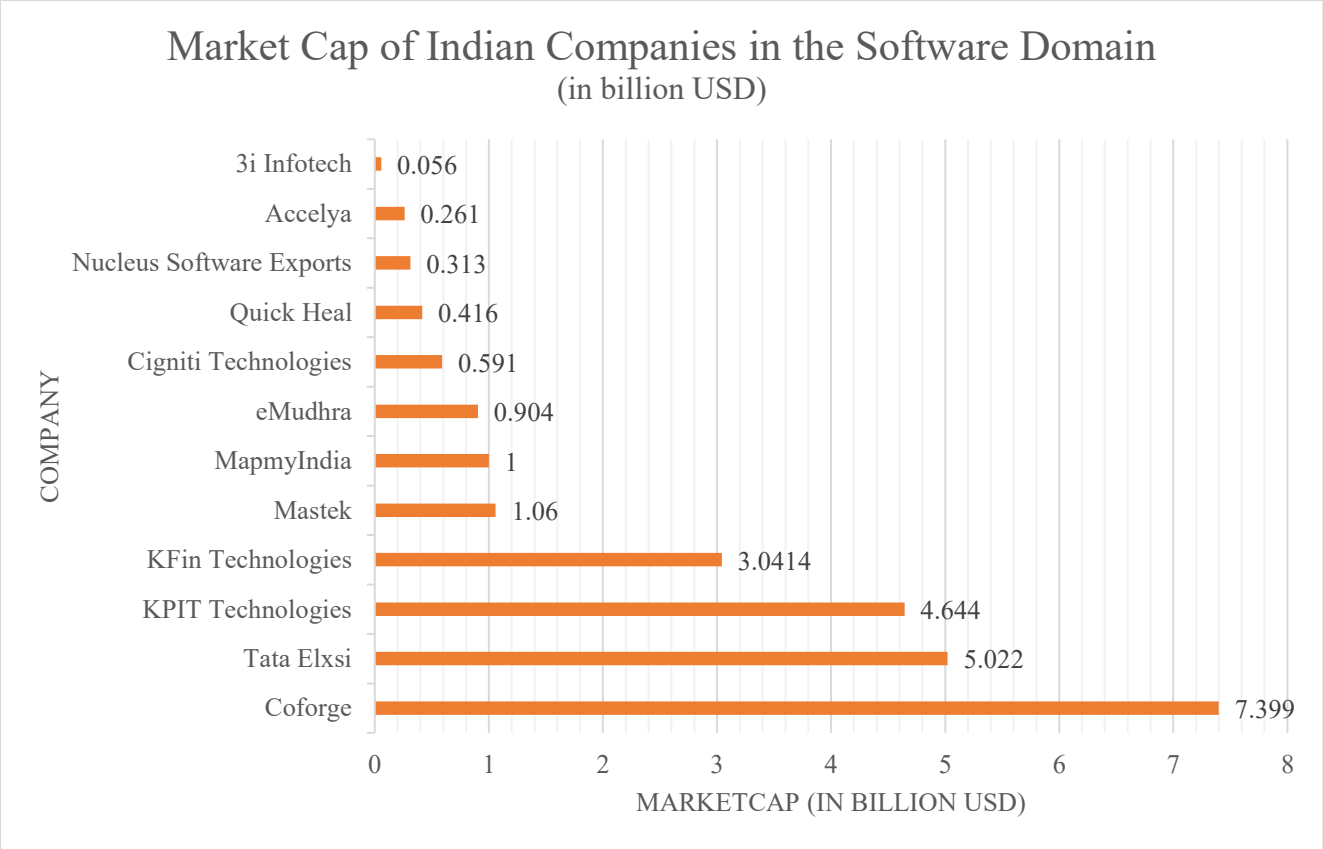
Figure A2.13



Source: [Companies' market cap]

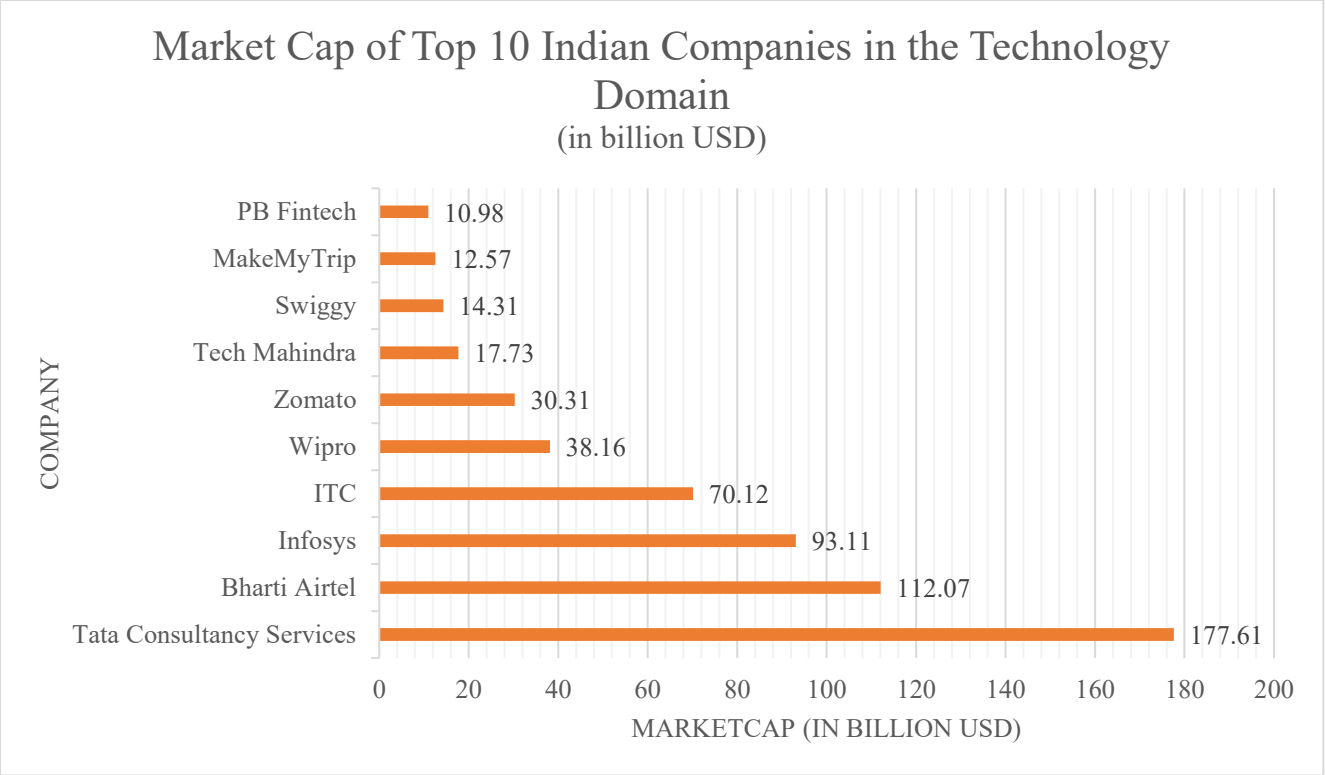
Figure A2.14 to A2.19: - Market Cap comparison of Companies in the Software Domain (in USD Billions)

