Cite As: Juan Pablo Gómez Moreno,
International Trade and the Rise of Digital Borders
16(1) TRADE L. & DEV. 55 (2025)

INTERNATIONAL TRADE AND THE RISE OF DIGITAL BORDERS

JUAN PABLO GÓMEZ MORENO*

With the advancement of the digital economy, the regulation of cross-border data flows and other matters related to international trade in digital goods and services has become a significant issue on the political agenda. The protection of citizens' data and national security and sovereignty are major concerns for many countries, leading to the implementation of digital borders, such as data localisation, content regulation, geo-blocking, cyber-security laws, and data transfer restrictions, which pose significant challenges to international trade and connectivity.

Policymakers and international organisations must consider a range of solutions that take into account the complexities and nuances of the digital economy to prevent this from happening. This includes developing a multilateral framework that balances the interests of different stakeholders and updating existing trade rules to promote transparency, predictability, and fair competition in the digital economy. Such a framework requires significant international cooperation and consensus-building, which may prove challenging given the current geopolitical climate.

TABLE OF CONTENTS

* Juan Pablo Gómez-Moreno is an expert consultant in international matters. He advises sovereign states and companies in foreign policy and transnational disputes. He teaches at Universidad de los Andes in Colombia. He can be contacted at jp.gomez12[at]uniandes.edu.co.

1. INTRODUCTION

The rapid development of the digital economy has placed the regulation of international trade in digital goods and services at the forefront of the global political agenda. The protection of citizens' data and other types of privileged information, including military, financial, or business-sensitive data, is a key concern for many countries. However, the implementation of measures to safeguard such information has led to the creation of digital borders, such as data localisation, content regulation, geo-blocking, cyber-security laws, and data transfer restrictions. These measures reflect states' attempts to reclaim sovereignty over their regulatory domains and safeguard national security. While these actions aim to address legitimate concerns, they also raise questions about their implications for multilateralism and the free flow of trade, including the potential emergence of digital protectionism and discrimination against digital trade from third countries.

To fully grasp the significance of these developments, it is essential to understand the terms "digital trade" and "e-commerce." The WTO's Work Programme on E-Commerce defines e-commerce as "the production, distribution, marketing, sale or delivery of goods or services by electronic means."[1] This definition is comprehensive, encompassing various forms of digital trade, including cross-border data flows. For the purposes of this research, this definition will be adopted. Moreover, as noted by Kende & Sen, the terms "digital trade" and "e-commerce" are often used interchangeably.[2] While some scholarship distinguishes between the two, this paper will treat them as synonymous, recognising that different regulators may favor one term over the other to describe similar phenomena. This definitional clarity establishes a foundation for analysing the regulation of digital trade within the

[1] World Trade Organization, *Work Programme on Electronic Commerce*, WT/L/274, (Sept. 30, 1998).

[2] Michael Kende & Nivedita Sen, *Understanding Digital Trade and Data Flows*, INTERNET SOCIETY (2019).

broader context of international commerce. While some literature makes a distinction between them, this article will disregard such a difference, considering that regulators in different countries may prefer one expression over another to refer to the same phenomenon.[3]

Against this backdrop, the regulation of digital trade and e-commerce must be examined within a global narrative that increasingly prioritises national and regional rules over multilateral approaches. By focusing on the growing phenomenon of digital borders, this paper will explore their implications for global trade, national sovereignty, and multilateralism, shedding light on the balance between protecting legitimate state interests and preserving the principles of free and fair trade in the digital age.

This article explores the rise of digital borders in the virtual sphere and their specific implications in the context of international trade. It describes the formation of digital borders and their impact on cross-border digital trade, considering the potential for discrimination and trade barriers, including the negative effects of these policies on actors lacking the resources to navigate complex market trade regulations, such as developing countries and micro, small and medium-sized enterprises (MSMEs). Further, the paper examines the role of international agreements and frameworks, such as the World Trade Organisation (WTO) and its different agreements (Covered Agreements), in addressing digital borders and promoting cross-border data flows. This seeks to promote a debate on digital governance and a discussion on the importance of striking a balance between protecting national security and reducing barriers to international trade at a time when States are making strong territorial claims.

This article is structured into four further parts. Part II provides an overview of the importance of digital in today's global economy, and the rise of digital borders, including their concept, scope and rationale. Part III focuses on the effects of digital borders on international trade and connectivity, exploring how they can exacerbate existing competitive inequalities between market actors. Part IV examines the role of existing WTO rules in addressing digital borders and promoting international trade. Finally, the article offers some conclusions and key takeaways Importance of digital trade and rise of digital borders

A. THE PREDOMINANCE OF DIGITAL TRADE TODAY

By 2020, digital trade accounted for approximately 64% of global service exports,

[3] Sherzod Shadikhodjaev, *Technological Neutrality and Regulation of Digital Trade: How Far Can We Go?*, 32 EUR. J. INT'L L. 1221, 1221–1247 (2021).

with a total value of USD 676 billion.[4] Digital trade has led to the emergence of new products and services,[5] playing a fundamental role in facilitating international transactions and global interconnectedness. Consumers have benefited from a streamlined form of trade, including the reduction of transaction costs in processes like transportation and payment. Similarly, the effects of digital trade on the elimination of boundaries have been significant. The suppression of geographical limitations for producers to access new markets has allowed companies all over the world to reach a larger base of customers.[6] This has also had an impact on new opportunities for innovation and entrepreneurship by providing a simpler platform for digital startups and helping the faster dissemination of ideas, projects, and market alternatives.[7] Digital trade is also impacted by the development of specific forms of technology and businesses. For instance, digital trade has been deeply influenced by the internet.[8] One prominent example is the rise of blockchain technology, which enables secure and transparent transactions, facilitating cross-border trade by reducing transaction costs and improving trust between parties.[9] The development of the internet has enhanced aspects of trade like an easier engagement with customers, making online purchases, and catering goods and services to evolving demands.

Another phenomenon that has been key to the development of digital trade and the current economy is data processing. Data processing enables the efficient handling and analysis of vast amounts of information, facilitating real-time decision-making and personalised services in the digital marketplace. A critical aspect of this process is the cross-border flow of data, which allows businesses to operate seamlessly across international boundaries, accessing global markets and resources. However, regulatory measures such as data localisation requirements can impede these flows, potentially hindering the growth of digital trade. For instance, the Organisation for Economic Co-operation and Development (OECD) notes that while cross-border data flows underpin data sharing and promote digital trade, the challenge lies in fostering a global digital environment that enables the movement of data across

---

[4] U.N. Conference on Trade and Development, *Trade Data for 2020 Confirm Growing Importance of Digital Technologies during COVID-19* (Oct. 27, 2021).

[5] Christopher Foster et al., *Digital Control in Value Chains: Challenges of Connectivity for East African Firms*, 94(1) ECON. GEO. 68-86 (Dec. 18, 2017).

[6] PETER WEILL & STEPHANIE WOERNER, What's Your Digital Business Model?: Six Questions to Help You Build The Next-Generation Enterprise (2018).

[7] *Id.*

[8] Susan Ariel Aaronson, *The Digital Trade Imbalance and Its Implications for Internet Governance, Global Commission on Internet Governance*, 25 CHATHAM HOUSE (Feb. 2016).

[9] Demirel, G, Ioannou, *I., Blockchain and supply chain finance: a critical literature review at the intersection of operations, finance and law,* J. BANK FINANC TECHNOL (2022). https://doi.org/10.1007/s42786-022-00040-*1*.

borders while ensuring adequate protection—a concept known as data free flow with trust (DFFT).[10]

Authors have argued that cross-border flows of data have created more value for the world economy than trade in goods.[11] This reality is also reflected in several fields such as the private and public sectors. In the modern corporate world, many companies have acknowledged the financial value of data and appreciated it as an essential asset of their business strategy. This is the case, for example, with companies such as Facebook or Google, who have calculated their earnings in data in billions of dollars per year.[12] Authors have stated that "data are the lifeblood of international trade in the digital age."[13] This shows the high-level significance of data for firms and the level of protection it requires in their campaigns. The public sector has also recognised the importance of data for promoting their interests. For instance, data has become paramount in the measures adopted by political groups and individuals in getting to know better the preferences of their potential electors. Additionally, institutions from this sector such as regulatory agencies use data as a valuable tool to understand the key parameters of a country, for example, the level of income and rate of employment. This is fundamental in the design and implementation of public policies, such as subsidies, welfare programs, tax collection, etc.[14]

Data and technology benefit not only firms and governments but also society by enabling global connectivity and access to information. The internet and social media help individuals stay informed, reinforcing the concept of a global village shaped by globalisation. Beyond practical uses, technology secures personal freedom and facilitates access to fundamental rights, underscoring its societal value. For individuals, technology is not only important due to its instrumental capacity but also because it allows them to secure freedom.[15]

---

[10] OECD, *Cross-Border Data Flows*, https://www.oecd.org/en/topics/cross-border-data-flows.html.

[11] James Manyika et al., *Digital Globalization: The New Era of Global Flows*, MCKINSEY DIGITAL (Feb. 24, 2016), https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows.

[12] Smith, M., *Identity in a Digital World: A New Chapter in the Social Contract*, WORLD ECON. F. (Aug. 2018), https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf

[13] Abendin, J. & Duan, J., *Data Sovereignty and International Trade*,24(1) J. INT'L ECON. L. 5, 1-26 (2021) [hereinafter Abendin & Duan]

[14] OECD, *Tax Administration 2019: Comparative Information on OECD and Other Advanced and Emerging Economies* (2019).

[15] LUCIANO FLORIDI, The Fourth Revolution: How the Infosphere is Reshaping Human Reality (2014).

At the same time, digital means have become essential to access fundamental rights and other similar protections. Education is a typical example of this. Most learning platforms nowadays are open-access, and populations with limited access to the internet face undue burdens in using them. The same applies to entrepreneurship and the digital economy, where MSMEs may not access specific markets due to constraints related to technology.[16] For instance, in rural areas of the Global South, micro-entrepreneurs often struggle to utilise e-commerce platforms effectively due to limited digital infrastructure and lack of technical skills, hindering their ability to reach wider markets. [17] Similarly, in Namibia, rural entrepreneurs face challenges in adopting ICT-enabled services because of inadequate access to technology and insufficient digital literacy, restricting their participation in the digital economy.[18] Additionally, in the United Kingdom, SMEs encounter difficulties in adopting big data and analytics due to limited resources and expertise, which can impede their competitiveness in digitally advanced markets.[19]

This varies from basic inputs like the internet – which allows some companies to offer their products to a wider audience – as well as more sophisticated forms of technology.

