JOURNAL OF INTELLECTUAL PROPERTY AND HUMAN RIGHTS

Volume: 4 Issue: 7 | july–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

Contractual Frameworks Regulating Digital Trade in International Law

Alijonov Ayubjon Qobiljon ugli
Lecturer of Tashkent State University of Law

Abstract: In the age of digital globalization, international trade is increasingly conducted through digital means, necessitating robust legal frameworks to regulate cross-border electronic transactions. This article explores the principal contractual frameworks that govern digital trade in international law, including WTO agreements, bilateral and regional free trade agreements (FTAs), and instruments by UNCITRAL and UNCTAD. The analysis focuses on the intersection of traditional trade law principles and emerging digital realities, evaluating the adequacy of current treaties, highlighting legal gaps, and proposing reforms. The article further addresses data flow governance, digital services, cybersecurity obligations, and consumer protection within the architecture of international digital trade law.

Key words: Digital trade, international law, WTO, FTAs, UNCITRAL, cross-border e-commerce, digital services, data governance, cyber law, international agreements.

Introduction. The rise of digital technologies has fundamentally reshaped the landscape of international trade. From cloud computing and artificial intelligence to blockchain and big data analytics, digital technologies have enabled the creation of new products, new services, and entirely new markets. This transformation has resulted in the emergence of ***digital trade***-a dynamic and evolving domain that transcends traditional boundaries of goods and services by incorporating the transmission of data, digital delivery, and the automation of cross-border transactions.

Despite its growing economic importance, the legal architecture governing digital trade remains fragmented and outdated. Many of the foundational agreements that govern international commerce, such as those under the World Trade Organization (WTO), were crafted in an era before the advent of the digital economy. As a result, they often struggle to provide clear guidance on issues like data flows, source code protection, and digital platform regulation.

The objective of this article is to provide a detailed and critical examination of the primary **contractual frameworks** that currently regulate digital trade in international law. In particular, it focuses on WTO agreements, UNCITRAL model laws, and key provisions in bilateral and regional trade agreements such as the USMCA, CPTPP, and DEPA. This analysis assesses the **legal adequacy, coherence, and enforceability** of these instruments, identifies the gaps and inconsistencies within them, and explores proposals for **modernizing digital trade governance** in a manner that balances trade facilitation with national policy objectives, including data privacy, cybersecurity, and consumer protection.

Defining Digital Trade in International Law. **Digital trade** is a term that lacks a universally accepted legal definition, but its conceptual scope has been increasingly clarified through multilateral and academic discourse. According to the Organisation for Economic Co-operation and Development (OECD), digital trade involves "digitally ordered and/or digitally delivered transactions that can involve both goods and services".[1] This definition reflects the duality of digital trade—its ability to operate within and across the domains of goods and services, underpinned by the **cross-border flow of**

[1] OECD. (2019). *measuring the digital transformation: A roadmap for the future*. OECD Publishing. https://doi.org/10.1787/9789264311992-en

Volume: 4 Issue: 7 | july–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

data.

Digital trade includes, but is not limited to:

- The cross-border purchase and delivery of digital goods (e.g., e-books, digital music, software)
- The provision of services through digital platforms (e.g., video streaming, telemedicine, financial technology)
- Licensing of intellectual property through online platforms
- Participation in digital marketplaces or platforms (e.g., Amazon, Alibaba)
- Data storage and processing across jurisdictions via cloud services
- Internet of Things (IoT) and machine-to-machine communications with commercial purposes

Moreover, **data flows** form the backbone of digital trade. Without reliable and secure flows of personal, commercial, and machine-generated data across borders, most digital trade activities cannot take place. This centrality of data introduces legal challenges surrounding sovereignty, privacy, surveillance, and competition—issues that are not yet fully addressed within most existing trade agreements.

Digital trade differs from traditional e-commerce in that it encompasses not only online retail but also services and industrial activities facilitated through digital infrastructure. As such, digital trade cuts across multiple legal domains including intellectual property law, telecommunications regulation, contract law, and data protection frameworks—making it **a multidisciplinary challenge** for international legal regimes.