Figure A2.14



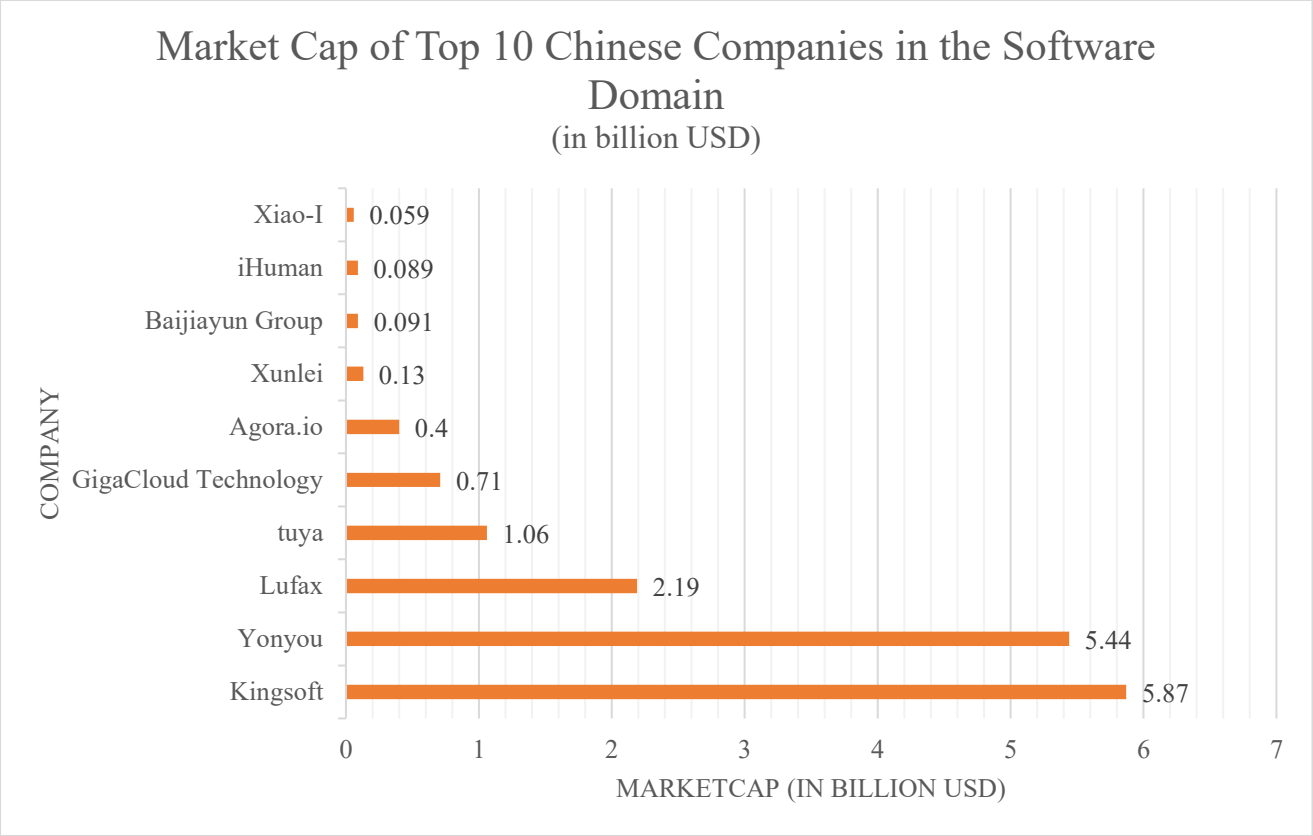
Source: [Companies' market cap.]

Figure A2.15



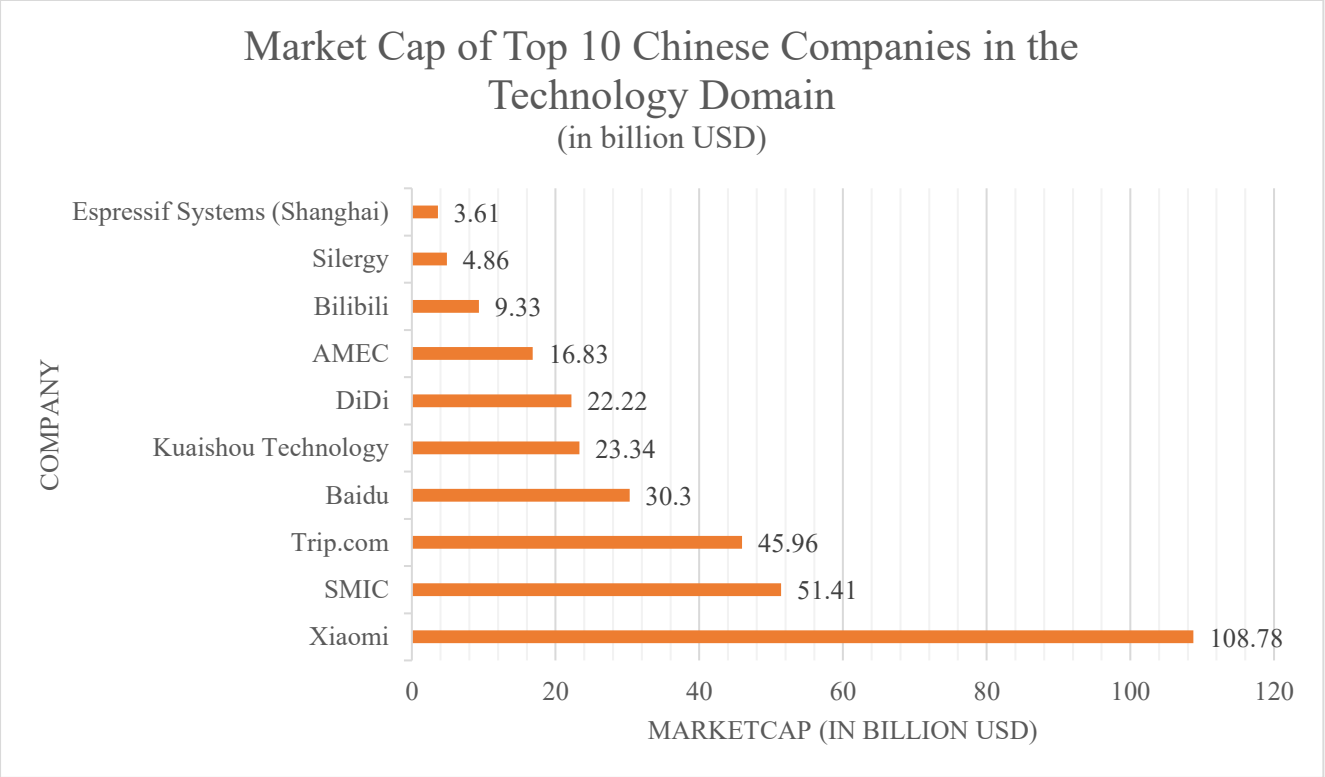
Source: [Companies' market cap]

Figure A2.16



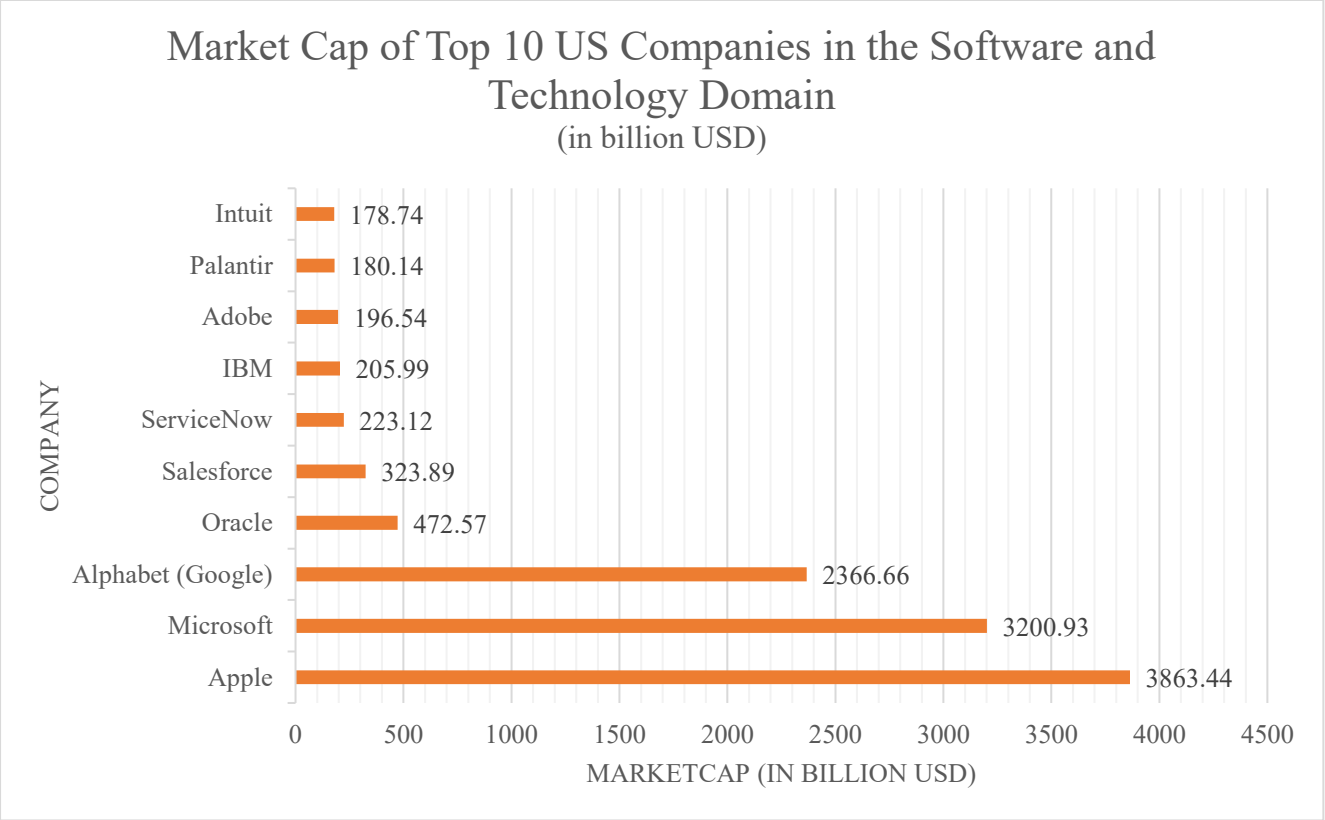
Source: [Companies market cap]