B. WHAT ARE DIGITAL BORDERS?

There is little literature on the concept of digital borders. The idea has not been proposed in the relevant literature and features related to it have not been discussed yet. For the purposes of this paper, digital borders are simply understood as measures enacted by States and resulting from their regulatory framework that have the effect of limiting the free flow of information, including the trade of digital goods and services. In the context of international trade, these measures would be typically referred to as 'barriers' (to trade), not borders. However, this article uses this language because, in the context of cross-border data flows, what they do is create de facto borders between users.

---

[16] U.N. Conference on Trade and Development, *Technology and Innovation Report 2021: Catching Technological Waves - Innovation with Equity*, (2021).

[17] *From Digital Divide to Digital Justice in the Global South: Conceptualising Adverse Digital Incorporation*, ARXIV (2021), https://arxiv.org/abs/2108.09783.

[18] *An Exploration of Factors Influencing the Adoption of ICT Enabled Entrepreneurship Applications in Namibian Rural Communities, ARXIV (2021),* https://arxiv.org/abs/2108.09789.

[19] *Trends of Digitalization and Adoption of Big Data & Analytics Among UK SMEs: Analysis and Lessons Drawn from a Case Study of 53 SMEs, ARXIV (2020),* https://arxiv.org/abs/2002.11623.

Digital borders are not good or bad in themselves. They just reflect a reality where certain concerns lead to the establishment of obstacles to the free flow of information. While this article largely questions the rise of digital borders and their impact on a series of issues such as free trade and, most importantly, people's access to information and free data flows, it does not take the stance that the imposition of digital borders is bad per se. On the contrary, as will be discussed in depth in the closing Part of this work, an important consideration to reduce these barriers is paying attention to the rationale behind them and offering States legitimate and reasonable alternatives.

These measures can take many forms. Indeed, it is common nowadays to see governments coming up with new and creative ways to raise digital borders. They may relate to a variety of assets ranging from data to computer centres, servers, and other forms of digital infrastructure. This makes it necessary to have clear definitions of concepts related to said measures like algorithms and source codes. On the one hand, algorithms refer to a set of instructions that must be followed by a program to complete a task. On the other hand, source codes are written by programmers and they each represent the language used in creating software.[20] Some of these source codes are only accessible to firms that developed them (proprietary codes), and others are available to anyone (open access codes).[21] Digital borders, encompassing regulations that control the flow of digital information across national boundaries, significantly impact the accessibility and transferability of source code. Certain trade agreements include provisions that restrict member countries from mandating the transfer of, or access to, proprietary source code as a condition for market entry. These measures aim to protect intellectual property rights and prevent forced technology transfers, thereby fostering innovation and safeguarding competitive advantages.[22] However, such restrictions can also impede regulatory efforts that require access to source code for purposes like ensuring transparency, security, and accountability in software applications. For instance, limitations on accessing source code may hinder the ability of governments to audit algorithms for biases or security vulnerabilities, potentially affecting public trust and safety.[23]
Some typical examples of digital borders that will be discussed in this article are the following:

---

[20] Amandeep Singh et. al., *Open Source Software vs Proprietary Software*, 114(18) INTL. J. COMPUT. APPLICATION 26-31 (Mar. 2015).

[21] Abendin & Duan, *supra* note 13, at 11.

[22] Joshua Levine et al., *Non-tariff Digital Trade Barriers*, (Nov. 14, 2023) https://www.americanactionforum.org/insight/non-tariff-digital-trade-barriers/.

[23] *Algorithms Off-limits? If digital trade law restricts access to source code of software, then accountability will suffer*, INST FOR INFO. L. (2022), https://www.ivir.nl/publications/algorithms-off-limits-if-digital-trade-law-restricts-access-to-source-code-of-software-then-accountability-will-suffer/.

1. *Data localisation policies* – Regulations that require certain types of data to be stored and processed within the geographic boundaries of a particular country or region. These policies mandate that data generated or collected within the jurisdiction must be stored on local servers or data centers, rather than being transferred or stored in other countries.[24]

2. *Geographic restrictions on digital content* – Limitations imposed on accessing or distributing digital content based on the geographical location of the user or the content itself. The most common form of geographic restriction is content blocking or geo-blocking, which involves preventing users from certain regions or countries from accessing specific digital content, such as streaming services, online platforms, or e-commerce websites.[25]

3. *Data-related regulations* – Restrictions on the treatment of personal data, including its transfer to foreign jurisdictions, encompassing data protection standards, cybersecurity laws, and measures to prevent cyber threats such as obligations on businesses and organisations regarding the collection, storage, and processing of personal data.[26]

4. *Content screening* – Policies that restrict the availability or dissemination of certain types of digital content, such as explicit or copyrighted materials.[27] Some governments employ content filtering and censorship mechanisms to control the availability of certain types of digital content, including blocking access to websites, social media platforms, or specific content deemed inappropriate.[28]

While digital borders in the form of data localisation policies, geographic restrictions on digital content, data-related regulations, and content screening measures may be motivated by legitimate concerns, they can have detrimental effects on international trade, access to information, innovation, and fundamental rights. Data localisation policies create barriers to the free flow of data across borders, hindering cross-border data transfers and limiting the global reach of businesses.[29] As a result,

---

[24] Komaitis, K. *The 'wicked problem' of data localisation*, 2(3) J. CYBER POL'Y 355-365 (2017).
[25] Ondrej Hamulak et al., *'This Content is not Available in your Country' A General Summary on Geo-Blocking in and Outside the European Union* 21(1) INTL. COMPAR. L. REV., 153-183 (2021).
[26] CHRISTOPHER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW (2013) https://doi.org/10.1093/acprof:oso/9780199674619.001.0001.
[27] Des Freedman et al. *The impact of the Internet on media policy, regulation and copyright law*, *in* THE INTERNET AND THE MASS MEDIA 102-121 (Lucy Kung et al. eds. 2008).
[28] Ververis, V. et al., *Cross-Country comparison of Internet censorship: A literature review*, 12(4) POL'Y & INTERNET 450-473 (2020).
[29] Potluri, S. R. et al., Effects of data localization on digital trade: An agent-based modeling approach, 44(9) TELECOM M POL'Y (2020), https://doi.org/10.1016/j.telpol.2020.102022.

companies may face increased costs and complexities in complying with multiple data storage requirements, leading to reduced efficiency and competitiveness.[30] Moreover, data localisation can fragment the digital economy, impeding innovation, collaboration, and the development of new technologies that rely on seamless data exchange. These barriers can stifle economic opportunities, hinder market access, and limit the potential for digital businesses to scale and expand globally.

Data localisation often requires companies to store or process data within a country's borders, creating silos that disrupt the free flow of information across jurisdictions. This not only increases operational costs for businesses—particularly multinational companies—but also limits their ability to leverage global data centers or cutting-edge technologies that may be located abroad.[31] It is important to note that data localisation does not necessarily imply a blanket ban on transferring data outside domestic territory. Instead, many regimes allow for conditional cross-border data transfers, contingent upon compliance with specific safeguards, such as adequate privacy protections, contractual obligations, or government approvals.[32]

Geographic restrictions on digital content, such as content blocking or geo-blocking, can significantly limit access to information, services, and opportunities for individuals and businesses in specific regions or countries. This form of digital border creates a fragmented digital landscape, where users are denied access to certain online platforms, streaming services, or e-commerce websites based on their geographical location. Such restrictions undermine the principles of an open and inclusive internet, inhibiting cross-border communication, cultural exchange, and the free flow of knowledge.[33] They can also perpetuate inequalities by denying individuals in certain regions the benefits of digital content and impeding their ability to participate fully in the global digital economy.[34] Similarly, content screening measures aimed at filtering or censoring specific types of digital content can have

---

[30] Matthias Bauer et al., *The costs of data localisation: Friendly fire on economic recovery, in* ECIPE OCCASIONAL PAPERS, EUR CTR FOR INT'L POL. ECON. (2014).
[31] Mira Burri, *The Regulation of Data Flows Through Trade Agreements*, 48 GEO. J. INT'L L. 107, 125 (2017).
[32] OECD, *Exploring the Economic Impacts of Data Localisation*, OECD Digital Economy Papers No. 233, https://www.oecd.org/sti/ieconomy/Exploring-the-Economic-Impacts-of-Data-Localisation.pdf.
[33] Giuseppe Mazziotti, *Is geo-blocking a real cause for concern in Europe?*, 43 EUI LAW (2015).
[34] GIOVANNI DE GREGORIO, *Regulating Geo-Blocking Discriminatory Practices In The Digital Single Market, in* RESEARCH HANDBOOK ON EU MEDIA LAW AND POLICY 190 - 207 (Elda Brogi & Pier L. Parcu eds., 2021).

profound implications for freedom of expression, access to information, and the open exchange of ideas.[35]

Content screening measures, when implemented to protect legitimate interests such as national security, often focus on restricting access to content that incites violence, promotes terrorism, or poses cyber threats.[36] For instance, governments may require the removal of extremist propaganda or hate speech to safeguard public safety and state stability. However, such measures must adhere to principles of legality, necessity, and proportionality to ensure compliance with international human rights standards.[37] While narrowly tailored policies can effectively address security concerns, overly broad or vague regulations risk suppressing dissent, stifling freedom of expression, or limiting access to information under the pretext of national security.[38] Transparency and accountability in enforcing these measures are essential to maintaining a balance between addressing legitimate threats and protecting fundamental rights.[39]

Lastly, while data-related regulations, such as data protection standards and cybersecurity laws, play a crucial role in safeguarding individuals' privacy and ensuring the security of digital transactions, they can impose significant compliance burdens on businesses operating across borders.[40] Inconsistent and divergent data regulations across different jurisdictions can lead to a complex web of legal requirements, making it challenging for companies to navigate and comply with varying standards. This can increase compliance costs, hinder cross-border data transfers, and limit the ability of businesses to leverage data for innovation and growth. Moreover, overly restrictive data regulations may unintentionally impede the sharing of valuable information for research, public health, and other societal benefits, limiting the potential of data-driven initiatives to address global challenges.[41] For instance, during the COVID-19 pandemic, the rapid development and distribution of vaccines relied heavily on the cross-border sharing of genomic

---

[35] Virgílio Almeida et. al., *The ecosystem of digital content governance*, 25(3) IEEE INTERNET COMPUTING, 13-17 (2021).
[36] U.N. Office of the High Commissioner for Human Rights (OHCHR), *Report on the Right to Freedom of Opinion and Expression*, A/HRC/23/40 (2013).
[37] Human Rights Committee, *General Comment No. 34: Article 19 (Freedoms of Opinion and Expression)*, U.N. Doc. CCPR/C/GC/34 ¶¶ 21-22 (2011).
[38] DAVID KAYE, SPEECH POLICE: THE GLOBAL STRUGGLE TO GOVERN THE INTERNET 102 (2019).
[39] U.N. Special Rapporteur on Freedom of Opinion and Expression, *Report on Encryption, Anonymity, and the Human Rights Framework*, A/HRC/29/32 (2015).
[40] Elizabeth Pollman, *Tech, regulatory arbitrage, and limits*, 20 EUR. BUS. ORG. L. REV. 567-590 (2019).
[41] Willem G. van Panhuis et al., *A systematic review of barriers to data sharing in public health*. 14(1) BMC PUB. HEALTH 1-9 (2014) p. 2.

data, clinical trial results, and epidemiological information.[42] Data localisation requirements or restrictions on international data flows could have delayed this process, hindering the global collaboration needed to combat the pandemic effectively.[43] This example highlights the critical balance needed between safeguarding privacy and national security and enabling the free flow of data to support collective problem-solving on a global scale. Most of these considerations, as well as their impact on international trade and how existing regulatory mechanisms may be used to address them, will be considered in the following Parts of this article.