WTO Legal Framework. The **World Trade Organization (WTO)** provides the foundational legal infrastructure for global trade. However, its capacity to effectively regulate digital trade is **constrained by the fact that most WTO agreements were negotiated before the digital economy emerged as a dominant force.** Nevertheless, several WTO instruments have been adapted or interpreted to cover aspects of digital trade.

The General Agreement on Trade in Services (GATS). **The General Agreement on Trade in Services (GATS),** adopted in 1995 as part of the Uruguay Round, establishes a multilateral legal framework for trade in services. It remains one of the primary instruments under which digital services are governed.

GATS classifies services into four "modes of supply":

- **Mode 1:** Cross-border supply (e.g., a U.S. software company selling licenses online to a buyer in Brazil)
- **Mode 2:** Consumption abroad (e.g., users traveling to another country to access digital services)
- **Mode 3:** Commercial presence (e.g., a company establishing a subsidiary abroad)
- **Mode 4:** Presence of natural persons (e.g., software engineers temporarily working in another country)

Digital trade primarily operates through Mode 1 and, to some extent, Mode 2, placing these squarely within GATS' remit. For example, video streaming, cloud storage, fintech applications, and SaaS (software as a service) models fall within the purview of Mode 1 supply. However, GATS was not designed with data governance, source code protection, or platform liability in mind. As such, while GATS enables digital service liberalization, its **legal silence on key digital trade elements** limits its regulatory effectiveness.

Volume: 4 Issue: 7 | july–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

Moreover, **GATS commitments are often narrow and vary by country**, which allows WTO members to selectively open their markets for certain digital services. Many developing countries have made minimal commitments in digitally-intensive sectors like telecommunications, financial services, and software.

The Information Technology Agreement (ITA). The **Information Technology Agreement (ITA)**, concluded in 1996 and expanded in 2015, is a plurilateral agreement among WTO members that eliminates tariffs on a wide range of IT products, including:

- Semiconductors
- Computers and peripherals
- Telecommunications equipment
- Integrated circuits
- Smartphones and tablets

Although the **ITA does not address digital services or data governance**, it plays a vital role in supporting digital trade by ensuring access to affordable technology hardware. The 2015 expansion of the ITA added 201 new tariff lines, estimated to cover around $1.3 trillion in annual trade.[2]

However, the ITA **lacks enforceable commitments on cybersecurity standards, encryption devices, or software products**, leaving substantial legal grey areas in digital commerce infrastructure. Its technological scope also excludes many emerging digital tools such as artificial intelligence systems or blockchain infrastructure.

E-Commerce Work Programme and Moratorium. In 1998, the WTO established a **Work Programme on Electronic Commerce** to explore how existing trade rules apply to e-commerce and to identify areas requiring new legal instruments. Key areas of examination include:

- Classification of digital products (goods vs. services)
- Customs duties on electronic transmissions
- Access to markets and infrastructure
- Privacy, security, and consumer protection

One of the most significant developments under this programme has been the **moratorium on customs duties on electronic transmissions**, which WTO members have renewed biannually since 1998. The moratorium prohibits WTO members from imposing tariffs on cross-border digital transmissions such as software, video, and data files.

However, the moratorium has faced criticism:

- **Developing countries**, including India and South Africa, argue that the moratorium limits their fiscal autonomy and harms domestic industries.
- **Developed countries**, particularly the U.S. and the EU, view it as essential to maintaining a free and open internet.

Moreover, the **classification of digital products** remains unresolved. There is no consensus on whether a digital product (e.g., a downloaded movie) should be classified as a good, a service, or an intellectual property product. This ambiguity affects the application of WTO rules on tariffs, market access, and national treatment.

[2] WTO. (2015). *Ministerial Declaration on the Expansion of Trade in Information Technology Products*. World Trade Organization. https://www.wto.org/english/news_e/news15_e/mc10_23dec15_e.htm

Volume: 4 Issue: 7 | july–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

To date, **no binding multilateral agreement on digital trade has emerged under WTO auspices,** though exploratory discussions continue under the **Joint Statement Initiative (JSI) on E-Commerce,** launched in 2019 and involving over 80 WTO members. These negotiations address topics such as:

- Cross-border data flows
- Data localization
- Source code protection
- Electronic contracts and authentication

Yet the JSI faces both **legal and political obstacles,** particularly given opposition from some non-participating WTO members and concerns about potential conflicts with domestic regulatory sovereignty.