Figure A2.17



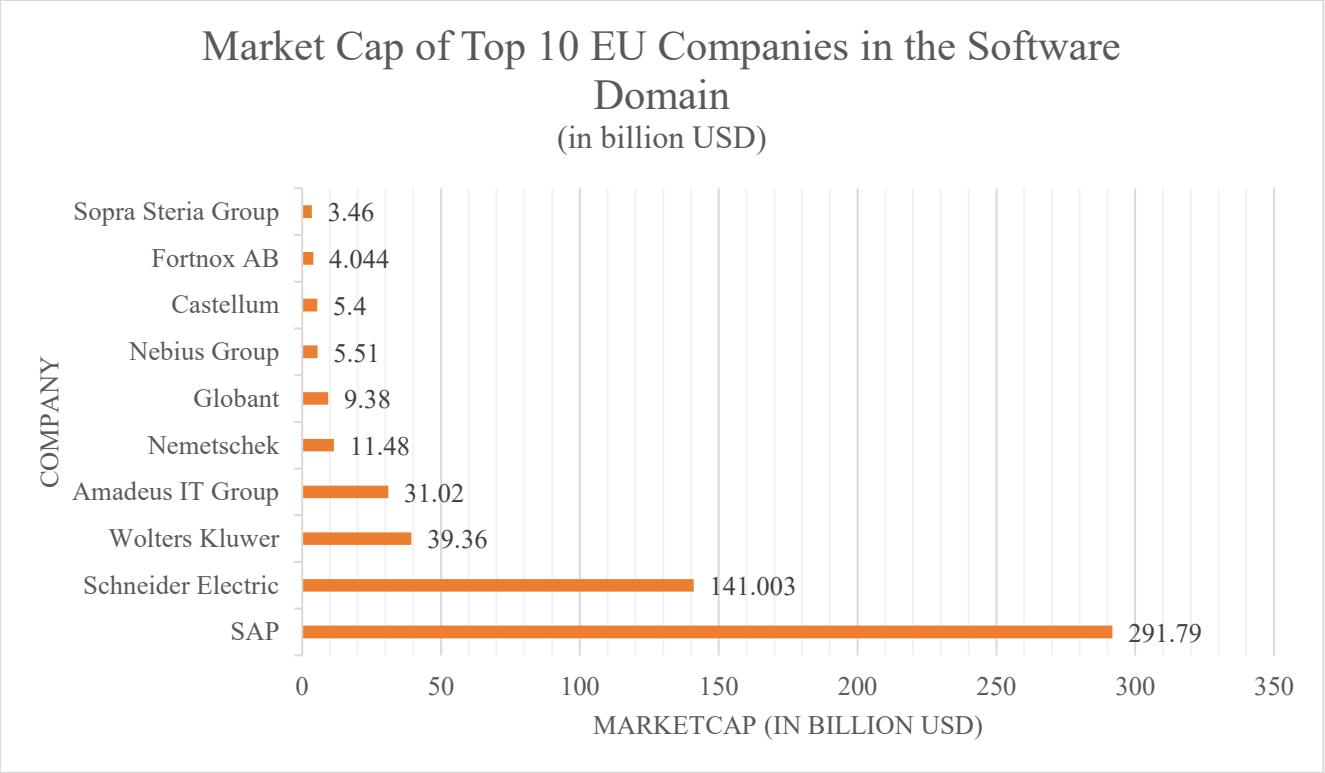
Source: [Companies' market cap]

Figure A2.18



Source: [Companies' market cap]

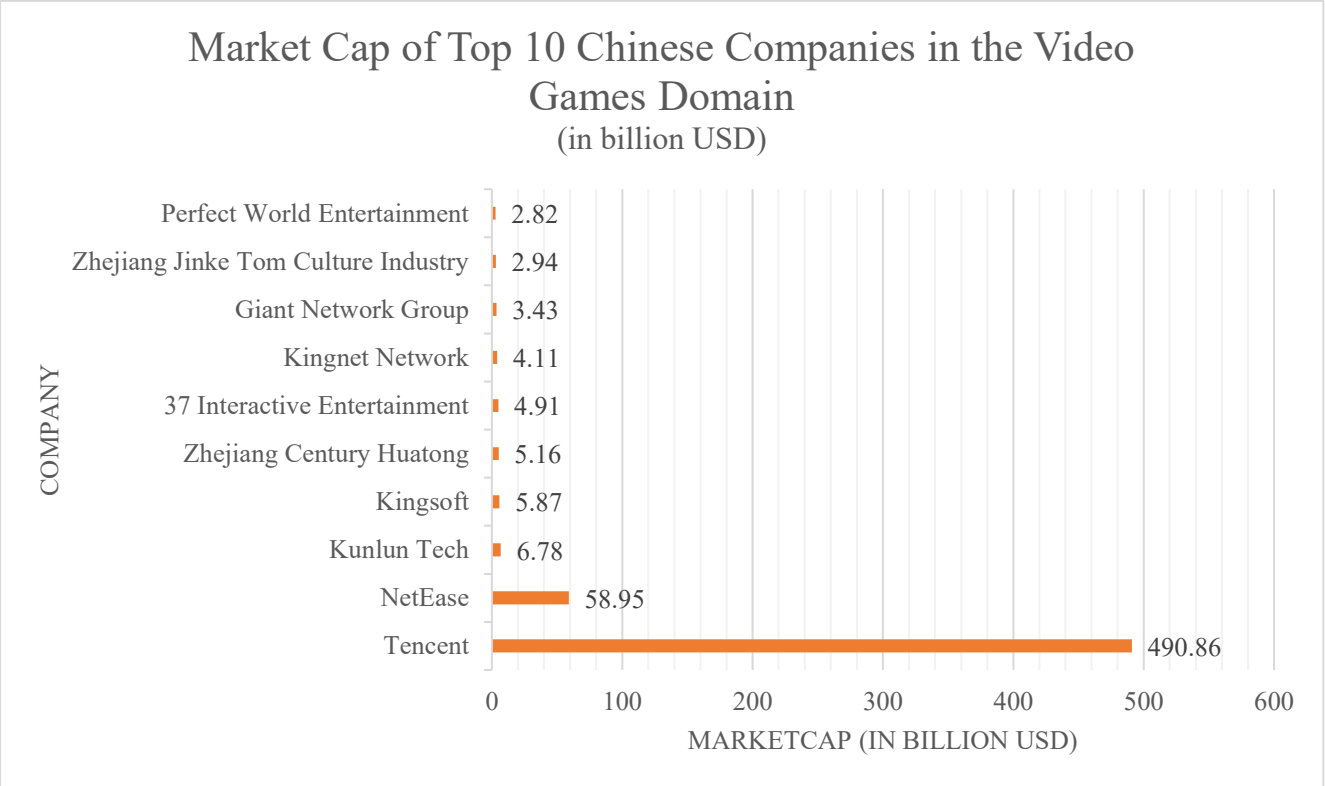
Figure A2.19



Source: [Companies' market cap]