C. WHAT ARE THE POLICY REASONS BEHIND DIGITAL BORDERS?

Regulatory authorities are facing significant challenges in keeping pace with the rapid technological developments of the digital era. Consequently, the intricacies of emerging technologies have resulted in regulatory gaps. For instance, some argue that the WTO's rules have not kept pace with the evolution of international digital trade, meaning that stakeholders basing their policies in the framework of the Covered Agreements have been left helpless.[44]

One notable example is the lack of comprehensive rules addressing data localisation requirements and cross-border data flows. The WTO's General Agreement on Trade in Services (GATS) provides a framework for trade in services, but it does not explicitly address the complexities of digital services, such as cloud computing or data-driven platforms.[45] Similarly, while the WTO's moratorium on customs duties for electronic transmissions has been in place since 1998, it has faced growing criticism for being outdated, as it does not account for the economic realities of modern digital trade, such as the classification of digital goods versus services.[46] Moreover, disputes like the *United States v. China* case concerning technology transfer

---

[42] World Health Organization, *Genomic Sequencing of SARS-CoV-2: A Guide to Implementation for Maximum Impact on Public Health* (Jan. 8, 2021), https://www.who.int/publications/i/item/9789240018440.

[43] *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them, Information Technology and Innovation Foundation* (2021), https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/.

[44] Gary Clyde Hufbauer & Zhiyao (Lucy) Lu, *The European Union's Proposed Digital Services Tax: A De Facto Tariff*, PETERSON INST. INT'L ECON. POL'Y BRIEF (2018) [hereinafter Hufbauer & Lu].

[45] General Agreement on Trade in Services, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183.

[46] WTO, Moratorium on Customs Duties on Electronic Transmissions, https://www.iisd.org/articles/policy-analysis/wto-moratorium-customs-duties-electronic-transmission.

have exposed gaps in the WTO's ability to handle issues related to intellectual property in the context of digital trade.[47] These examples illustrate the challenges stakeholders face when relying on outdated frameworks to navigate the rapidly evolving digital economy.

Even though many times regulatory authorities have a limited understanding of emerging technologies, they have witnessed their impact on society and the economy. Sharing economies in key industries such as transportation and real estate have caused business concerns for traditional groups, while the influence of data on public opinion, including political purposes, has been recognised. Such a regulatory gap has led governments to react with fear, resulting in the introduction of restrictive policies on digital assets.

i. Claiming State sovereignty

Governments' attitudes towards emerging technologies and the regulatory gap can be largely attributed to a misconception of sovereignty. While retaining sovereignty is the cornerstone of a State, many authorities think that emerging technologies pose a risk to their sovereign rights as they move a significant number of things beyond the State's capacity of surveillance and control. However, this is not merely a perception; evidence from existing literature demonstrates that emerging technologies, such as blockchain, cloud computing, and cross-border data flows, have indeed shifted significant matters beyond the traditional jurisdictional reach of States.[48] The misconception lies in equating the inability to control all aspects of these technologies with a complete erosion of sovereignty, rather than recognising the need for adaptive regulatory frameworks that balance sovereignty with the realities of a globalised, technology-driven landscape. This misunderstanding underscores the necessity for policymakers to reimagine sovereignty in the context of digital governance to address regulatory gaps effectively.

For example, with the rise of digital assets and revolutionary technologies such as crypto and digital banks, States have lost track of how money flows within their economy, which poses difficulties for matters like collecting taxes. Beyond these tax-related difficulties, digital assets also pose additional risks that demand urgent attention. The rapid market disruptions characteristic of these assets highlight the need for transparency and robust regulatory frameworks. The lack of uniform data disclosure standards across platforms further complicates aggregate analysis, making it difficult for regulators to develop comprehensive and enforceable policies.

---

[47] Panel Report, *China — Certain Measures Concerning the Protection of Intellectual Property Rights*, WTO Doc. WT/DS542/R.

[48] Mira Burri, *The Regulation of Data Flows Through Trade Agreements*, 48 GEO. J. INT'L L. 107, 125 (2017); ANUPAM CHANDER, THE ELECTRONIC SILK ROAD: HOW THE WEB BINDS THE WORLD TOGETHER IN COMMERCE 102 (2013) [hereinafter Anupam].

Moreover, the pseudonymous nature of many digital assets creates opportunities for money laundering, terrorism financing, and tax evasion, raising serious concerns for national security and financial stability. These risks underscore the critical importance of establishing global standards and cooperative mechanisms to ensure that digital assets contribute positively to economic development while minimising potential harm.

This problem has been called by many names by different authors. For instance, various relevant literature refers to the intangibility, extraterritoriality, and exceptionality of data. As described by Kristen Eichensehr, "the problem is not that data is located *nowhere*, but that it may be located *anywhere*, and at least parts of it may be located nearly *everywhere*."[49] This is exemplified by precedents where multiple authorities have made simultaneous jurisdictional claims on data-related matters. A leading case in this regard was that of *United States v. Microsoft*, where a dispute concerning a claim of the US government to obtain electronic communications stored by the company on a server in Ireland made it to the Supreme Court of the first State.[50]

Sovereignty has long been associated with the concept of territoriality, a key element in determining and delimiting a State's sovereign powers.[51] Traditional legal categories, mostly in areas like public international law, make it challenging to reconcile digital trade and territoriality. The digitalisation of the economy represents a risk to sovereignty as it threatens to dissolve the idea of territory. The question then is: how is the State expected to exercise its jurisdiction over intangible assets? This expectation of territoriality is evident in specific branches of the regulatory arena, such as labour law. Labour law is highly regulated, and little is left to the free will of employers. In many countries, labour rights cannot be negotiated freely between employer and employee, as there are rights that cannot be waived, such as the minimum wage. Similarly, the State expects to exercise significant control over labour matters, such as the terms of employment of its nationals. However, emerging technologies could make most of these pillars tremble, giving place to a need for new and enhanced regulations.[52] Alternative payment methods allow employers to keep the terms of payment of their employees reserved. Additionally, outsourcing, which represents a great problem for traditional employment terms, enables companies to hire services from people in other jurisdictions, which poses challenges

---

[49] Kristen E. Eichensehr, *Data Extraterritoriality*, 95 TEXAS L. REV.145 (2017).

[50] Sharon Bradford Franklin, *The Microsoft-Ireland Case: A Supreme Court Preface to the Congressional Debate*, LAWFARE (Feb. 22, 2018).

[51] Allen Buchanan & Robert O. Keohane *The legitimacy of global governance institutions,* 20(4) ETHICS & INT'L AFF., 405-437 (2006).

[52] J. Berg, Protecting Workers in the Digital Age: Technology, Outsourcing, and the Growing Precariousness of Work 41 COMP. LAB. L. & POL'Y J. 69 (2019).

for States regarding labour regulation.[53] Changing from a context of high control to uncertainty is problematic for traditional labour enforcement agencies.

Similarly, in the intellectual property (IP) arena, there are significant questions about the territoriality of copyright. Rules are unclear regarding issues such as the applicable law in cases where there is the use or sharing of information within several jurisdictions. Governments advocating for data localisation requirements have used sovereignty as a main argument, stating that storing their citizens' data in servers located outside their territory would hinder their sovereignty. For instance, under Law No. 242-FZ, Russia requires all domestic and foreign companies to accumulate, store, and process personal data of its citizens on servers physically located within Russian borders.[54]

Sovereignty concerns are also visible in the field of digital taxes or the taxation of digital goods and services. Therefore, sovereignty claims refer to a state's assertion of its authority to regulate and control matters within its jurisdiction, particularly concerning issues like taxation, citizens' rights, and national security.[55] These claims often overlap with broader concerns, as regulating multinational corporations and safeguarding public interests are inherent aspects of sovereignty. For instance, the 2016 European Commission decision requiring Apple to pay €13 billion in back taxes to Ireland illustrates how sovereignty claims can conflict with supranational frameworks aimed at ensuring fair competition and transparency. Such cases highlight the challenge of balancing national sovereignty claims with adherence to international regulations in an interconnected global economy.[56]

The key problem here is that transactions in cyber-space make it difficult for a regulatory agency or alike to trace the flow of funds between users, which could promote tax evasion. While economic development should not burden the free flow of data, there is a backdrop of scandals involving tax evasion by big tech companies that is unsettling for regulatory agencies. The 2016 EU measure ordering Apple to pay back taxes to Ireland is a clear example.[57]

ii. Protecting citizens' rights

---

[53] A. L. Kalleberg, Precarious Work, Insecure Workers: Employment Relations in Transition, 83 AM. SOCIO. REV. 22 (2018).

[54] Michael Newton, *Russian Data Localization Laws: Enriching "Security" & the Economy,* HENRY M. JACKSON SCH. OF INT'L STUD (Feb. 28, 2018).

[55] *Sovereignty Claim*, COLLINS ENGLISH DICTIONARY, https://www.collinsdictionary.com/dictionary/english-word/sovereignty-claim

[56] European Commission, *State aid: Ireland gave illegal tax benefits to Apple worth up to €13 billion*, (Aug 30, 2016) https://ec.europa.eu/commission/presscorner/detail/en/IP_16_2923.

