Monitoring international legal regulation trends for developing legislation in the digital economy in Russia

- How Russia legalizes crypto market
- Approaches to data regulation in the US and the EU: should it be stricter or weaker?

Monitoring No.4 (28) (April 2026)

Monitoring has been prepared by a team of employees of the International Best Practices Analysis Department at the Gaidar Institute.
Associated authors: Maria Girich, Researcher; Ivan Ermokhin, Researcher; Antonina Levashenko, Senior Researcher; Olga Magomedova, Researcher; Kirill Chernovol, Researcher; Diana Golovanova, Researcher

Cryptocurrency market with a limited access

Authors: Ivan Ermokhin, Diana Golovanova

In April 2026, the State Duma passed the first reading of the bill "On Digital Currency and Digital Rights," which includes new rules for regulating cryptocurrencies in Russia. The key provision of the bill is the legalization of digital currency trading, which is proposed to be implemented through the existing financial market infrastructure.

The bill does not provide for setting of specialized crypto exchanges: trading in digital currencies will be permitted only to existing market participants licensed by an exchange or trading system (there are **8** of them in Russia). Access to trading will be provided through brokers.

One of the key provisions of the bill is the requirement for Russian residents to store cryptocurrency with Russian digital depositories[1], however, withdrawal of digital currencies to foreign custodial wallets[2] will be possible only if one of the 7 set grounds is available (for example, in the context of execution of a foreign trade contract), while withdrawal to one's own "cold" wallets is not permitted.

The bill also defines which digital currencies will be allowed on the Russian market: to be admitted to trading in Russia, a digital currency must meet quantitative criteria, and its average daily trading volume must exceed Rb 1 trillion (in practice, this means allowing Bitcoin, Ethereum, and possibly the stablecoins USDT and USDC), while access to thousands of other cryptocurrencies will be closed to unqualified investors.

16 500

tokens are tracked on the global crypto market

In addition, individuals (both qualified and non-qualified investors) will be required to undergo annual testing to be eligible to purchase cryptocurrency, while for non-qualified investors, an additional annual purchase limit has been approved (the limits have not yet been determined, but amounts from Rb 300.000 to Rb 600.000 on one platform are being considered).

The bill also permits foreign trade transactions with settlements in digital currency between residents and non-residents, but using cryptocurrency as a means of payment within the country remains prohibited.

Rb 50 bn per day

the volume of cryptocurrency transactions in Russia (data from the Ministry of Finance)

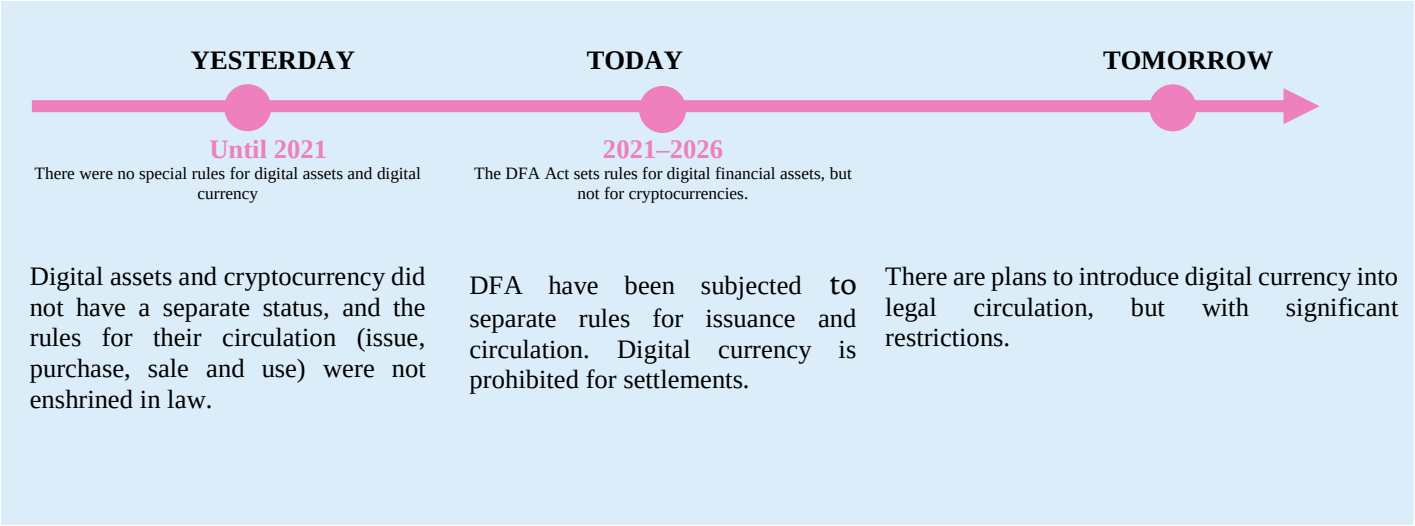
The bill introduces the following regulations for crypto exchangers: if the volume of transactions for the purchase, sale, and exchange of digital currency over-the-counter (OTC) trading exceeds Rb 3.5 mn per month, only organizations included in the register of the Central Bank of the Russian Federation will be able to conduct such transactions (transactions involving smaller amounts are not subject to this mode).