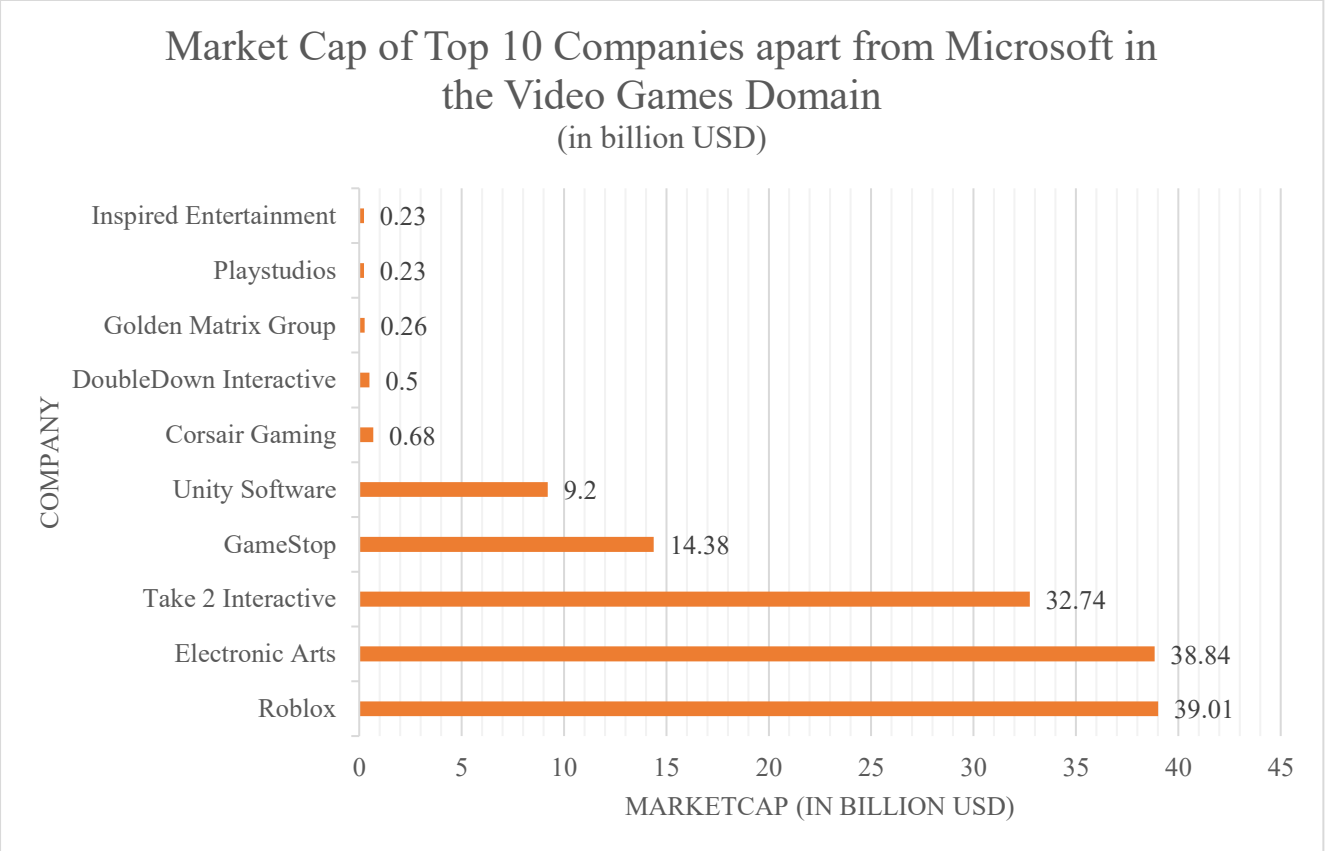
Figure A2.20 to A2.22 – Market Cap Comparison of Companies in the Video Games Domain