[57] *Id.*

On the other hand, there are arguments that highlight the importance of protecting citizens' rights. The use of data in digital transactions has become increasingly important in the digital economy. With the rise of big data, companies are now able to collect, store, and analyse vast amounts of data to gain insights into consumer behaviour and preferences.[58] This has raised concerns over privacy and consumer rights as users are often unaware of how their data is collected and used.[59]
Regulators and civilians alike have been shocked by the reality of the business behind data. In response, some countries have implemented strong data protection regimes to prevent abuses by companies. For example, the European Union has implemented the General Data Protection Regulation (GDPR) to protect the privacy and personal data of its citizens. The GDPR establishes strict rules for the collection, processing, and transfer of personal data, and imposes heavy fines on companies that violate these rules. European countries have been harsh in the implementation of these policies, fining Google a sum of EUR 50 million in 2018 for failing to disclose to users how their data was collected.[60] However, despite these efforts, the reality is that most users in other parts of the world remain unaware of the true extent of data collection and processing, and the potential risks that come with it.[61] This is concerning as data analysis can reveal sensitive information about individuals, such as their political affiliations or sexual orientation, which can then be used to manipulate them through targeted marketing or even blackmail.[62] Moreover, data breaches and cyber-attacks pose a serious threat to individual privacy and corporate security. In recent years, there have been several high-profile data breaches, such as the Equifax breach in 2017, which compromised the personal data of millions of people. These breaches expose individuals to the risk of identity theft and financial fraud, among others.

iii. Safeguarding national security

Lastly, digital borders are also said to be justified on grounds of national security. Interestingly, discourses of safeguarding national security have been used by States

[58] David Lyon, *Surveillance, Snowden, and Big Data: Capacities, consequences, critique*. 1(2) BIG DATA & SOC'Y 1-13 (2014), https://doi.org/10.1177/2053951714541861.
[59] Javier López González & Janos Ferencz, *Digital trade and market openness*, 217 OECD (2018), http://dx.doi.org/10.1787/1bd89c9a-en.
[60] Adam Satariano, *Google Is Fined $57 Million under Europe's Data Privacy Law*, N.Y. TIMES (Jan. 21, 2019).
[61] Nili Steinfeld, *"I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment*, 55(B) COMPUT. IN HUM. BEHAV. 992 –1000 (2016).
[62] Nir Kshetri, *Big data's impact on privacy, security and consumer welfare* 38(11), TELECOM M POL'Y 1134-1145.

to promote the protection of sensitive information such as secrets of State and military data through trade-restrictive measures. The same happened with corporate data, which was protected by most domestic and regional laws given the sensitivity of information like trade secrets for market purposes.[63]

In many countries, there are now categories of specially protected data like information about a person's health, political thoughts or religious beliefs. However, the internet and social media opened the possibility of sharing large amounts of information about one or more persons without being able to filter this risk or enable any protections. At the same time, digital platforms are designed to take that data, store it, and analyse it for specific purposes like marketing.[64]

Against this backdrop, how are national security interests at stake? It is not impossible that data treatment can put at risk the stability of an entire country. The case of *Cambridge Analytica* unravelled this reality as it refers to a firm in charge of managing data using and secretly keeping information of millions of Facebook users. Following the scandal, media reported how thousands of profiles were used to manipulate voters in elections in several countries like Malaysia, Kenya, and Brazil, as well as the alleged Russian intervention in the 2016 US presidential election.[65] Another case of interest in this regard is that of *Wikileaks*,[66] which revealed sensitive information about government surveillance and the protection of sensitive information, leading to public outrage due to secret information on issues like the wars in Iraq and Afghanistan.

III. THE IMPACT OF TRADE BARRIERS ON INTERNATIONAL TRADE AND GLOBAL CONNECTIVITY

A. SHIFT TOWARDS NATIONAL AND REGIONAL ALTERNATIVES

To discuss the impact of trade barriers on international trade and connectivity, it is important to consider the historical context of multilateral trade and its paradigm. After World War II, international trade was characterised by free trade and the absence of barriers to trade.[67] Institutions resulting from global agendas like Bretton Woods were rooted in the idea of promoting exchanges between countries seamlessly, with trade barriers being the exception and not the rule. As recognised

---

[63] Sanford J. Grossman & Oliver D. Hart, *The costs and benefits of ownership: A theory of vertical and lateral integration*, 94(4) J. OF POL. ECON. 691-719 (1986).

[64] VIKTOR MAYER-SCHONBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK (2013).

[65] Carole Cadwalladr, *Fresh Cambridge Analytica Leak "Shows Global Manipulation Is out of Control"*, THE GUARDIAN (Jan. 4, 2020) https://www.theguardian.com/uk-news/2020/jan/04/cambridge-analytica-data-leak-global-election-manipulation.

[66] Lyon D*The Snowden leaks and the US empire*, 8 INT'L J. OF COMMC'N 1728-1736 (2014).

[67] Michael D. Bordo & Harold James, *A Retrospective on the Bretton Woods System: Lessons for International Monetary Reform* 24(4) J. ECON. PERSP. (2010).

by the WTO's Appellate Body (AB), one of the objectives of the system was to "put an end to the fragmentation."[68]
Many governments promoted the free exchange of goods and services. Big economies, such as the UK and US, followed an open-frontier and neoliberal policy.[69] These key agendas set the stage for the globalisation of trade and the emergence of multilateral institutions such as the WTO. But there were also shifts in emerging markets and developing countries. Many Latin American countries opened their borders and became a part of the multilateral community.[70] One notable example is the establishment of the Mercosur trade bloc in South America in 1991, which brought together Argentina, Brazil, Paraguay, and Uruguay in a commitment to free trade and economic integration.

However, in recent years, the pillars of this paradigm have been shaken by the imposition of important trade barriers, creating de facto blockages to free and multilateral trade. This shift towards nationalism has been accompanied by discussions about the return to an economy focused on domestic industries and local productivity.[71] The fact that new developments in trade and the digitalisation of the economy coincide with this trend towards nationalism is not something to be taken lightly, as it has important implications for the regulation of digital trade. As such, it is necessary to consider the effects of digital borders as part of this global trend towards nationalism. The imposition of tariffs and other trade restrictions has become a popular tool among some of the world's largest economies, creating significant tensions in the global trading system. For example, the US has imposed tariffs on Chinese goods in an effort to reduce the trade deficit, while China has responded with its retaliatory measures.[72] The UK's decision to leave the EU has also raised concerns about the future of trade relations in the continent.[73] At the same time, many countries are rethinking their approach to international trade, with some advocating for greater protectionism and a focus on supporting domestic industries. This shift towards nationalism in trade policy has been identified as a

---

[68] Appellate Body Report, *Brazil —Measures Affecting Desiccated Coconut,* WTO Doc. WT/DS22/AB/R, ¶18 (adopted Feb. 21, 1997).
[69] Manfred B. Steger & Ravi K. Roy, NEOLIBERALISM: A VERY SHORT INTRODUCTION (2nd ed. 2017).
[70] FREDERICK STIRTON WEAVER, LATIN AMERICA IN THE WORLD ECONOMY: MERCANTILE COLONIALISM TO GLOBAL CAPITALISM (LATIN AMERICAN PERSPECTIVE) (2006).
[71] Maurice Obstfeld, *Globalization and Nationalism: Retrospect and Prospect*, 39(4) CONTEMP. ECON POL'Y 675690 (2021).
[72] Larisa Kapustina et al., *China trade war: Causes and outcomes*73 SHS WEB OF CONF. (2020).
[73] David Blake, *How bright are the prospects for UK trade and prosperity post-Brexit?* 8(1) J. OF SELF-GOVERNANCE MGMT ECON. 7-99 (2020).

global trend by trade theorists.[74] The digitalisation of the economy has also had a significant impact on the way trade is conducted, and the intersection of these two trends creates new challenges in shaping digital trade. Additionally, trade experts have also highlighted a separate, yet similar, trend towards regional alternatives which is of particular popularity in matters of e-commerce.

An example of this is the US, where there are varying data protection rules across different jurisdictions.[75] Developed countries have promoted their own agendas through plurilateral trade agreements, particularly on the free flow of data by restricting measures such as national localisation requirements and government use of data.[76] This trend aligns with calls for plurilateralism as an alternative to the WTO,[77] which allows powerful WTO members to promote new rules from the OECD and FTAs without requiring market access concessions.[78] Notably, this approach may reinforce the dominant position of tech giants who collect vast amounts of data, potentially undermining consumer rights. There are additional regional initiatives of interest in the regulation of the digital economy, such as the Trans-Pacific Partnership (CTPP), which contains regulations that secure the free flow of information and prevent policies on data localisation.[79] An example is Article 14.11, which incorporates a specific restriction on the ability of governments to restrain the cross-border flow of data. There is also a rule preventing the parties from asking software companies for access to their source codes. Similar provisions are in other regional agreements like the Trade in Services Agreement (TiSA).

B. KNOWLEDGE ASYMMETRIES AND (UN)FAIR COMPETITION

As discussed in the previous section, free trade has been the paradigm of international trade for years. Trade, back then, was thought of as an exchange of money for a specific catalogue of goods or services. Therefore, regulations previously were mostly focused on tangible goods like semiconductors, agricultural products and textiles. There is no doubt, however, that there have been important developments in the way we think of objects that could be defined as goods or

---

[74] Dani Rodrik, *Populism and the economics of globalization,* 1(1) J. INTL. BUS. POL'Y 12-33 (2018).
[75] Carsten Rhod Gregersen, *The US Is Leaving Data Privacy to the States and That's a Problem*, BRINK: THE EDGE OF RISK (2019) https://www.brinknews.com/the-us-is-leaving-data-privacy-to-the-states-and-thats-a-problem/.
[76] Meriong Guo, *A Comparative Study on Consumer Right to Privacy in E-Commerce* 3(4) MOD. ECON. 402–407 (2012) [hereinafter Guo].
[77] Rudolf Adlung & Hamid Mamdouh, *Plurilateral Trade Agreements: An Escape Route for the WTO?* 52(1) J. WORLD TRADE 85 (2018).
[78] Jane Kelsey, *The illegitimacy of joint statement initiatives and their systemic implications for the WTO*, 25(1)J. INTL. ECON LAW5, 2-24 (2022).
[79] Gary Clyde Hufbauer & Cathleen Cimino-Isaacs, *How will TPP and TTIP Change the WTO System?* 18(3) J. INTL. ECON L. 679-696 (2015).

services. For instance, the introduction of IP supposed an important shift in this model because it relates to many intangible assets. To that end, specific rules and institutions dealing with it were created.
But nowadays we face an even more complex challenge. Digital trade questions even the existence of a good and its classification. Janow and Mavroidis use the example of 3D printing to show this problem. They say, "think of a US company engaging in 3D for a client in Switzerland. Is a service being exported when recourse to 3D is made, or a good being imported?"[80] The same happens with other platforms like Kindle, which once again blurs the line between goods and services as arguably there is no clear-cut distinction between the e-books and the platform as such. This poses significant challenges for traditional trade rules and institutions.