UNCITRAL Model Laws and Conventions. The United Nations Commission on International Trade Law (UNCITRAL) has played a pivotal role in creating **harmonized legal instruments** to facilitate digital transactions across borders. Unlike WTO's trade-oriented framework, UNCITRAL focuses on establishing **uniform contract law principles and procedural standards** that underpin the functionality of digital commerce. Its model laws have been voluntarily adopted or adapted into national legal systems, serving as a global reference for regulating electronic transactions.

Model Law on Electronic Commerce (1996). The **Model Law on Electronic Commerce (MLEC)** was adopted by UNCITRAL in 1996 to address the legal uncertainties surrounding the use of electronic means in international commercial transactions. At its core, the MLEC introduced the **"functional equivalence"** principle, asserting that electronic communications and digital records should be accorded the same legal validity as their paper-based counterparts.

Key features of the MLEC include:

- Legal recognition of **electronic messages (data messages)** as evidence and contract formation tools.
- Legitimization of **electronic signatures** and authentication processes.
- Endorsement of the **"technology neutrality"** principle, allowing countries to adopt diverse forms of secure electronic systems.
- Establishing standards for **time and place of dispatch and receipt** of data messages, crucial in resolving cross-border contractual disputes.

Over 80 countries have incorporated MLEC provisions into their domestic legislation. The law has been particularly influential in **supporting the growth of cross-border e-commerce,** as it reduces legal friction by aligning contract law principles with digital realities.[3] Moreover, it fosters trust in digital environments by creating enforceable rules that facilitate **reliable, secure, and predictable e-transactions.**

***Model Law on Electronic Signatures (2001)*.** Building upon the MLEC, the **Model Law on Electronic Signatures (MLES),** adopted in 2001, offers a more detailed regulatory framework for the use of electronic signatures in commercial transactions. Its main objective is to promote **interoperability** and **mutual recognition** of electronic signature systems between jurisdictions.

[3] UNCITRAL. (1996). *Model Law on Electronic Commerce with Guide to Enactment*. United Nations. https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce

Volume: 4 Issue: 7 | july–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

The MLES emphasizes:

- The **non-discrimination principle,** which ensures that contracts cannot be denied legal effect solely because they were signed electronically.
- Standards for **"reliable" electronic signatures**, incorporating technical and procedural benchmarks to assess validity and authenticity.
- Guidance on **certificate-based and third-party trust systems**, particularly relevant in cross-jurisdictional trade.

By addressing the technical and procedural aspects of digital signatures, MLES provides a legal infrastructure to promote **cross-border trust and enforceability.** Countries that have adopted this model law—such as Singapore, South Korea, and Colombia—report a marked increase in the efficiency and speed of contract execution and legal enforcement.

New Developments. Recognizing the increasing importance of data flows in digital trade, **UNCITRAL is currently working on a new legislative instrument: a Model Law on Cross-Border Data Flows and Data Protection,** slated for finalization in the coming years. This development reflects a significant **paradigm shift** in international legal thinking-acknowledging that **data is not only an economic asset but also a regulatory object,** raising profound questions about jurisdiction, human rights, and national security.

This proposed law aims to:

- Establish **uniform principles for regulating data transfers** across jurisdictions.
- Create **legal certainty** for businesses engaging in cross-border data processing.
- Provide **exceptions and safeguards** for national security, public order, and data privacy.
- Align with other instruments such as the **Council of Europe's Convention 108+** and regional frameworks like the **EU General Data Protection Regulation (GDPR).**

If adopted widely, this model law could significantly **harmonize divergent regulatory approaches** and support a more **predictable environment for digital trade,** especially for small and medium enterprises (SMEs) in emerging economies.

Bilateral and Regional Trade Agreements. Given the **slow pace of multilateral consensus** within the WTO, many states have turned to **bilateral and regional trade agreements (RTAs)** to advance digital trade agendas. These agreements are increasingly incorporating **dedicated digital trade chapters** or at least digital-related provisions—covering issues such as data flows, e-signatures, cybersecurity, source code protection, and platform governance.

