Key Threats to Digital Trade 2025

# Eurasia

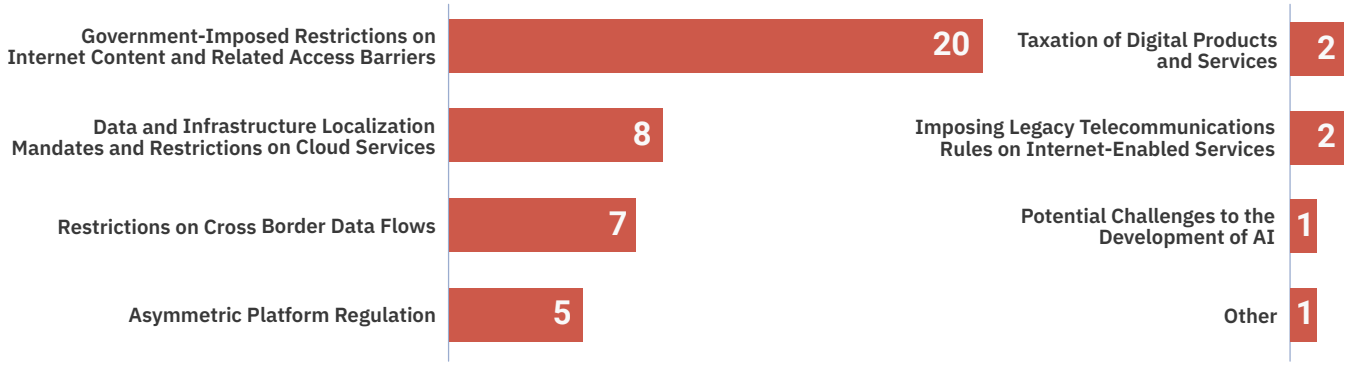
This accompanies CCIA's annual National Trade Estimate Report filing. Information and data is current as of October 30, 2025. For more, visit: digitaltradebarriers.ccianet.org.

The Eurasia region, comprising Türkiye, Kazakhstan, Uzbekistan, Ukraine, and Russia, represents a complex and vital frontier for U.S. digital trade. **U.S. digital services exports to leading markets in the region totaled at least US$2.4 billion** in 2024, demonstrating the market's continued economic importance, despite geopolitical instability. The U.S. has formalized its engagement through initiatives like the C5+1 diplomatic platform and Trade and Investment Framework Agreements (TIFAs) with Central Asian states.

The relationship between the US and Eurasian countries is at a critical juncture, as the region faces severe digital fragmentation driven by geopolitical tension and a rising wave of protectionist regulation. These policies are creating clear non-tariff barriers that favor domestic or non-U.S. competitors and actively undermine the principles of an open internet.

The following is excerpted from CCIA's annual comments submitted to the Office of the U.S. Trade Representative regarding its National Trade Estimate report—including broad takeaways from the region, followed by details of key trends.

## Key Threats to the U.S.-Eurasia trading relationship in 2025





CCIA identified

**46**

digital trade barriers in the Eurasia region

**38** policies enacted

**8** policies in development

# Digital Trade Barrier Trends for the Americas in 2025

## Asymmetric Platform Regulation

### Kazakhstan:

- Proposed amendments to competition laws would introduce EU-style **"gatekeeper" regulation for major digital platforms**. Modeled on the EU's Digital Markets Act, the proposal would impose ex ante obligations on large global firms deemed to have significant market power, with potential market access restrictions for non-compliance.

### Russia:

- The proposed **Bill No. 654254-8**, introduced in the State Duma, seeks to amend the **Law on Consumer Protection** to regulate app stores, mandating **sideloading** and requiring app store owners to allow interoperable access with other programs and payment systems. This measure, which raises security barriers and is explicitly aimed at U.S. companies as retaliation for sanctions, appears intended to facilitate the mandatory pre-installation of the government-controlled **RuStore**.