If there is no clear rule on whether we are dealing with a good or a service, then which rules should relevant stakeholders apply to handle situations related therewith? The Covered Agreements have a rather clear distinction between instruments dealing with goods—as is the case of the General Agreement on Tariffs and Trade (GATT)—and services—which are regulated in the General Agreement on Trade in Services (GATS). This is precisely one of the reasons why, according to standing research, current trade rules would not be equipped to deal with digitalisation.[81]

Relevant literature and past case laws have also clarified how different some of the rules are in each agreement, even if they share some similarities. In the end, this reflects a problem of a regulatory nature because policymakers basing their decisions in the framework of the Covered Agreements are left clueless when it comes to the regulation of digital trade and related matters. In other words, States and institutions interested in creating rules and regulations for international trade in digital markets do not know how to address the complexities of the digital economy. Since the failure of the Doha Round of multilateral negotiations, several stakeholders at the WTO have been concerned about alternative routes to prevent trade barriers in digital trade.[82] Developing countries, for instance, have raised concerns about the effects of the Moratorium imposed on electronic transactions in revenue collection and want to better understand how this issue affects their economies.[83] On the other hand, the development of digital assets has created a disparity between countries

[80] Merit E. Janow & Mavroidis PC, *Digital Trade, E-Commerce, the WTO and Regional Frameworks* 18 WORLD TRADE REV S1-S7 (2019).
[81] Ismall, *supra* note 3, at 7.
[82] Surendra Bhandari, The Doha Round Negotiations of the World Trade Organization: Free or Managed Trade?, SSRN ELEC. J. 1-22 (2012).
[83] General Council, Work programme on electronic commerce: The E-commerce moratorium and implications for developing countries WTO Doc. WT/GC/W/774 (June 4, 2019).

with more developed digital economies and those with less developed ones, making it more difficult for the latter to access markets. In consequence, measures to incentivise digital borders create higher restrictions on market access for these less-developed (LDCs) or developing countries. This presents a problem for fair competition in international trade.

In addition, big tech firms have invested considerable resources in the development of digital assets, such as source codes, which could be at risk if States require them to be made transparent as a condition of operating in certain markets.[84] Empirical evidence has shown that these measures create borders in economic terms for multinational firms in the Information and Communications (ICT) industry.[85] Therefore, in economic terms by imposing additional compliance costs, limits market access, and discourages investment. For instance, when governments mandate the disclosure of source codes or algorithms, multinational firms in the Information and Communications Technology (ICT) industry may face barriers to entering or continuing operations in those jurisdictions.[86] This not only increases operational complexity but also raises concerns about intellectual property theft and the risk of proprietary technology being exploited by competitors.For example, there have been complaints in China regarding this issue.[87] The transfer of source codes has become a point of discussion between the US and the EU, with both agreeing that it should not be a precondition to enter a market.[88] The EU has proposed criteria for identifying situations where the transfer of source codes may be necessary, including as a remedy for competition law violations, protection of IP rights, and security concerns.[89] However, the trend towards digital assets has raised concerns among developing countries that their traditional physical goods may be discriminated against in favour of digital products. One of the issues that developing countries face is the loss of revenue due to the transformation of physical goods into

[84] Jonathan Haskel & Stian, Westlake, Capitalism without capital: The rise of the intangible economy (2017).
[85] Nigel Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, INFO. TECH. & INNOVATION FOUND (2017). https://itif.org/publications/2017/05/01/cross-borderdata-flows-where-are-barriers-and-what-do-they-cost.
[86] Chander *supra* note 48.
[87] Deborah James, Anti-development Impacts of Tax-Related Provisions in Proposed Rules on Digital Trade in the WTO, 62(1) SOC'Y INTL DEVELOP, 58-65 (2019).
[88] Rachel Stelly, *Countries Table Proposals, Talks Continue on WTO E-Commerce Rules*, DISRUPTIVE COMPETITION PROJECT (Aug. 23, 2019) http://www.project-disco.org/21st-century-trade/082319-countries-table-proposals-talks-continue-on-wto-e-commerce-rules/.
[89] World Trade Organization, *Joint Statement on Electronic Commerce, EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce*, Communication from the European Union, WTO Doc. INF/ECOM/22 (Apr. 26, 2019).

digital assets.[90] In 2019, Côte d'Ivoire submitted a text to the WTO highlighting the importance of considering the unique challenges faced by low-income countries and their market actors, mostly MSMEs, in digital trade discussions.[91] Similarly, at the WTO, several Members from LDCs and developing countries have already raised questions on technicalities related to the regulation of digital trade. This creates critical problems at the root of the negotiations, as lacking the knowledge needed to address these discussions with a sufficient level of sophistication makes it difficult for these countries to even enter the debate.[92]

Some authors have already discussed how the absence of a regulatory framework on digital trade has given place to an anti-competitive market where some firms dominate the business.[93] This means that new companies face a de facto barrier in entering the market, a limitation that typically crystallises for MSMEs from LDCs and developing countries.[94] The absence of a regulatory framework on digital trade has allowed dominant firms to leverage their technological prowess, including advanced tools, extensive data reserves, and integrated platforms, to establish de facto barriers that prevent new entrants, particularly MSMEs from LDCs and developing nations, from competing. This dynamic exacerbates economic inequalities, as smaller firms with limited access to technology and funding struggle to penetrate markets dominated by well-resourced competitors.[95] These countries also lack frameworks on issues such as electronic transactions, signatures, and contracts, which exacerbates the technology gap and digital divide. Authors like Roger Brownsword have studied the challenge that regulators face when dealing with developing technologies and elaborated concepts like regulatory connection to consider the question of how regulators get connected to these technologies and how do they stay connected.[96] Interestingly, this literature refers to the Collingridge dilemma, which consists of the following, "regulators tend to find themselves in a position such that either they do not know enough about the (immature) technology to make an appropriate intervention or they know what regulatory intervention is

---

[90] Marko Köthenbürger, *Taxation of Digital Platforms*, (Working Paper no. 41, Vol. 3, Jan. 2020) https://doi.org/10.1093/oso/9780192855244.003.0009.

[91] WTO, Joint Statement on Electronic Commerce - Communication from Côte d'Ivoire, INF/ECOM/49 (Dec. 16, 2019).

[92] Ismall, *supra* note 3 at 24.

[93] Neeraj Rajan Sabitha, *Trade Rules on Source Code- Deepening the Digital Inequities by Locking up the Software Fortress* (INDIAN INST. FOREIGN TRADE, Working Paper, 1–37, 2017).

[94] Abendin & Duan, *supra* note 13, at 3.

[95] United Nations Conference on Trade and Development (UNCTAD), *Digital Trade and Development Challenges in LDCs*, UNCTAD Policy Brief No. 91 (2021), https://unctad.org/system/files/official-document/presspb2021d10_en.pdf.

[96] Roger Brownsword & Morag Goodwin M, LAW AND THE TECHNOLOGIES OF THE TWENTY-FIRST CENTURY: TEXT AND MATERIALS (2018).

appropriate but they are no longer able to turn back the (now mature) technology."[97] As a result of this lack of knowledge and technical capacity, the reality is that the multilateral framework results in a discriminatory trading system that perpetuates asymmetrical power relationships between developed and non-developed Members.[98]

C. CIRCUMVENTING EXISTING TRADE RULES

The rise of digital protectionism poses challenges to the existing trade rules and multilateralism. The principle of free trade has been a fundamental pillar of world trade, shaping the way organisations and trade rules operate. Therefore, any attempt to erect digital trade barriers could potentially violate several trade instruments, including the Covered Agreements. For instance, the imposition of digital trade barriers may violate the national treatment obligation under Article III of the GATT and the most-favoured-nation treatment obligation under Article I thereof. Digital borders could also be contrary to the prohibition of quantitative restrictions under Article XI of the GATT. This could lead to disputes and retaliation reflected in trade-restrictive measures from affected countries.

Similarly, digital borders may also have implications for other types of instruments, such as treaties on IP. Digital protectionism may violate the national treatment obligation under Article 3 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). This Agreement is paramount in digital trade discussions as digital assets may either be subject to IP rights on themselves—as could be the case for software or networks—or implicate other forms of IP-protected content like e-books.[99] Therefore, provisions on IP drafted many years before the expansion of current technology could fall short in dealing with the intricacies of current digital assets and data-related transactions.

From the perspective of the GATS, scholars have shown that most of the topics of high relevance to digital trade are within the scope of this agreement.[100] However, important concerns arise here. One of them is that current rules apply to a closed list of sectors, which leaves a great deal of matters relevant to digital trade outside the regulations. While some have proposed extending the application of the GATS to additional matters—arguably,[101] all forms of trade in services, without

---

[97] *Id*, at 380.

[98] Michael Trebilcock, *Between theories of trade and development: the future of the world trading system*,16(1) J. WORLD INV. & TRADE 132, 122-140, (2015).

[99] *Id.*

[100] Ismall, *supra* note 3 at 5-6.

[101] Rudolf Adlung & Hamid Mamdouh, *Plurilateral Trade Agreements: An Escape Route for the WTO?* 52(1) J. WORLD TRADE 85-108 (2018).

distinction—there are convincing arguments on why this approach would be unworkable in practice as the GATS was designed to be an agreement with a limited scope and an opt-in corpus rather than an expansive approach.

There are additional WTO instruments of great importance to this matter. The Agreement on Technical Barriers to Trade (TBT) could deal with standards applicable to electronic products such as regulations on encryption.[102] For example, some authors have explored how entry-level requirements related to digital assets should be treated as de facto technical barriers to trade.[103] Notably, as discussed before, these requirements are already applied by some countries as a prerequisite for accessing the local market or practising specific actions such as technology transfers or the use of domestic technology.[104] These concerns have already been put on the table by many countries in many official fora. At the General Council of the WTO, Japan suggested several concerns on administrative due process for government intervention in data treatment.[105] This refers to matters such as disclosure of customer data by businesses, release of government and trade secrets, as well as administrative measures forcing actors to disclose source codes and algorithms. However, there are significant issues with the implementation of current regulatory concerns on digital trade in existing trade instruments. For instance, scholars have already argued that it would not be possible to implement solutions developed outside the Covered Agreements in the instruments of the WTO like the GATS.[106]

D. LIMITATIONS ON GLOBAL CONNECTIVITY

Digital trade has the potential to increase global connectivity and enhance the exchange of information and access to the digital economy. However, there is a risk that the benefits of digital trade will not be equitably distributed, leaving marginalised communities without access to the goods and services that are already available to

---

[102] Ismall, *supra* note 3 at 6.