USMCA and the Digital Trade Chapter. The **United States-Mexico-Canada Agreement (USMCA),** which replaced NAFTA in 2020, features one of the most advanced digital trade chapters in modern treaty practice (Chapter 19). The chapter includes the following groundbreaking elements:

USMCA's approach is both **comprehensive and enforceable,** with dispute settlement mechanisms applicable to digital trade violations. It has become a **model for future U.S. trade agreements,** including negotiations with the United Kingdom, Kenya, and Indo-Pacific Economic Framework (IPEF) partners.

CPTPP and DEPA. The **Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)** and the **Digital Economy Partnership Agreement (DEPA)** represent cutting-edge attempts to define **digital trade norms beyond North America.**

Volume: 4 Issue: 7 | july–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

- The **CPTPP,** involving countries such as Japan, Australia, and Singapore, contains extensive rules on:

✓ Paperless trade and digital authentication

✓ Free cross-border data transfers

✓ Non-imposition of data localization requirements

✓ Open internet access and net neutrality

- The **DEPA,** signed in 2020 by Singapore, New Zealand, and Chile, adopts a **modular structure** allowing new members to join gradually. It introduces **innovative provisions** on:

✓ **Digital identities** and interoperability of digital credentials

✓ **AI and algorithmic governance**

✓ **Fintech regulation and regulatory sandboxes**

✓ **Open government data** and data-driven innovation

DEPA represents a **prototype for a multilateral digital trade framework,** emphasizing trust, cooperation, and experimentation. It positions itself as "**living agreement",** adaptable to new technologies and evolving regulatory needs.

EU's Digital Trade Provisions in FTAs. The European Union (EU) adopts a **rights-based and regulatory-intensive approach** to digital trade. Its free trade agreements—such as the **EU-Japan Economic Partnership Agreement (EPA) and EU-Singapore FTA**-incorporate provisions on:

✓ **Cross-border data transfers,** contingent on ensuring an "adequate level of protection" under the GDPR.

✓ **Digital services liberalization** consistent with EU law.

✓ **Consumer protection,** including transparency obligations and complaint handling procedures.

✓ **Cybersecurity and digital standards** cooperation.

The EU's **GDPR framework** exerts an extraterritorial influence, often referred to as the **"Brussels Effect",** whereby third countries adjust their legal systems to achieve **adequacy status**-a prerequisite for seamless data flows to and from the EU.[4]

China's Digital Silk Road. As part of its **Belt and Road Initiative (BRI),** China has launched a **Digital Silk Road (DSR)** initiative to promote digital infrastructure development in partner countries. While not a formal trade agreement, the DSR involves multiple **bilateral MoUs and cooperation frameworks** with digital trade implications.

China's digital trade provisions emphasize:

✓ **Infrastructure development** (e.g., 5G networks, fiber-optic cables)

✓ **E-commerce promotion** through platforms like Alibaba and JD.com

✓ **Standard-setting** in areas such as e-payments, smart cities, and IoT

✓ **State-led regulatory models,** including data sovereignty and content controls

[4] Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.

Volume: 4 Issue: 7 | july–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

China's model presents an **alternative digital governance paradigm**-focused on state control, cybersecurity, and industrial policy. Its growing influence in Asia, Africa, and Latin America has ignited debates on **normative competition in digital trade regulation.**

Digital Trade and Data Flows. Data flows are the **lifeblood of digital trade,** enabling everything from real-time logistics and financial transactions to remote work and telemedicine. Yet, the regulation of cross-border data transfers remains **legally fragmented and politically sensitive.**

Most modern trade agreements now include provisions that:

- ✓ **Guarantee the free flow of data** across borders
- ✓ Prevent countries from imposing restrictions without legitimate public policy justifications
- ✓ Promote **interoperability of data protection regimes**

Such clauses are found in **USMCA, CPTPP, and DEPA,** reflecting a pro-liberalization stance. However, they usually allow **exceptions** based on national security, privacy, or public morals—creating interpretive flexibility and potential for conflict.