Figure A2.20



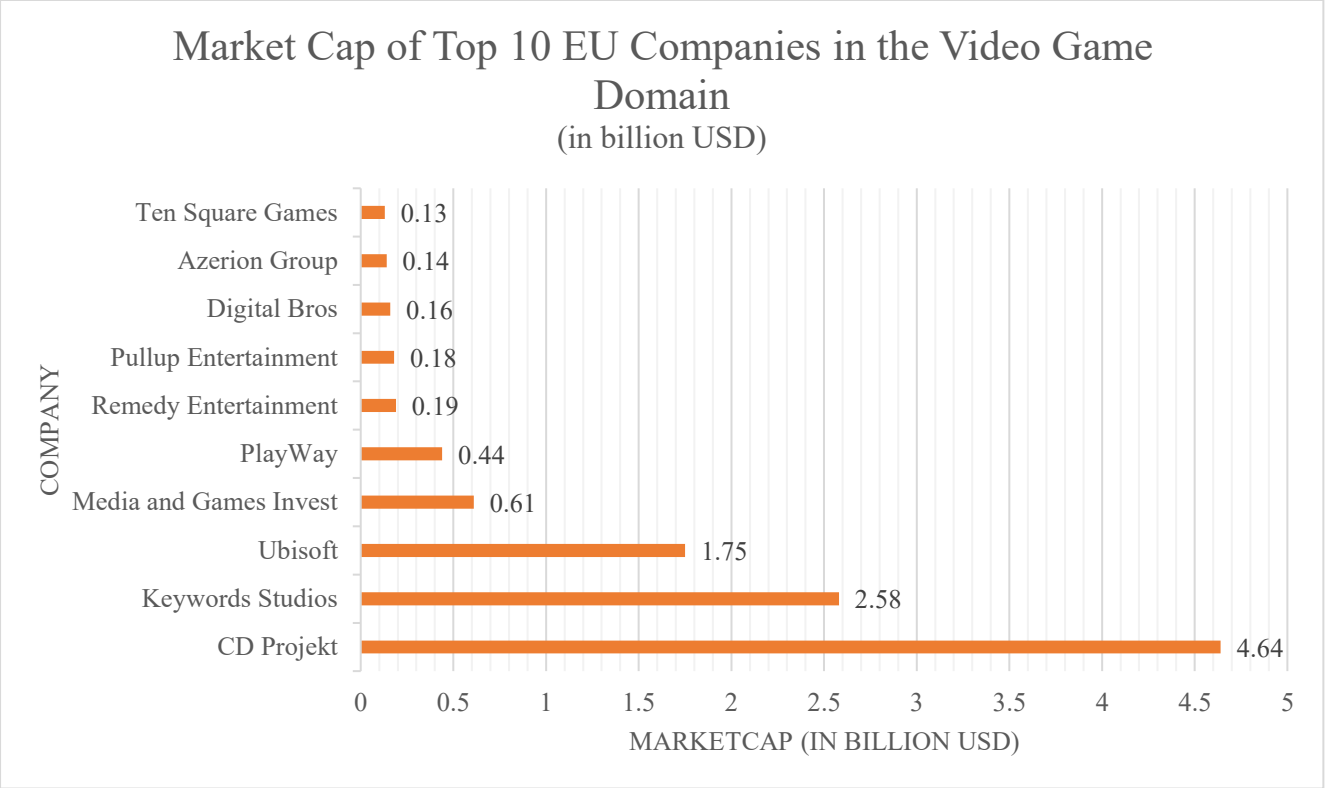
Source: Companies' market cap

Figure A2.21



Source: Companies' market cap

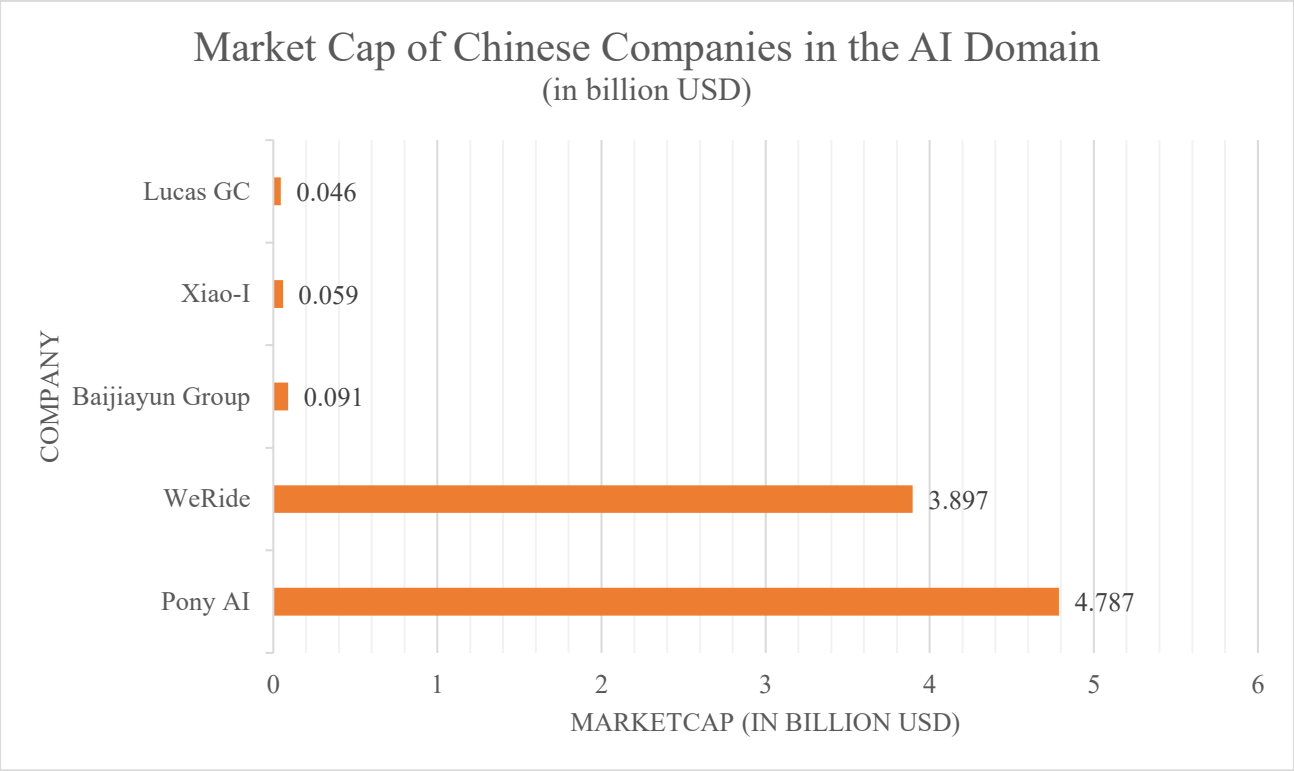
Figure A2.22



Source: [Companies' market cap]

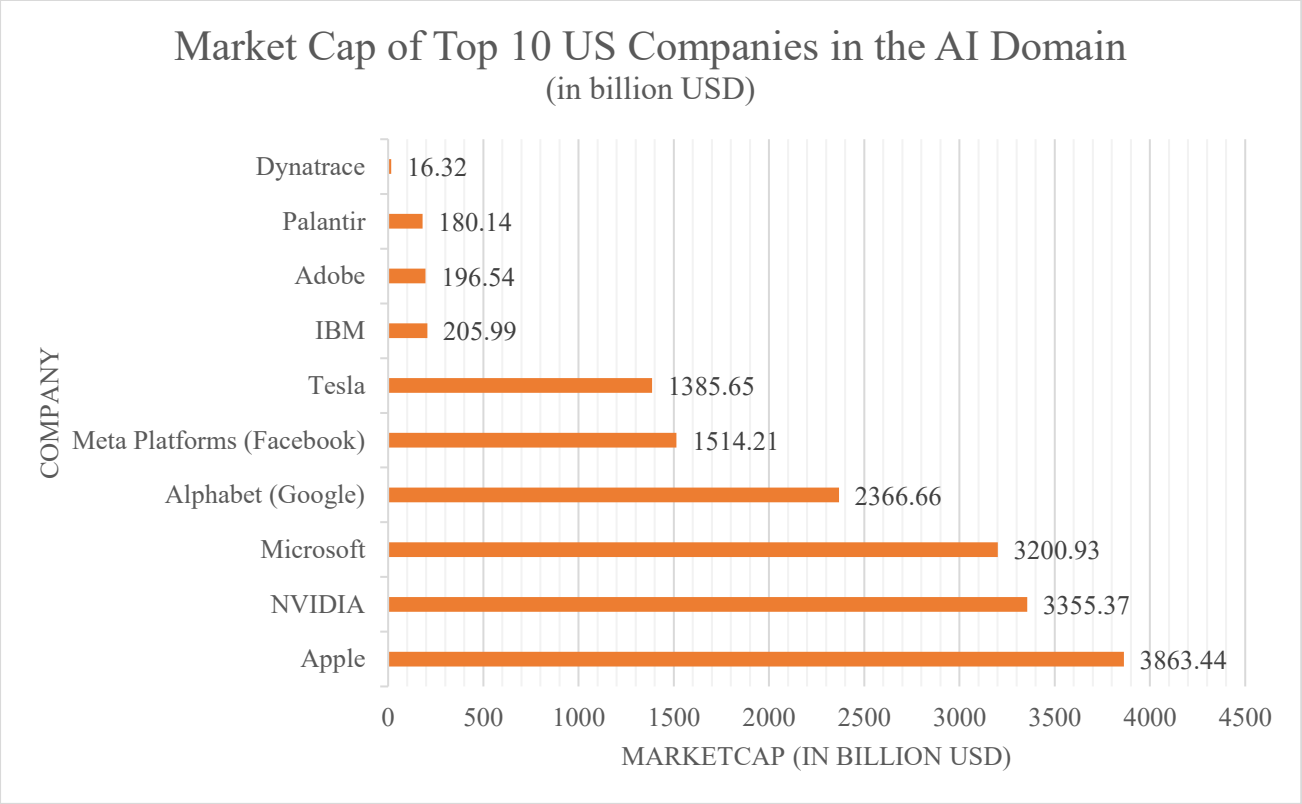
Figure A2.23 and A2.24 – Market Cap Comparison of Companies in the AI Domain

Figure A2.23



Source: Companies' market cap

Figure A2.24



Source: Companies' market cap

Domestic Electronic Transaction Framework – India, in its FTA with the UAE, agreed on a soft obligation to maintain a legal framework governing electronic transactions consistent with the principles of the UNCITRAL Model Law on Electronic Commerce (1996). However, in its latest FTA with the UK, India agreed on a hard obligation to maintain a legal framework consistent with the principles of the UNCITRAL Model Law on Electronic Commerce. Further, in both these FTAs, India committed that it would endeavour to avoid overly burdensome regulation of electronic transactions and facilitate inputs by interested persons in the development of its legal framework for electronic transactions. In the UK FTA, India further committed to endeavour to adopt or maintain a legal or regulatory framework governing electronic transferable records.

India is already a signatory to the UNICTRAL Model Law on Electronic Commerce and the Preamble of its IT Act, 2000, notes that the United Nations, adopted this by resolution A/RES/51/162. The resolution recommends, *inter alia*, that all states give favourable consideration to the Model Law, when they enact or revise their laws, to provide for uniformity of the law applicable to alternatives to paper-based methods of communication and information storage. The Indian Parliament enacted the Information Technology Act, 2000.