[103] Hufbauer & Lu, *supra* note 44.

[104] Bernard M. Hoekman et al., Transfer of Technology to Developing Countries: Unilateral and Multilateral Policy Options, World Bank (2004), https://openknowledge.worldbank.org/entities/publication/defb7c52-921f-5f2a-90c2-d0de681b8be6.

[105] World Trade Organization, WTO Doc. JOB/GC/177 (Feb. 25, 2019); World Trade Organization, WTO Doc. JOB/GC/180 (Apr. 24, 2019). https://www.wto.org/english/res_e/booksp_e/wtr20_e/wtr20_e.pdf.

[106] Hamid Mamdouh, *Plurilateral Negotiations and Outcomes in the WTO* (KING & SPALDING, Apr. 16, 2021), https://fmg-geneva.org/7-plurilateral-negotiations-and-outcomes-in-the-wto/.

more sophisticated actors.[107] This could lead to a scenario where connectivity is enhanced, but access remains limited for those who lack the basic inputs to obtain goods and services.

This is not a minor issue, as policies related to digital trade are closely linked to broader agendas around access to culture, education, and knowledge. While liberalising trade may benefit market competitors and the tech industry, it may not do much for under-resourced populations. For example, in the case of LDCs and developing countries, digital borders may exacerbate existing inequalities and widen the gap between those who have access to digital goods and services and those who do not.

Scholars have pointed out that the basic existing e-commerce framework has been driven by the US tech industry.[108] This highlights the need for LDCs and developing countries to have a greater say in the development of digital trade policies and regulations. It is important to consider the unique challenges faced by low-income countries and their market actors, mostly MSMEs, when designing regulations for digital trade. This includes addressing issues like the technology gap, lack of frameworks for electronic transactions, and anti-competitive market practices that disadvantage new companies.

The potential benefits of digital trade should be balanced with the need to ensure equitable distribution of those benefits. Policymakers must be cognisant of the potential for digital trade to create or reinforce existing inequalities and should work to develop policies that address these challenges. By doing so, we can ensure that digital trade is a force for positive change, rather than a source of further division and inequity.

IV. THE ROLE OF EXISTING RULES

Various rules and institutions exist to deal with international trade, not limited to the WTO and its Covered Agreements. However, for the purpose of this article, the discussion will be limited to such instruments, which could be a stepping stone for future research aiming to expand the scope of the analysis. The Covered Agreements contain some principles and rules to deal with digital trade in a multilateral economy. To a certain extent, they could provide a regulatory response to the current gap between the knowledge and practice of regulators and that of additional tech-related stakeholders like civil society and corporations. However, the implementation of this

---

[107] K. V. Bhanu Murthy et al., *Digital economy in a global perspective: is there a digital divide?,*13(1) TRANSNAT'L CORP. REV. 1-15 (2021).

[108] Jane Kelsey, *Recalibrating New Zealand's Trade Law Strategy in Turbulent Times*, *in* INT'L LAW IN AOTEAROA N. Z. 455 (Anna Hood & An Hertogen eds., 2021) [hereinafter Kelsey].

alternative faces significant challenges endemic to the organisation, that must be considered and tackled.

A. CHALLENGES

The issue of e-commerce was introduced to the WTO agenda at the Ministerial Conference in 1998.[109] At that time, a Declaration was issued imposing a Moratorium that specified that Members would not enforce customs duties on electronic transmissions. It is also of fundamental importance that WTO stakeholders put digital trade as a key component of the regulatory agenda. Issues around IP pertaining to e-commerce have been discussed in several meetings of the TRIPS Council as a miscellaneous issue under "any other business."[110] For instance, between 1998 and 2003, the TRIPS Council discussed issues such as IP in the digital trade sphere and concluded that further study was necessary due to their complexity.[111]

However, over 20 years later, no consensus has been reached on the most contentious issues.[112] A challenge that WTO regulations face in this regard is the fact that developed and non-developed countries are divided regarding the rules on these matters.[113] As reported by the relevant literature, States have converged on non-contentious issues like electronic signatures and users' protection from fraud but remain divided on the key problems.[114] On issues such as data localisation requirements, the situation is radically different, and Members have been unable to find a middle ground on aspects that trigger strong opposition. Authors like Ido show that this is reflected in the fact that, despite the acknowledgement of the importance of issues such as IP in the context of e-commerce, the TRIPS Council was not actively discussing them by 2019.[115] While there are countries that defend removing digital barriers as a policy matter, states like Japan adopt the stronger position of preventing any form of trade with countries that impose such types of restrictions.

---

[109] Mark Wu, *Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System,* (INT'L CENTRE FOR TRADE AND SUSTAINABLE DEV., Working Paper, 2017), http://www.rtaexchange.org/ [hereinafter Wu].

[110] Victor Ido, Intellectual Property and Electronic Commerce: Proposals in the WTO and Policy Implications for Developing Countries, 62 POL'Y BRIEF 1 (2019).

[111] *Id.*

[112] Katya Garcia-Israel & Julien Grollier, *Electronic commerce joint statement: Issues in the negotiations phase*, CUTS INT'L (2019), http://www.cuts-geneva.org/pdf/1906-Note-RRN-E-Commerce%20Joint%20Statement2.pdf.

[113] Wu, *supra* note 109.

[114] Abendin & Duan, supra note 13 at 1.

[115] *Id*, at 2.

A critical problem, then, is the lack of consensus that ends up leading to the search for national and regional, rather than multilateral, regulations. Some authors have already argued that one of the main benefits of regionalism is solving the gridlock of consensus-driven regulations at the WTO.[116] This means that frustrated by the multilateral system and its lack of progress given the strict rules in place to amend the Covered Agreements, Members have turned to regional agreements and domestic policies to solve urgent needs more efficiently.[117] As argued by Powell and Low, "because of the collective decision-making process of the WTO, negotiation processes can be cumbersome, especially in new areas such as services and information technology products."[118]

Experience has shown that regulatory tools like the Covered Agreements and other initiatives and instruments developed at the heart of the WTO are often destined to fail if they are unable to adapt to changing conditions. For example, the blockage of the WTO's AB due to disagreements among Members led to a legitimacy crisis that took the organisation some time to address.[119] To address these issues, some countries proposed creating a parallel arbitral tribunal to decide disputes related to digital trade, which is again a form of solution outside the original framework of a multilateral rules-based trading system.[120]

Besides, it is clear that digitalisation calls for a review of all trade instruments in the context of digital trade, this is, (re)thinking traditional rules to the unique features of digital technologies. While a specific agreement for this purpose reflects an interest of the Members to incorporate this issue in the agenda, many countries have discussed the importance of including an e-commerce agenda that encompasses all relevant WTO disciplines.[121] Therefore, the question remains: how can the Covered Agreements be adapted to make workable a comprehensive regulation of digital trade? This is a complex issue that will require significant attention and effort from policymakers and stakeholders alike. Right now, however, processes like the

---

[116] Sungjoon Cho, *Defragmenting World Trade*, 27 NW. J. IR'L L. & BUS. 39, 41 (2006).
[117] Peter Sutherland et al., *The Future of the WTO: Addressing Institutional Challenges in the New Millennium: Report by the consultative board*, WTO 19 (2004), https://www.wto.org/english/thewto_e/10anniv_e/future_wto_e.pdf.
[118] Stephen J. Powell & Trisha Low, *Is the WTO Quietly Fading Away: The New Regionalism and Global Trade Rules* 9 GEO. JL & PUB. POL'Y, 261 (2011), http://scholarship.law.ufl.edu/facultypub/382.
[119] Rubens Ricupero, *WTO in Crisis: Déjà Vu All Over Again or Terminal Agony?, in* THE WTO DISPUTE SETTLEMENT MECHANISM: A DEVELOPING COUNTRY PERSPECTIVE, 17-23 (Alberto do Amaral Junior et. al. eds. 2019).
[120] Olga Starshinova, *Is the MPIA a Solution to the WTO Appellate Body Crisis?,* 55(5) J. WORLD TRADE (2021).
[121] World Trade Organization, WTO Doc. JOB/GC/174.

negotiation Rounds and the text of the Covered Agreement suggest that this is far from being a viable solution as reforming these rules has been extremely difficult.

B. POTENTIAL SOLUTIONS

i. Digital sovereignty

At the outset, legal education is necessary to address the challenges of digital trade. Many regulatory authorities view digital trade as a threat to their regulatory capacity, but a transformative discourse could contribute to making it a powerful tool to improve good governance within a state.[122] This can include a variety of data-driven policies and measures favourable to the dissemination and free access of citizens to digital trade platforms like streamlining administrative processes, fostering the development of new businesses, and leveraging statistical data to design better social and economic programs. For instance, sharing economies have been seen by most States as big problems to their sovereignty as they make asset concealment easier and prevent certain forms of surveillance. However, studies suggest that if the State were able to bring these economic actors to the table and regulate digital economies properly, it would actually increase its ability to raise public funds.[123] Similarly, other literature has reviewed in great detail the problem of internet fragmentation, which relates to the possibility that a technology designed to operate beyond borders and to facilitate connectivity worldwide, ends up being broken by national policies and regulatory mechanisms that impose barriers on this framework.[124]

In order to change these views, concepts like territoriality must be deconstructed. This does not mean destroying them completely as they remain fundamental to understanding the applicability of a State's sovereignty. However, rules of private international law like the 'personal statute' demonstrate that the application of laws outside a State's territory is possible and preserves sovereignty. This refers back to what ancient Romans knew as *ius gentium* and allows, for instance, maintaining sovereign powers over someone's marital status based on their nationality, not their location.[125] The territory is still present here, as a national of a State is typically someone born within its borders. But it does not mean that it is incompatible with digital trade and cyberspace. A State can very well remain sovereign over someone in respect of an act committed against that individual overseas or even in an

---

[122] Fernando Filgueiras & Virgilio Almeida, Governance for the Digital World: Neither More State nor More Market (1st ed., 2021).
[123] Bernard Hoekman, *Digital Trade: Opportunities and Challenges,* UN-OHRLLS (2022).
[124] Milton Mueller, Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace (2017).
[125] Jeremy Waldron, *Foreign Law and the Modern Ius Gentium,* 119(1) HARVARD L. REV., 129-147 (2005).