Disputes may arise regarding:

- ✓ Whether a data localization rule is genuinely protective or disguised protectionism
- ✓ Whether a cross-border data transfer mechanism satisfies foreign legal adequacy standards
- ✓ The balance between **economic efficiency** and **fundamental rights protection**

Data localization involves the requirement that personal or commercial data be stored or processed within a country's borders. Proponents argue it:

- ✓ Enhances **sovereignty and data security**
- ✓ Supports **domestic industry development**
- ✓ Facilitates **law enforcement access**

Examples include:

- ✓ **India's Draft Personal Data Protection Bill,** which mandates local storage of sensitive data
- ✓ **Russia's Federal Law No. 242-FZ,** requiring that personal data of Russian citizens be stored in Russian territory
- ✓ **Indonesia's Government Regulation No. 71,** mandating certain public service data to be stored locally

Critics assert that such measures **raise costs, reduce efficiency,** and create **barriers to entry** for foreign firms. WTO compatibility remains contested, particularly in light of **GATS Articles XIV and XIV bis,** which provide general exceptions for public policy and national security.

Cybersecurity, Trust, and Consumer Protection in Digital Trade. As digital trade becomes more integrated into the global economy, questions around **cybersecurity, consumer protection,** and **trust in digital infrastructure** have assumed increasing importance. Unlike traditional trade in goods, digital trade is vulnerable to cyberattacks, data breaches, algorithmic manipulation, and misinformation — all of which can have cross-border consequences.

Most modern digital trade agreements now include **provisions on cybersecurity cooperation,** particularly in the context of:

Volume: 4 Issue: 7 | july–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

- ✓ **Exchange of best practices** on cyber threat mitigation
- ✓ **Public-private partnerships** to build secure networks
- ✓ **Minimum standards for software integrity and encryption**
- ✓ **Notification obligations** in the event of cross-border cyber incidents

For instance, the **USMCA** (Art. 19.15) obligates parties to **maintain a legal framework that protects personal data,** including through consumer consent, transparency, and security safeguards. Similarly, **DEPA** encourages cooperation on cybersecurity frameworks and introduces **digital trust modules** that support mutual recognition of cybersecurity certifications.

Digital consumer protection is another emerging priority. The **asymmetric information environment** of digital platforms puts consumers at risk of fraud, exploitation, or manipulation. Effective consumer protection provisions in digital trade law should address:

- ✓ **Transparent and accessible information** on terms of sale and dispute resolution
- ✓ **Effective mechanisms** for consumer redress
- ✓ **Protection against deceptive and fraudulent commercial practices**
- ✓ **Cross-border cooperation between enforcement authorities**

Yet, implementation remains uneven. Many developing countries lack adequate legal infrastructure or technical capacity to enforce such provisions, leading to **regulatory asymmetries** that undermine trust in digital markets. Multilateral cooperation and capacity-building are therefore essential.

Challenges in Harmonization and Enforcement. Despite the growing number of digital trade provisions in bilateral and regional treaties, global governance in this area remains **fragmented, inconsistent, and underdeveloped.**

Key challenges include:

1. **Lack of a universal definition and scope** of digital trade across agreements, leading to overlaps and contradictions.
2. **Fragmentation of legal standards** on data flows, privacy, cybersecurity, and algorithmic governance.
3. **Enforcement asymmetries,** especially where dispute settlement mechanisms are weak or politically constrained.
4. **Conflicting values and interests,** such as:

- ✓ The US emphasis on market liberalization vs.
- ✓ The EU's rights-based data protection model vs.
- ✓ China's sovereignty-first digital governance framework.

5. **Exclusion of the Global South** from norm-setting processes, reinforcing digital divides and dependency on foreign infrastructure.

The **WTO Joint Statement Initiative (JSI)** on e-commerce - though a promising forum - remains unofficial and lacks binding authority. Its limited inclusiveness (over 80 countries) further hinders its legitimacy and effectiveness as a global standard-setting platform.

Enforcement mechanisms under regional treaties (e.g., USMCA, CPTPP) rely on **state-to-state dispute resolution,** which may not be well-suited to the **fast-paced, multi-stakeholder nature** of

Volume: 4 Issue: 7 | july–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

digital trade. Issues such as cross-border data breach liability, platform algorithmic transparency, or AI accountability cannot be effectively resolved through traditional trade dispute mechanisms alone.

Legal Gaps and Reform Proposals. To build a coherent and future-proof global legal framework for digital trade, the following **reform proposals** should be considered:

The WTO should prioritize the negotiation of a **Multilateral Agreement on Digital Trade,** underpinned by existing JSI discussions. Such an agreement could:

- ✓ Provide a **clear, technology-neutral definition** of digital trade.
- ✓ Establish minimum standards for **data flow liberalization** with human rights safeguards.
- ✓ Include **cross-border dispute resolution mechanisms** tailored to digital contexts.