Authentication – E-contracts, E-signatures, E-authentication, and Electronic Trust Services.

- E-contracts (electronic contracts) are agreements formed and executed electronically, without the need for physical documents or signatures. India recognises e-contracts under Section 10A of Information Technology Act, 2000, subject to certain exceptions listed in first Schedule of the IT Act.
- E-signatures (electronic signatures) are digital equivalents of handwritten signatures, used to indicate consent or approval on electronic documents. Section 3A of IT Act defines electronic signature and Section 5 of the IT Act recognises the legality of e-signatures, subject to certain conditions and exceptions.
- E-authentication and E-trust services include a range of digital services that ensure the security and trustworthiness of electronic interactions. These services are typically

provided by trust service providers (TSPs). E-authentication is the process of verifying the identity of a user or system before allowing access to online services or transactions.

Under Article 9.6 of the India-UAE FTA, India agreed on a hard obligation to not deny the legal validity of a signature solely on the ground that the signature is in a digital or electronic form. Under Article 12.5 of the India-UK FTA, India agreed to ensure that its legal framework allows for a contract to be concluded by electronic means and its law does not result in an electronic contract being deprived of legal effect, enforceability or validity solely on the ground that the contract has been concluded by electronic means except in circumstances otherwise provided for in its law. Further, Paragraph 2 of the Article laid down a transparency provision to publish the exceptional circumstances referred to in Paragraph 1 on any official website hosted by the central government and review those circumstances with a view to reducing them over time.

Under Article 12.6 of the India-UK FTA, India acknowledges the legality and admissibility of an electronic document, an electronic signature, an electronic seal, an electronic time stamp, the authenticating data resulting from electronic authentication, or of data sent and received using an electronic registered delivery service as evidence in legal proceedings and agreed that it would not deny their legal effect and admissibility as evidence in legal proceedings. The Article further restricts the parties from adopting or maintaining a measure that would prohibit parties to an electronic transaction from mutually determining the appropriate electronic authentication method or prevent parties to an electronic transaction from having the opportunity to establish before judicial and administrative authorities that the use of electronic authentication or an electronic trust service complies with applicable legal requirements.

Paragraph 4 of the Article empowers the parties to lay down the requirement of certification of electronic authentication or electronic trust service by an authority accredited in accordance with its law or performance standards which shall be objective, transparent, and non-discriminatory. The parties further committed to work towards the mutual recognition of electronic trust services and electronic authentication, and to endeavour to engage in regulatory co-operation.

Section 61 and 63 of the Bhartiya Sakshya Adhiniyam (BSA) 2023 pertains to the admissibility of electronic records. It states that any information contained in an electronic record, which is printed on a paper, stored, recorded or copied in optical or magnetic media, is deemed to be a

document and is admissible in legal proceedings without the need for the original device. Further, section 85 of the Adhiniyam lays down the provision for presumption of electronic agreement. Section 86 of the Adhiniyam relates to the presumption regarding electronic records and digital signatures, giving them the same recognition as physical signatures. Section 90 of the Adhiniyam recognises electronic messages as evidence, and courts may presume the integrity of the communication, as it is fed in the computer of the addressee unless proven otherwise.

Similarly, Section 2(y) of Digital Signature (End entity) Rules, 2015, defines the time stamp as a mean of notation that indicates the correct date and time of an action and the identity of the person or device that sent or received the time stamp and is enforced using the time stamp token.

The time stamp token, is defined as a cryptographically secure confirmation generated by applying the digital signature of a time stamping service provider that includes the time when the confirmation was generated.[79]

The office of Controller of Certifying Authorities (CCA) was set up under the Information Technology (IT) Act in the year 2000. The CCA licensed eight certifying authorities (CAs) to issue digital signature certificates (DSC) under the IT Act 2000. Licensed CAs in India may issue certificates for the purpose of time stamping.[80] Adding a trusted timestamp to a code or an electronic signature provides a digital seal of data integrity and a trusted date and time of when the transaction took place.[81]

India recognises the benefits of electronic authentication and electronic trust services. It is recommended that India recognise the legal effect and admissibility of an electronic document, e-signature, e-seal, etc., as evidence in legal proceedings, subject to the conditions otherwise provided for under applicable laws and the regulatory framework. It is also recommended that India accord mutual recognition to electronic trust services and electronic authentication, and to endeavour to engage in regulatory co-operation. It is also recommended to mutually

[79] Section 2(x) of Digital Signature (End entity) Rules, 2015.
[80] Controller of Certifying Authority, Interoperability Guidelines for Digital Signature Certificates issued under IT Act, V. 3.9, (2021). available at: https://cca.gov.in/sites/files/pdf/guidelines/CCA-IOG.pdf
[81] India PKI Forum, Time Stamping, available at: https://www.indiapki.org/time-stamping.html

recognise e-contracts subjected to domestic laws and regulation so that the exceptions listed in the first schedule do not conflict with its FTA obligations.

Digital Identities - A digital identity is the electronic representation of an individual's or entity's identity in the digital space. It consists of a set of data attributes that are used to uniquely identify and verify the identity of a person, organisation or device during online interactions. Digital identities are crucial for enabling secure access to online services, conducting electronic transactions and ensuring trust in digital ecosystems.

India established a statutory body, the Unique Identification Authority of India (UIDAI), under the provisions of the **Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act 2016")** to issue unique identification numbers (UID), named as "Aadhaar", to all residents of India. It has been established to empower residents of India with a unique identity (Aadhaar), and a digital platform to authenticate their identity anytime, anywhere. Aadhaar has become the digital infrastructure of good governance, enabling both ease of doing business and ease of living for residents. It has become the cornerstone of India's digital and social infrastructure, with nearly every sixth person in the world holding this unique identification, symbolising its transformative impact on society.[82] Aadhaar plays a critical role in enhancing the efficiency of social welfare schemes by offering a dependable, unified identity verification system that ensures transparency in service delivery.

India, under the digital trade chapter of its bilateral agreements, proposed an article to ensure co-operation between the parties to mutually recognise digital identities. India, in its FTA with the UAE, recognises the benefits of co-operation among the parties on digital identities to promote connectivity and further the growth of digital trade, and to endeavour to pursue mechanisms to promote co-operation between their respective digital identity regimes. However, it also recognises that parties may take different legal and technical approaches to digital identities. In the India-UK FTA, the parties have favoured pursuing a mechanism to promote compatibility and interoperability of digital identity regimes between the bilateral partners and have agreed to foster technical co-operation, develop comparable protection of

[82]Kumar Santosh, Angral Sheetal, Lakaria Kamna, Iqbal Madiha, Aadhaar: A Unique Identity For the People, PIB, (2024), available at: https://pib.gov.in/PressReleasePage.aspx?PRID=2067940#:~:text=Aadhaar%3A%20Revolutionizing%20Technology%20Across%20India&text=This%20ambitious%20initiative%20has%20grown,services%2C%20benefits%2C%20and%20subsidies.

digital identities, support the development of international frameworks, identify and implement use cases for mutual recognition, and exchange knowledge and expertise on best practices relating to digital identity.

In its FTA with the UAE, India agreed that the parties' respective digital identity regimes would co-operate to better understand each other's legal and technical frameworks and approaches to implementing digital identities. India and UAE also agreed to co-operate with each other in various international forums to support the development of international frameworks on digital identity regimes.

Paperless trading and e-invoicing – Paperless trading refers to the use of electronic means to exchange trade-related information and documents, such as invoices, bills of lading, certificates of origin and customs declarations, between parties involved in a transaction. This process eliminates the need for paper-based documents, speeding up trade processes and reducing the administrative burden.

India continues to demonstrate its commitment to digital and sustainable trade facilitation, as evidenced by its outstanding performance in the recently released United Nations Economic and Social Commission for Asia Pacific's (UNESCAP) Global Survey on Digital and Sustainable Trade Facilitation. The 2023 survey, covering more than 140 economies and evaluating 60 trade facilitation measures, has positioned India at the forefront of global trade facilitation efforts, with an impressive score of 93.55 per cent in 2023 as against 90.32 per cent in 2021.[83] These remarkable scores are a testament to India's relentless efforts to streamline trade processes, enhance transparency and promote co-operation among stakeholders through initiative such as *turant* customs, single window interface for facilitation of trade (SWIFT), pre-arrival data processing, e- sanchit, co-ordinated border management, etc.