intangible arena.[126] For example, a State can exercise jurisdiction over someone who engages in cybercrime against its citizens or over its own nationals when they are outside the State's borders. Another feasible alternative is rethinking the concept of territoriality. Some authors have argued against data exceptionalism arguing that, "despite the wizardry and wonder of modern technological advances […] cloud-based data resides on servers–essentially large hard drives—and wherever those servers sit, they are subject to territorial assertions of jurisdiction."[127]

All of these policies and ideas for reform are based on a larger concept of digital governance, which appeals to capacity-building and technical training rather than digital borders and trade-restrictive measures. However, digital sovereignty must be differentiated from other concepts under a similar disguise like 'internet sovereignty.' This concept is defended by countries like China but, unlike the proposal of digital governance developed in this paper, it poses a significant risk to fundamental rights, according to many scholars on free connectivity.[128] Specifically, under internet sovereignty, States have the power to surveil the internet and other digital spaces to supervise 'irregular' activity. This is not limited to surveillance activities and may extend to forms of active censorship. Some literature has already differentiated between homonymous yet different concepts relating to sovereignty in a digital space. Taking the example of Buzan et al., these authors have explained the difference between the securitisation move, understood as the act of saying that something is under threat—as it happens, for instance, in the case of national security speeches to promote restrictive measures on digital trade—and the successful achievement of securitisation as such, which relates to the inter-subjective acceptance by all relevant stakeholders of the urgency of said threat—as it could be the case of legitimate reasons behind cybersecurity and data protection policies.[129]

Other authors have differentiated between weak and strong forms of digital data sovereignty. According to them, "weak data sovereignty […] refers to private sector-led data protection initiatives with an emphasis on the digital-rights aspects of data sovereignty, whereas strong data sovereignty favours a state-led approach with an emphasis on safeguarding national security."[130] Nonetheless, this should not mean using the speech of national security or a similar discourse to cover up protectionist

---

[126] Mireille Hildebrandt, *Extraterritorial jurisdiction to enforce in cyberspace? Bodin, Schmitt, Grotius in cyberspace*, 63(2) UNIV OF TORONTO L. J. 196-224 (2013).
[127] Andrew Keane Woods, *Against Data Exceptionalism*, 68(4) STAN. L. REV., 729 (2016).
[128] Min Jiang, *Authoritarian Informationalism: China's Approach to Internet Sovereignty*, 30(2) SAIS REV. OF INT'L AFF. 71-89 (2010).
[129] BARRY BUZAN ET AL., SECURITY: A NEW FRAMEWORK FOR ANALYSIS (1997).
[130] Dana Polatin-Reuben & Joss Wright, *An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet*, USENIX, https://www.usenix.org/conference/foci14/workshop-program/presentation/polatin-reuben.

measures or policies seeking to disrupt data privacy rights. An interesting example is a joint resolution issued by Germany and Brazil in 2013 which addressed data sovereignty as a human rights issue and focused on the problem of violation of privacy rights due to mass surveillance by authorities.[131] Lastly, building digital sovereignty also means striking a balance between the concerns of States and the free flow of data. The fact that many regulatory measures in the digital economy are based on fear and ignorance does not imply that all of them are flawed and unjustified. An important issue then is how to deal with concerns related to real threats. For instance, the exchange of sensitive data in protected industries like financial services is an issue that should be treated with some degree of deference prima facie. These segments of the economy pose a particular concern to national security and the protection of consumers as they are vulnerable to several forms of cybercrime.

ii. Promoting clear, transparent standards

A salient issue of WTO's role in this matter has been the absence of fundamental concepts, which reflects a problem of *vagueness* in the language of the relevant instruments that results in inoperative rules and disempowered Members. Despite this issue having been discussed at the WTO in no less than six conferences, Members have been unable to narrow down key points on the comprehensive regulation of e-commerce and other matters related to digital trade. For instance, there is no consensus regarding definitions and scope of basic words. Another problem is the lack of clarity on the best approach to the problem and whether it is preferable to create new rules or review existing provisions. Moreover, there are also issues of *ambiguity* in the use of certain concepts of the Covered Agreements – as well as those in potential new rules – in the context of digital trade. As a matter of interpretation, for instance, there has been a debate on the use of 'best endeavour' clauses versus mandatory language. Notably, this is already an important issue as there is existing jurisprudence within the WTO on the interpretation and scope of provisions with mandatory language as 'shall'.[132] Eliminating ambiguity in certain language also rises as a priority. Concepts like internet 'sovereignty' put undue power in the hands of Members, making it difficult to identify, assess and control domestic trade policies creating digital borders.

The other large problem is determining how to *balance* the need of Members to have some degree of regulatory space in digital matters and the imposition of protectionist measures. This issue is not new to the WTO, whose decision-making bodies are

[131] G.A. Res. 68/167, The right to privacy in a digital age (Dec. 18, 2013).
[132] Sharif Bhuiyan, Mandatory and Discretionary Legislation: the Continued Relevance of the Distinction under the WTO, 5(3) J. OF INT'L ECON. L. 571 (2002).

familiar with the task of assessing whether certain policies were adopted for a legitimate purpose or not. China is a leading example of sovereign concerns on data-related regulations.[133] For instance, it requires that operators of certain information infrastructure must store data locally under Article 37 of its Cybersecurity Law, and data to be transmitted internationally must pass through a security assessment administered by domestic authorities.[134] Additionally, the government supports alternative providers of similar services like Baidu and WeChat, which raises discussions on trade discrimination as some tech operators are secluded from the market while others may offer their services free from any trade restrictive measures.[135]

Again, under the purview of free trade in the Covered Agreements, these measures should only be allowed for legitimate regulatory purposes. But the problem then is the question of what can be considered a legitimate regulatory purpose. Interestingly, some Members have sought clarification or examples on the scope of legitimate objectives that can be pursued through these trade barriers.[136] However, making such a clarification would be contrary to the standing practice of the WTO. This would *de facto* create a distinction between other types of trade barriers and the ones related to digital trade. There is no clear principle for why they should be differentiated. This is important because it enhances transparency and provides a greater extent of predictability in terms of what can or cannot be pursued through these restrictions, potentially reducing their use. Countries like Argentina and Brazil have put forward important considerations on the possibility of, for example, developing new exceptions for the digital environment.[137]

Proportionality is a key concept in achieving such a goal, and existing instruments and standards in trade law already refer to a similar concept. The necessity test in provisions of the Covered Agreements, such as Article XX of the GATT, covers the general exceptions and has been interpreted as referring to a weighing and balancing test when assessing a measure.[138] Following previous decisions of the WTO's

---

[133] Aimin Qi et al., *Assessing China's Cybersecurity Law*, 34 COMPUT. L. & SEC. REV. 1342 (2018), https://linkinghub.elsevier.com/retrieve/pii/S026736491830315.

[134] People's Republic of China, Law on Cybersecurity (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016), http://www.xinhuanet.com//politics/2016-11/07/c_1119867015.htm.

[135] Christina Maags, *The Limitations of the Great Firewall of China*, FAIR OBSERVER (2019), https://www.fairobserver.com/region/asia_pacific/great-firewall-china-censorship-chinese-news-today-vpn-china-38018/.

[136] World Trade Organization, WTO Doc. JOB/GC/182.

[137] World Trade Organization, WTO Doc. JOB/GC/200/Rev.1 (Dec. 5, 2019).

[138] Csongor István Nagy, Clash of trade and national public interest in WTO law: the illusion of 'weighing and balancing' and the theory of reservation, 23(1) J. OF INTL. ECON. L., 143-163 (2020).

decision-making bodies, necessity can be determined on a case-by-case basis and considering several factors. There are, however, powerful precedents that are very useful for this purpose. For example, the WTO accepts bans on spirits in certain countries based on religious beliefs, even when they are clearly trade restrictive and contrary to the Covered Agreements.

However, the situation is more complex when it comes to public morals, as illustrated by the debate over free internet access. China, for instance, considers it legitimate to regulate the internet domestically by taking actions such as filtering or removing content of a 'sensitive' nature.[139] In addressing issues such as data protection and national security, balancing these competing interests becomes critical. An example of this imbalance is the case of local requirements for data treatment or data localisation standards. The Japanese law on data protection provides a useful point of reference for protecting data, as it is based on four principles that reflect proportionality:

1. *Restrictions on data collection* – According to which, for instance, consumers must be informed that their data is being collected.

2. *Preventing the taking of undue advantage from collected data* – Which limits the scope of use of the data and sets forth that it should only be used for the purposes it was collected.

3. *Securing personal participation of data owners* – This allows data owners to adopt measures such as modifying the data that is stored by a firm; and

4. *Proper management of data* – Which prevents situations such as data theft, alteration or undue circulation.[140]

Similarly, Article 5 of the GDPR includes "Principles relating to the processing of personal data." This provision has similar language to the Japanese regulations, including the rule that data shall be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes."[141] Besides, it adds that further processing of data may take place as long as it is made for achieving purposes "in the public interest, scientific or historical research purposes or statistical purposes."[142] This incorporates an important

---

[139] Feng Yang& Milton L. Mueller, *Internet governance in China : A content analysis*, 7(4) CHINESE J. OF COMMC'N 446-465 (2014).
[140] Guo, *supra* note 76.
[141] GDPR, Art. 5(b).
[142] *Id.*

consideration for a rules based system like the one of the Covered Agreements as it includes explicitly the concept of public interest.

A precedent that can be relevant in addressing issues related to public morals is the *US Gambling* case, which allowed US states to regulate online gambling within their borders while prohibiting gambling from outside their borders. In this case, the US had implemented a ban on online gambling services in order to protect public morals and public order. Antigua and Barbuda challenged the ban at the WTO arguing that it was a violation of US obligations under the GATS. The US, on the other hand, argued that the ban was justified under the general exception clause of Article XX of the GATS, which allows WTO Members to take measures to protect public morals or maintain public order.