### Türkiye:

- The Turkish Competition Authority's draft amendment to **Law No. 4054 on the Protection of Competition** is modeled on the EU's Digital Markets Act (DMA), imposing extensive ex-ante obligations, such as **mandatory interoperability** and **prohibitions on self-preferencing** and **cross-service data utilization**, on designated "Undertakings Holding Significant Market Power."
- Separately, the **Regulation of E-Commerce Law** imposes discriminatory and trade-restrictive obligations on larger platforms, including a **prohibition on selling their own trademarked goods** and a ban on the largest providers from expanding into complementary industries like payments and logistics, while also providing tax relief favoring Turkish-headquartered companies.

### Uzbekistan:

- Uzbekistan published a regulation in May 2024, **Resolution N256**, that designates digital platforms with dominant or superior bargaining power and imposes extensive, EU DMA-style ex-ante obligations, including new categories like AI-based platforms. The regulation, which was developed with a concerning lack of transparency and industry consultation, creates a risk of undermining the growth of digital services and fair operation for companies.

## Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

### Kazakhstan:

- Strict data localization requirements stem from the **Law on Personal Data** and the **Protection and the Informatization Law**, mandating that personal and communications data be stored on servers located within the country. Complementary measures, including **Order No. 38/NK** and the **Communications Law**, extend these obligations to domain registrars and telecom operators, prohibiting most cross-border data transfers.

### Türkiye:

- Türkiye continues to advance laws pressuring data localization, led by a 2019 **Presidential Circular on Information and Communication Security Measures** that mandates hosting of "strategic" government workloads on servers in the UAE.

- Localization requirements are strictly enforced in the financial sector: the **Regulation on Information Systems of Banks** requires banks to keep primary and secondary information systems within the country and restricts cloud use to locally located services.
- **Law No. 6493** on payment systems establishes a licensing regime that acts as a substantial market barrier for foreign payment providers, mandating the establishment of a local company with high capital requirements and imposing a strict **data localization mandate** that requires all primary and backup information systems and records to be physically hosted within Türkiye's borders.

### Ukraine:

- While Ukraine's **Martial Law**, introduced in February 2022, temporarily lifted restrictions allowing government and key private sectors to utilize U.S. public cloud services, the **prior legal regime** remains a concern for potential reinstatement. The previous framework raised obstacles for cross-border cloud providers through a **preference for local cybersecurity standards**, **exclusive application of Ukrainian law** to govern cloud agreements, **limitations on foreign providers** serving public institutions, and the **potential for mandatory re-localization of data** after martial law expires.

## Government-Imposed Content Restrictions and Related Access Barriers

### Kazakhstan:

- The proposed **Digital Code** would expand on a 2023 law imposing **local legal presence requirements** on foreign social media platforms with over 100,000 daily users. Although presented as a framework to improve digital governance and address harmful content, the Digital Code has drawn criticism for its potential to enable political censorship, chill online expression, and restrict the free flow of information across borders.

### Russia:

- Russia's **Sovereign Internet Law** enables the country to establish a centralized, local internet infrastructure, while the **Federal Law on Amending Article 15-3** and **Federal Law on Amending the Code of Administrative Violations** establish penalties and a blocking framework for "knowingly spreading fake news."
- Laws like **Federal laws N482-FZ** and **N511-FZ** mandate content removal and prohibit the restriction of Russian state media content, with non-compliant U.S. firms facing massive, punitive fines, **throttling of service (e.g., WhatsApp, YouTube)**, and being compelled to initiate bankruptcy proceedings.
- New laws, including **Law No. 31-FZ** and **Law No. 32-FZ**, criminalize the publication of content determined to be falsehoods about the war in Ukraine, and **Law No. 42-Fz** bans advertising on platforms owned by entities designated as "foreign agents," effectively creating a de facto ban on digital foreign advertising.
- The government has also accelerated its campaign to **block VPNs** and requires the **pre-installation of Russian software** on consumer electronic products, further centralizing control over online access and content.

### Türkiye:

- **Law No. 7253** mandates that social network providers with over one million daily users establish a **domestic representative office**, respond rapidly to takedown requests, and **store Turkish user data domestically**.
- **Law No. 7418 (Amendment of Press Law, and Certain Laws)** further restricts freedom of expression by requiring platforms to **disclose algorithms and users' personal data** to the government upon demand, and establishes new criminal liability for spreading "disinformation."