In its FTA with the UAE, India agreed to the proposal to oblige parties to endeavour to provide trade administration documents in electronic form. It agreed on a soft obligation to accept digitally administrated trade documents as the legal equivalent to paper documents. India also agreed to publish information on measures related to paperless trading on relevant official websites and make trade administration documents available to the public in an electronic format.

[83] Supra note. 16

Further, India promotes co-operation bilaterally and in international fora in which India participates to enhance acceptance of electronic versions of trade administration documents.

Under the India-UK FTA, Article 12.8, the parties agreed that, to the extent possible, they would make trade administration documents available to the public in electronic form. The Article further stated that, except in cases that violate their domestic law or international law or where doing so would reduce the effectiveness of the trade administration process, the parties will accept a trade administration document submitted electronically as the legal equivalent of the paper version of that document.

The parties further committed to take into account the principles and guidelines of relevant international bodies while developing initiatives concerning the use of paperless trading and, where appropriate, the parties would co-operate bilaterally and in international fora on matters related to paperless trading.

E-invoicing (electronic invoicing) is the process of issuing, receiving and processing invoices in a digital format, typically structured using standards like XML, UBL (Universal Business Language), or EDIFACT. E-invoices are transmitted electronically between businesses and can be integrated directly into accounting and enterprise resource planning (ERP) systems.

The GST Council in India has recommended the introduction of electronic invoice ('e-invoice') in GST in a phased manner. It has many advantages for businesses such as standardisation, inter-operability, auto-population of invoice details into GST returns and other forms (like e-way bill), reduction in processing costs, reduction in disputes, improvement in payment cycles and improved overall business efficiency. E-invoice is a system in which B2B invoices are authenticated electronically by GSTN for further use on the common GST portal. Under the electronic invoicing system, an identification number will be issued against every invoice by the Invoice Registration Portal (IRP) to be managed by the GST network (GSTN). All invoice information is transferred from the einvoice1.gst.gov.in portal to both the GST portal and e-way bill portal in real time. Therefore, it eliminates the need for manual data entry while filing GSTR-1 return as well as generates Part A of the e-way bills as the information is passed directly by the IRP to GST portal.

India recognises the importance of electronic invoicing to increase the efficiency, accuracy and reliability of commercial transactions. It also recognises the benefits of ensuring that the

systems used for electronic invoicing within its territory are interoperable. India, in its FTA with the UAE, agreed to implement cross-border measures related to electronic invoicing based on international frameworks in their territory. It further agreed to share best practices and promote the adoption of international digital and electronic invoicing systems.

The India-UK FTA recognises the importance of electronic invoicing to increase the efficiency, accuracy and reliability of commercial transactions. It recognises the benefits of ensuring that the systems used for electronic invoicing within its territory are able to exchange relevant usable information. The parties agreed to ensure that the implementation of measures related to electronic invoicing in its territory is designed to support the cross-border exchange of relevant usable information, for which the parties will take into account relevant international frameworks when developing measures related to electronic invoicing.

The parties further committed to endeavour to facilitate the adoption of electronic invoicing by juridical persons, promote the existence of policies and processes that support electronic invoicing, generate awareness of and build capacity for electronic invoicing, and share best practices and collaborate, where appropriate, on promoting the adoption of electronic invoicing systems.

India encourages the cross-border interoperability of electronic invoicing and recognises the economic importance of promoting the global adoption of digital and electronic invoicing systems.

Open Internet Access – Open internet access refers to the principle that all individuals and organisations should have unrestricted, equal and non-discriminatory access to the internet. It supports the idea that users can freely access any lawful content, applications and services on the internet without interference from internet service providers (ISPs) or governments. This concept is closely tied to net neutrality, which advocates open and fair treatment of all internet traffic. DoT constituted a six-member committee on net neutrality in January 2015 to recommend overall policy, regulatory and technical responses. Adopting an assimilative, analytical and participative approach to address issues, the recommendations of the committee were placed in the public domain for inputs from stakeholders. The committee report has contributed qualitatively to the different narratives on the subject.

TRAI released its regulation "Prohibition of discriminatory tariffs for data services, Regulations, 2016" on February 8, 2016, which, inter alia, prohibits any service provider from offering or charging discriminatory tariffs for data services on the basis of content.

Under the Digital India Initiative, the government has taken several initiatives to ensure internet connectivity not only in metros but also in tier-2 and tier-3 cities, and in rural and remote areas. As of March 2024, out of the total internet subscribers of 954.40 million in India, there are 398.35 million rural internet subscribers. Further, as of April 2024, out of 6,44,131 villages in the country (villages data as per Registrar General of India), 6,12,952 villages had 3G/4G mobile connectivity. Thus, 95.15 per cent of villages have access to the internet. The total number of internet subscribers in the country has increased from 251.59 million as of March 2014 to 954.40 million in March 2024 at a compound annual growth rate (CAGR) of 14.26 per cent.

The India-UAE FTA recognises the benefits of having the ability to access and use services and applications of a consumer's choice available on the internet, subject to its laws and regulatory framework, and connect the end-user devices of a consumer's choice to the internet provided that such devices do not harm the network and are not otherwise prohibited by the party's laws and regulatory frameworks.

The India-UK FTA provides that, subject to domestic policies, laws and regulations, each party shall endeavour to adopt or maintain appropriate measures to ensure that an end-user in its territory may access, distribute and use a service and application of their choice available on the internet, connect a device of their choice to the internet, provided that the device does not harm the network; they may also access information on the network management practices of their internet access service supplier, as appropriate.

Having access to information on the network management practices of a consumer's internet access service supplier could also benefit the facilitation of digital trade. Although India recognises the benefit of the principle of access to and use of the internet for digital trade, it is recommended to include this Article under the scope of the telecommunication service chapter instead of the digital trade chapter of an FTA.

Data Innovation – Data innovation refers to the process of leveraging data, analytics and emerging technologies to create new products, services, business models or processes that drive

value, enhance decision-making and foster growth. It involves the creative use of data to solve problems, improve efficiency and generate insights that were previously unattainable. Examples include big data analytics, artificial intelligence (AI) and machine learning (ML), Internet of Things (IoT), blockchain, etc.

The Government of India will launch its 5th National Science, Technology and Innovation Policy, a holistic and pragmatic policy dedicated to science, technology and, most importantly, innovation. Science, technology and innovation (STI) are the key drivers for economic growth and human development. The policy aims to reorient STI in terms of priorities, sectoral focus and strategies. The 5th National STIP is initiated jointly by the Office of the Principal Scientific Adviser (Office of PSA) and the Department of Science and Technology (DST). A secretariat with in-house "policy knowledge and data support unit" has been set up at the Department of Science and Technology to co-ordinate the entire process.

The policy aims to bring about profound changes, through short-term, medium-term and long-term mission mode projects, by building a nurtured ecosystem that promotes research and innovation on the part of both individuals and organisations and leads to the establishment of a national STI observatory that will act as a central repository for all kinds of data related to and generated from the STI ecosystem. It will encompass an open centralised database platform for all financial schemes, programmes, grants and incentives existing in the ecosystem. The observatory will be centrally co-ordinated and organised in a distributed, networked and interoperable manner among relevant stakeholders.

Further, MeitY released the Draft National Data Governance Framework Policy on May 26, 2022, for public consultation. Currently, the draft policy is under finalisation. The policy aims to ensure that non-personal data and anonymised data from both government and private entities are safely accessible by the research and innovation eco-system. The policy aims to provide an institutional framework for data/datasets/metadata rules, standards, guidelines and protocols for sharing non-personal data sets while ensuring privacy, security and trust.