Given the technical complexity of digital trade, current dispute settlement systems may lack expertise. A **Digital Trade Appellate Body** or panel of **technical arbitrators** could enhance dispute resolution under WTO or regional FTAs.

There is a need to recognize and regulate digital infrastructure — such as open-source software, digital ID systems, and cross-border payment platforms — as **global digital public goods.** International law must support:

- ✓ Open access to digital tools and platforms
- ✓ Technology transfer to developing economies
- ✓ Fair competition and interoperability

Trade agreements should incorporate **sunset clauses** and **impact assessments** to align digital trade rules with:

- ✓ **Climate goals** (e.g., energy-intensive data centers)
- ✓ **Ethical AI development**
- ✓ **Platform accountability for misinformation and hate speech**

Current digital trade negotiations are dominated by governments and large tech companies. Opening the space for **civil society organizations, data rights activists,** and **digital rights defenders** would improve **transparency and legitimacy.** Provisions for **open standing in digital trade-related disputes** would also ensure broader accountability.

Conclusion. Digital trade is redefining the structure, speed, and scope of global commerce. It creates unprecedented opportunities for economic growth, innovation, and cross-border integration, but also introduces complex legal, ethical, and governance challenges. The current contractual frameworks — spanning WTO instruments, UNCITRAL model laws, and regional trade agreements — offer a **fragmented and uneven patchwork of norms** that struggles to keep pace with digital realities.

A successful digital trade regime must:

- ✓ Promote **interoperability** between different legal systems
- ✓ Balance **economic liberalization** with **rights-based regulation**
- ✓ Strengthen **institutional capacity** for enforcement and dispute resolution
- ✓ Ensure that digital trade benefits are **inclusive and equitable**

Moving forward, **international cooperation must shift from competition to coordination,** recognizing digital trade as a multidimensional policy arena that intersects law, technology, security,

Volume: 4 Issue: 7 | july–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

human rights, and development. Without a unified approach, the promise of digital trade may become overshadowed by regulatory fragmentation, geopolitical friction, and societal backlash.

The reform agenda is urgent. By embracing inclusive rule-making, embedding digital ethics, and modernizing legal infrastructures, the international community can ensure that digital trade remains a force for good in the global legal order.

REFERENCES

1. Aaronson, S. A., & Leblond, P. (2018). Another digital divide: The rise of data realms and its implications for the WTO. *Journal of International Economic Law*, *21*(2), 245–272. https://doi.org/10.1093/jiel/jgy019
2. Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.
3. European Commission. (2018). *EU-Japan Economic Partnership Agreement: Texts of the agreement*. https://trade.ec.europa.eu/doclib/press/index.cfm?id=1684
4. OECD. (2019). *measuring the digital transformation: A roadmap for the future*. OECD Publishing. https://doi.org/10.1787/9789264311992-en
5. UNCITRAL. (1996). *Model Law on Electronic Commerce with Guide to Enactment*. United Nations. https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce
6. UNCITRAL. (2001). *Model Law on Electronic Signatures with Guide to Enactment*. United Nations. https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures
7. UNCITRAL. (2022). *Working Group IV: Digital economy — Cross-border data flows and harmonization issues*. United Nations. https://uncitral.un.org/en/working_groups/4/electronic_commerce
8. USMCA. (2020). *Agreement between the United States of America, the United Mexican States, and Canada*. Office of the United States Trade Representative. https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement
9. WTO. (1995). *General Agreement on Trade in Services (GATS)*. World Trade Organization. https://www.wto.org/english/tratop_e/serv_e/gatsqa_e.htm
10. WTO. (2015). *Ministerial Declaration on the Expansion of Trade in Information Technology Products*. World Trade Organization. https://www.wto.org/english/news_e/news15_e/mc10_23dec15_e.htm
11. WTO. (2021). *Work Programme on Electronic Commerce*. World Trade Organization. https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm
12. Zeng, J. (2021). China's Digital Silk Road: Regional and global implications. *Journal of Contemporary China, 30*(130), 1–17. https://doi.org/10.1080/10670564.2020.1824885