In its decision, the Appellate Body (AB) of the WTO agreed that the US ban on online gambling constituted a violation of US obligations under the GATS. The AB found that the US had failed to demonstrate that its measures were necessary to protect public morals or maintain public order, as required under Article XX of the GATS. The AB concluded that the US had acted inconsistently with its GATS obligations by imposing a discriminatory ban on the supply of online gambling services from foreign operators while allowing domestic operators to provide such services.[143]

This precedent illustrates the importance of finding a balance between regulating certain activities while ensuring that international trade is not unnecessarily restricted. Also, this case is of the utmost importance to assess proportionality and 'necessity', as the AB found that the US measure was inconsistent because it allowed some forms of gambling while prohibiting others.[144] Similarly, WTO decision making bodies have condemned in the past other measures that are inconsistent, protecting trade liberalisation by inquiring into the real aims and effects of these regulations.[145]

Existing rules on transparency under the Covered Agreements, such as the notification obligations under the TBT Agreement, could be used to address digital trade barriers. However, there may be a need to adjust or interpret existing rules to account for the unique features of digital trade. Developing and enforcing new regulations could be challenging and may result in duplication and fragmentation of the regulatory landscape.

---

[143] Appellate Body Report, *United States — Measures Affecting the Cross Border Supply of Gambling and Betting Services*, WTO Doc. WT/DS285/AB/R (adopted Apr. 20, 2005).
[144] *Id.*
[145] Appellate Body Report, *United States — Standards for Reformulated and Conventional Gasoline*, WTO Doc. WT/DS2/AB/R (adopted May 20, 1996).

iii. Tackling technical discrimination

The differential treatment of LDCs and developing countries has been recognised in international law for a long time, including in the WTO's Enabling Clause. The Enabling Clause allows developed countries to provide trade preferences to developing countries, without violating the most-favoured nation principle, under certain conditions.[146] However, in practice, this provision has been used sparingly. Literature has found that "although 86.5% of all regional trade agreements in force involve one or more developing countries as members, and nearly half of all RTAs in force involve only developing countries, the Enabling Clause has been invoked as legal cover for only 15.4% of all RTAs in force."[147] Similar provisions may be found in additional Covered Agreements.

The idea behind differential treatment (S&DT) is that developing countries face structural disadvantages that hinder their ability to compete on an equal footing with developed countries in the global economy.[148] The mechanisms provided for by these provisions have been helpful in promoting development and addressing trade imbalances. However, there have been difficulties in applying these provisions, particularly in determining which countries are eligible for S&DT and to what extent.[149] Further, S&DT in the context of digital trade is special and raises new and complex challenges that do not have a clear precedent that policymakers and other stakeholders may rely on. Differences in this scenario are related to sophisticated forms of technology rather than any form of trade in goods and services. While they may be similar to traditional trade measures in aspects like bureaucratic capacity and technical requirements, technical differences in the digital arena require expert knowledge to be understood and dealt with properly.

In any event, the reality is that, since the 1998 WTO Declaration on e-commerce issues, Members have recognised that measures relating to digital trade must consider the 'economic, financial, and development needs of developing countries.' However, it is unclear how this plays a role in practice. In the context of digital trade discussions, some Members – unsurprisingly including LDCs and developing

---

[146] Amrita Narlikar, Fairness in international trade negotiations: Developing countries in the GATT and WTO, 29(8) WORLD ECON. 1005-1029 (2006).

[147] Won Mog Choi & Yong – Shik Lee, Facilitating Preferential Trade Agreements between Developed and Developing Countries: A Case for Enabling the Enabling Clause, 21 MINN. J. INT'L L. 1 (2012).

[148] Paola Conconi, & Carlo Perroni, *Special and differential treatment of developing countries in the WTO*, 14(1) WORLD TRADE REV. 67-86 (2015).

[149] Bernard Hoekman, *Operationalizing the concept of policy space in the WTO: beyond special and differential treatment* 8(2) J. OF INT'L. ECON. L., 405-424 (2005).

countries – have already raised multiple questions for General Meetings about the application of S&DT and how it can be implemented effectively in the digital economy. Responses, however, are lacking both from the organisation and from other countries.

Given the rapidly changing nature of digital technologies and the growing importance of digital trade, it is important to find ways to ensure that LDCs and developing countries are not left behind and can benefit from the opportunities offered by digital trade. But current alternatives—largely supported by developed countries—are going in the opposite direction. In the case of Joint Statement Initiatives (JSIs), there is an interesting intersection of open regionalism and technical discrimination. JSIs are negotiating tools initiated by some WTO Members who seek to advance discussions on certain trade-related issues without adhering to the rule of consensus decision-making applicable in WTO negotiations. Put in terms of Prof. Jane Kelsey, who had studied the development of JSIs on e-commerce, these instruments are contrary to the WTO's principles of multilateralism, Member-driven consensus, decision-making and S&DT. Additional research has pointed out that JSIs are at odds with the application of any form of S&DT as new rules are drawing practices from the OECD and FTAs of developed countries, shaping the framework of digital trade based on rules that they already have but which are not attuned to the situation of developing countries.[150] At the same time, it is important to consider what is the stance of LDCs and developing countries in this regard? This question has a simple answer: they are also against such initiatives. Some developing Members, like India and South Africa, have already questioned the legitimacy of JSIs on similar grounds as those discussed by the literature.[151]

It is important to carefully consider the implementation of any regulatory agenda and its potential effects on LDCs and developing countries. Proposals from developed countries could have significant negative implications for other sovereign States. For example, if source codes are protected by patents, this could disincentivise new companies from entering these markets, as they would face additional costs to acquire licenses. Such a measure could also prevent local software developers in developing countries from using source codes subject to licenses and developing their own products. Therefore, while it is important to protect IP, there should also be consideration of the potential impact on the development and growth of digital industries in LDCs and developing countries. National entities at LDCs and developing countries also need to improve their knowledge of issues such as cybersecurity. Technical assistance and cooperation are critical aspects in this regard. States can share their expertise on technical matters such as encryption and network security. Business firms, on the other hand, are more interested in sharing

[150] Kelsey, *supra* note 78, at 8.
[151] *Id.* 2-24.

information on best practices and industry standards. By collaborating with each other, national entities can enhance their cybersecurity capabilities and ensure the security of their digital infrastructures. This is particularly important for said countries, which often lack the resources and expertise to deal with sophisticated cyber threats.[152] Technical assistance and cooperation can help bridge this gap and promote a more secure and inclusive digital economy.

Research has identified some of the greatest advantages of e-commerce to be reducing costs and barriers of entry into markets and offering MSMEs better competitive opportunities against larger counterparts.[153] These objectives align with the cornerstones of the rules-based trading system and should ideally be promoted through the rules and mechanisms provided in the Covered Agreements. This implies that the organisation has a responsibility to pursue such harmonisation. Furthermore, the fact that digital trade is being hindered while trade rules fail to address these issues raises serious concerns about the legitimacy of the WTO from a development perspective, especially considering that LDCs and developing countries have been marginalised in trade rule discussions for years.[154]

V. CONCLUSIONS

As discussed in the previous sections, the development of a digitalised global economy has created important regulatory challenges to States. This has led to the implementation of digital borders on the basis of fears like the loss of national sovereignty, surveillance, and regulatory powers, which are measures that create restrictions on the free flow of information. But digital borders pose a significant challenge to international trade and connectivity, limiting the freedom of users and creating a risk of States using pretexts like protecting consumers and safeguarding national security to advance protectionist measures that could strongly hinder free competition in technology.

In order to address these challenges, policymakers and international organisations must consider a range of solutions that consider the complexities and nuances of the digital economy. One potential solution is to develop a multilateral framework that addresses the unique challenges of digital trade. This framework should be designed to balance the interests of different stakeholders, including governments,

---

[152] Ellada Gamreklidze, *Cyber security in developing countries, a digital divide issue: The case of Georgia*, 20(2) J. OF INT'L COMMC'N 200-217 (2014).

[153] *Debating the Future of E-Commerce and Digital Trade in Buenos Aires*, 21(40) BRIDGES NEGOTIATION BRIEFING 14-19 (2017), https://www.tralac.org/images/Resources/MC11/bridges-negotiation-briefing-an-ictsd-guide-to-the-buenos-aires-ministerial-december-2017.pdf.

[154] Kelsey, supra note 78, at 6.

corporations, civil society, and consumers. However, these discussions have been on the table for decades without a comprehensive or effective instrument being released at leading fora like the WTO. On the contrary, today countries are shifting towards national and regional alternatives like regulating digital trade domestically, in FTAs or through JSIs.

Another possible solution to the problem at hand is to strengthen and update existing international trade agreements, such as the different Covered Agreements. This would involve developing new provisions that specifically address digital trade and removing existing provisions that may hinder the growth of the digital economy. For example, the GATS could be updated to include new commitments on cross-border data flows, while the TRIPS could be amended to provide greater clarity and protection for digital IP. Aside from modifying existing rules or creating new ones, another option is to use existing practice to promote interpretations that are fit for digital trade's unique features. This includes developing clear and transparent standards on digital sovereignty through resources like past case law on necessity and proportionality.

In any event, the WTO and its community have a major problem figuring out how to work out these rules with plurilateralism. As identified by Sauvé, there is a problem in negotiating plurilateral agreements within a framework that commands a multilateral instrument.[155] These solutions should also aim to promote transparency, predictability, and fair competition in the digital economy. However, developing such a framework will require significant international cooperation and consensus-building, which may prove challenging given the current geopolitical climate. An effective change would therefore require surpassing the current status of debates on digital trade, where lack of consensus and conflicting regulatory agendas have become the rule.

Deconstructing concepts like territoriality can help change the perception of digital trade as a threat to regulatory capacity and make it a tool for good governance. These ideas, rooted in traditional concepts of other fields of law, should be reconsidered in light of today's economy and social relations. For instance, governments could promote the development of good governance practices in anything related to digital trade and the flow of data. This would help enhance a healthy form of digital sovereignty, avoiding problems of trade-restrictive and poorly justified regulatory policies.

---

[155] EUR. UNION COMMITTEE ON INT'L TRADE, *Workshop: The Plurilateral Agreement on Services*, 9 (Mar. 26, 2013), https://www.europarl.europa.eu/RegData/etudes/workshop/join/2013/433722/EXPO-INTA_AT%282013%29433722_EN.pdf.

Additionally, it is important to address the broader issues of economic inequality and exclusion that underlie many of the challenges of digital trade. This requires a commitment to inclusive growth and development, as well as policies that support access to digital infrastructure and technology for marginalised communities. By ensuring that the benefits of digital trade are shared more equitably, policymakers can help to reduce the negative effects of digital borders and promote greater international connectivity.

While there is no one-size-fits-all solution to the challenges of digital trade, and a range of approaches will need to be considered in order to address the complex issues involved, the solutions outlined in this article represent some possible avenues for policymakers and international organisations to explore in their efforts to promote fair, transparent, and inclusive digital trade.