The Ministry of Statistics and Programme Implementation (MoSPI) of the Government of India has taken a number of initiatives to transform the statistical data ecosystem, which inter-alia include creation of a data catalogue portal for the dissemination of MoSPI’s key data products, developing a central data repository, e-sigma solution for large socio-economic surveys, as well as a framework for measuring the achievement of sustainable development goals (SDGs).

Under the proposed IT initiatives of the ministry, the Computer Centre (CC) [erstwhile Data Informatics and Innovation Division (DIID)] of MoSPI has been mandated to facilitate imbibing new technology solutions in the field of data acquisition, processing and dissemination, and other related field of official statistics. There is need for continual improvement and innovation in the field of official statistics that can be achieved by setting a data innovation lab (DI Lab). The objectives of the data innovation lab is to promote innovation, adoption of information technology in the field of official statistics, including survey related methodology, and address the challenges being faced by the National Statistical System (NSS). The data innovation lab will create an ecosystem for experimentation, offering new ideas and proof-of-concept through the wide participation of individuals such as entrepreneurs/researchers from national and international organisations, and other organisations including start-ups, academic research organisations and institutes of national and international eminence.

India recognises the importance of data innovation for promoting economic, societal and consumer benefits through improved data-driven services and technologies. It also recognises the importance of creating an environment that enables, supports and is conducive to experimentation and innovation, while also acknowledging the need to protect personal information. It is recommended that data innovation be promoted by collaborating on data projects, including projects involving academia or industry, using regulatory sandboxes as required, co-operating on the development of policies, frameworks and standards for data mobility, including consumer data portability, and sharing research and industry practices related to data innovation.

Open Government Data – Open government data (OGD) is the practice of making government-held data freely available to the public in a structured, machine-readable format, without any restrictions on its usage or redistribution. The goal of OGD is to increase transparency, improve public services, foster innovation and drive economic growth by leveraging data collected by public institutions. However, India has concerns regarding the misuse of government data by countries India deems hostile to its interests such as Pakistan and China.

The union government, through the Ministry of Science and Technology, has formulated the National Data Sharing and Accessibility Policy (NDSAP), with the Ministry of Electronics & Information Technology (MeitY) being the nodal ministry to implement the policy. NDSAP

aims to enable proactive disclosure of shareable data generated by various Government of India entities as open government data on the OGD platform India data.gov.in. The policy aims to facilitate access to Government of India-owned shareable data and information in both human readable and machine-readable forms through a network all over the country in a proactive and periodically updatable manner, within the framework of various related policies, Acts and rules of the government, ensuring wider accessibility and use of public data and information.[84]

Under the India-UAE FTA, India recognises that the use of open data contributes to stimulating economic and social welfare, competitiveness, productivity improvements and innovation. It agreed to ensure that such open data is allowed to be searched, retrieved, used, reused and redistributed freely by the public, to the maximum extent possible, subject to its laws and regulations. Further, India and the UAE agreed to co-operate to identify ways in which each party can expand access to and use open data to enhance and generate business and research opportunities. Facilitating access to and the use of government data may contribute to stimulating economic and social welfare, competitiveness, productivity and innovation.

The India-UK FTA commits to encouraging the expansion of the coverage of government data and information digitally available for public access and use through engagement and consultation with interested stakeholders. It also provides that the parties will provide interested persons with a mechanism to request the disclosure of specific government data and information. It also obliges parties to endeavour to ensure that the data and information is in a machine-readable and open format to the extent possible, and can be searched, retrieved, used, reused and redistributed.

Online Consumer Protection – Online consumer protection refers to a set of laws, regulations, and best practices designed to safeguard consumers' rights and interests in the digital marketplace. Online consumer protection aims to ensure that consumers can engage confidently in digital transactions with a guarantee of fair treatment, privacy, and security. Here also, India has concerns related to jurisdiction challenges in cross-country legal disputes.

To strengthen consumer protection in the era of globalisation, e-commerce and online platforms, the **Consumer Protection Act, 2019,** was enacted on August 9, 2019. It expands

[84]PIB, National Data Sharing and Accessibility Policy, (2012). available at: https://pib.gov.in/newsite/PrintRelease.aspx?relid=80196#:~:text=The%20NDSAP%20policy%20is%20designed,for%20national%20planning%20and%20development.

the definition of "consumer" to include individuals engaging in online purchases of goods or hiring of services. Additionally, the Act defines advertisements to encompass all forms of publicity, including those on electronic media, the internet and websites. Section 94 of the Act, outlines measures to prevent unfair trade practices in e-commerce, direct selling, etc. It empowers the central government to take measures to prevent unfair trade practices in e-commerce and direct selling, and to protect the interest and rights of consumers. To safeguard consumers from unfair trade practices in e-commerce, the Department of Consumer Affairs has also notified the Consumer Protection (E-commerce) Rules, 2020, under the provisions of the Consumer Protection Act, 2019. These rules, *inter-alia*, outline the responsibilities of e-commerce entities and specify the liabilities of marketplace and inventory e-commerce entities, including provisions for customer grievance redressal.

India in its FTA with the UAE recognises the importance of maintaining transparent and effective measures to protect consumers from misleading, deceptive and fraudulent commercial practices when they engage in digital trade. It has been agreed that the two countries would maintain online consumer protection laws to proscribe misleading, deceptive and fraudulent commercial activities to protect consumers engaged in digital trade. To facilitate online consumer protection in their jurisdictions, the parties recognise the importance of co-operation between their respective consumer protection authorities. The parties have further agreed on a soft obligation to publish information about the remedies a consumer can avail of and the legal requirement a business is required to comply with.

India and the UK in their FTA have agree to adopt and maintain measures that provide the same level of protection to consumers engaged in digital trade as provided under their laws to a consumer engaged in other forms of commerce and have affirmed that paragraphs 2 and 3 of Article 16.4 (Consumer Protection – Competition and Consumer Protection Policy) would apply when consumers are engaged in digital trade. The two countries further agreed to promote co-operation between their respective national consumer protection authorities and agencies or other relevant bodies on activities related to online consumer protection. They recognise the importance of improving awareness of and providing consumers access to grievance redressal mechanisms to protect those engaged in an online commercial activity, including for consumers of a party transacting with a supplier of the other party. The countries will also explore the benefits of mechanisms, including alternative dispute resolution mechanisms, to facilitate the resolution of claims concerning digital trade.

ABOUT THE CENTRE

About CRIT

India's Foreign Trade Policy (FTP) Statement 2015-20 suggested a need to create an institution at the global level that can provide a counter-narrative on key trade and investment issues from the perspective of developing countries like India. To fill this vacuum, a new institute, namely the Centre for Research on International Trade (CRIT), was set up in 2016. The vision and the objective of the CRIT were to significantly deepen existing research capabilities and widen them to encompass new and specialised areas amidst the growing complexity of the process of globalization and its spill-over effects in domestic policymaking. Secondly, enhancing the capacity of government officers and other stakeholders in India and other developing countries to deepen their understanding of trade and investment agreements.

About CWS

The Centre for WTO Studies which is a constituent Centre of CRIT, pre-dates the CRIT since it was created in 1999 to be a permanent repository of WTO negotiations-related knowledge and documentation. Over the years, the Centre has conducted a robust research program with a series of papers in all spheres of interest at the WTO. It has been regularly called upon by the Government of India to undertake research and provide independent analytical inputs to help it develop positions in its various trade negotiations, both at the WTO and other forums such as Free and Preferential Trade Agreements and Comprehensive Economic Cooperation Agreements. Additionally, the Centre has been actively interfacing with industry and Government units as well as other stakeholders through its Outreach and capacity-building programs by organizing seminars, workshops, subject-specific meetings, etc. The Centre thus also acts as a platform for consensus-building between stakeholders and policymakers. Furthermore, the inputs of the Centre have been sought after by various international institutions to conduct training and studies.

CENTRE FOR WTO STUDIES

5th to 8th Floor, NAFED House, Siddhartha Enclave, Ashram Chowk, Ring Road, New Delhi – 110014

http://wtocentre.iift.ac.in/