- A decision by the ICTA, effective April 1, 2023, introduced significant new obligations, holding social network providers legally responsible for user-generated content, mandating the appointment of a **local representative**, requiring the creation of an **advertising library**, and imposing detailed compliance requirements and sanctions for failure to remove unlawful content.

## Imposing Legacy Telecommunications Rules on Internet-Enabled Services

- **Türkiye:**
  - Türkiye's **Law No. 7418** and a March 2025 consultation from the Information Technologies and Communications Authority (ICTA) propose sweeping regulations that would effectively subject cross-border OTT communications providers (above one million monthly users) to the regime of legacy telecommunications firms.
  - These proposed rules impose onerous obligations, including mandatory **local incorporation** (Turkish subsidiary), registration under the **Electronic Communications Law**, and compulsory **contributions to the universal service fund** which subsidizes traditional telecom services.
  - Failure to comply with these rules—which also include extensive data disclosure requirements and exposure to vague "public order and national security" obligations—could result in severe penalties, including fines up to ₺30 million (US$1.6 million) or **service throttling/blocking**.

## Potential Challenges to the Development of AI

- **Kazakhstan:**
  - The draft **Law on Artificial Intelligence** introduces a risk-based regulatory framework requiring AI systems to be classified by risk and autonomy, with high-risk systems subject to audits, documentation, and state supervision. These measures create heavy compliance costs, legal uncertainty, and delays for companies seeking to introduce or update AI products. The government's broad discretion to define "high-risk" systems and mandate local oversight further increases regulatory unpredictability, discouraging investment and limiting cross-border AI innovation and deployment.

## Restrictions on Cross-Border Data Flows

- **Russia:**
  - **Russia Law N236-FZ** (the "landing law") mandates that certain foreign companies, primarily U.S. technology platforms with over 500,000 daily users, **establish a direct local legal presence** in Russia, which subjects them to Russian jurisdiction and makes it easier for the government to demand content removal and threaten local representatives.
  - Local presence non-compliance carries severe penalties, including potential **full or partial blocking/throttling** and a ban on Russian advertisers and payments, with subsequent legislation imposing even heavier fines, potentially **up to 20% of prior year's revenue**.
  - Russia has intensified its data localization efforts, levying fines against U.S. firms like Google for failing to **store the personal data of Russians within the country**.
  - Furthermore, amendments to the **Federal Law on Personal Data** establish transfer impact assessments and give Russia the power to **suppress outgoing data flows in an extra-judicial procedure**, while **Bill No. 502113-8** proposes expanding criminal penalties for illegal cross-border data transfers, including up to eight years in prison.

- **Türkiye:**
  - Cross-border data transfers are governed by the **Law on the Protection of Personal Data (Law No. 6698)**, which permits transfer only under three conditions: (1) to countries with an adequate level of protection, (2) with the data subject's explicit consent, or (3) with ad-hoc approval from the **Data Protection Board** through an undertaking agreement. As of 2023, the **Data Protection Board** has **not yet announced a list of adequate countries** nor granted the necessary ad-hoc approvals, leaving the framework incomplete and creating significant barriers to data transfer.

- **Uzbekistan:**
  - Uzbekistan's **Law No. ZRU-666** established strict data localization requirements, mandating that foreign and local entities process the personal data of Uzbek citizens using technical means physically located within Uzbekistan, with servers also requiring registration in the **State Register of Personal Databases**. Non-compliance can lead to the state regulator, Uzkomnazorat, restricting access to the online resource and imposing fines or criminal liability, creating a major barrier for U.S. businesses, particularly those offering AI and cloud services.

## Taxation of Digital Products and Services

- **Türkiye:**
  - Türkiye enacted a **7.5% DST**, which is imposed on gross revenues for various services including digital advertising, content sales/streaming, and platform interaction services, with a global revenue threshold of €750 million and a local threshold of €20 million.
  - The government also amended **Law No. 6563** to impose potentially burdensome and uncertain **withholding tax requirements** for non-resident companies that operate e-commerce platforms, effective January 1, 2025.