However, the bill does not resolve all issues arising in the context of FATF standards. It addresses a key issue, i.e., lack of specific regulation of market participants involved in cryptocurrency circulation, however, it does so primarily through the existing financial infrastructure. As a result, a number of issues that the FATF classifies as sensitive (transactions with non-custodial wallets, circulation of certain types of crypto-assets, and international cooperation) will likely require further study. At the same time, the following bills on liability were introduced:

- criminal liability is proposed for mining digital currency not included in the miner registry (a fine of up to Rb 2.5 mn or imprisonment for up to 5 years);
- administrative fines (up to Rb 1 mn) are proposed for crypto exchangers for violating rules of digital currency circulation, including transactions with unqualified investors exceeding limits;

1 Organization included in the CB register, which which keeps records of digital currency in digital accounts..

2 Wallets that are stored and maintained by a third-party service



– criminal liability is proposed for the illegal organization of digital currency circulation (purchase, sale, exchange) (a fine of up to Rb 1 mn or imprisonment for up to 7 years).

There are also plans to obligate people to notify tax bodies about opening and closing of foreign crypto wallets, report on the accounts' operations. The notification must be submitted no later than 1 month from the date of opening or closing of such a wallet.

However, the Central Bank has already mitigated rules for non-qualified investors with regard to DFA: now they will be able to purchase simple digital financial assets without restrictions, whereby payments are clear in advance and do not depend on variable indicators, if the issuer has a high credit rating (A+ on the national scale or BB on the international scale). More complex digital financial assets, where the income depends, for example, on the key rate or stock prices, will be available to non-qualified investors only within a limit of Rb 600.000.

- Amid legalization of the crypto market in Russia, the EU has tightened its sanctions approach as follows: as part of the 20th sanctions package, a ban has been introduced on any transactions with Russian platforms that allow transferring and exchanging crypto assets.

Moreover, operations with RUBx (a ruble stablecoin) are prohibited, as well as support for developing a digital ruble.

More regulations, less protection

Tight regulation vs. digital growth: The US and EU fight over data governance model

Authors: Olga Soldatkina, Maria Girich

Regulatory burden often hinders the development of technologies. For example, studies show that a less civilized US approach to data regulation marked by more favorable conditions for digital platforms compared to a stricter European regulation model (EU General Data Protection Regulation (GDPR), Digital Market Act (DMA) in terms of competition) resulted in a more intensive development of companies: in terms of capitalization, 7 major technological companies in Europe are 20 times behind 7 US tech giants.

However, now in the US as well, where 75% of the largest companies belong to the technological sector, the introduction of a unified federal law on personal data is being discussed and the SECURE Data Act draft was introduced in April 2026. So far, sectoral laws regulate data (such as Health Insurance Portability and Accountability Act) or local regulations in 23 states.

The draft law has received mixed reviews from American lawyers. On the one hand, it establishes a unified federal set of rights and protection tools for personal data subjects, including the right to access collected data, correct and delete data, receive data in a format suitable for transfer to other operators, refusal to use data for advertising, sale to third parties, for creation of a digital profile of the data subject, and so on.

As in European law, it is proposed to distinguish between the "controller" (who collects data and gives consent to its processing) and the "processor" of data (who stores and processes the data). Data brokers (intermediaries in the sale of data) are required to register with the Federal Trade Commission.[1]

Adopting such a federal law would allow the US to reduce the pressure of European regulators on American tech giants operating in the EU: 8 of 10 largest fines in the GDPR history have been issued particularly to the US companies, and the amount of these fines reaches 63% of all fines issued to GDPR breachers.

On the other hand, the law could weaken the level of data protection in those states that already have stricter regulations. As federal law takes precedence over state laws, companies will primarily focus on federal requirements.

For example, the state of California (where personal data protection laws are most developed) has announced that it will lower the bar for data protection: thus, users have the right to prohibit sale of their data once for all websites in their browser settings. However, the federal bill only enshrines the general right to opt out of data sales without establishing a mechanism for its implementation.

Ultimately, the intention to improve data protection in the US as a whole undermines the best practices of the states. Federal law should establish a "floor", not a ceiling" on regulation, so that states can retain more detailed data protection rules.

Meanwhile, in April, the EU published a report on the Digital Market Act for the first 2 years of its implementation with regard to 7 major technological companies and their 23 services. It is worth noting that 5 companies are American (Alphabet, Amazon, Apple, Meta[2] and Microsoft), whereas Booking is the only company repesenting the EU.

1 Section 5 Data Brokers, Part (c).

1 It is recognized as an extremist organization and is banned in the Russian Federation.

Based on the report data, over **40** companies, mainly SME, due to demands towards major platforms on provision of data portability, have received access to platform data in order to launch their own innovation services. Likewise, users now have the ability to prohibit merging of their data across various company services and transfer their data between platforms and ecosystems (for example, between iPhone and Android devices), which has reduced the practice of unwanted profiling and eliminated binding of users to only one ecosystem.

What is next?

In Russia, unlike the EU and the US, the state protects data not by expanding data management rights, but by introducing additional instruments of state control over data circulation. In 2025, both turnover-based fines for repeated data leaks and an automated violation monitoring system were introduced, which identified violations of the personal data protection law in **84%** of conducted inspections, with the number of Roskomnadzor inspections increasing by **40%** year-on-year.

It should be noted that a number of companies' inspections has declined in Russia since 2019 by **5.6** times, from **1.52** mn to **275.000**. However, digital sector increased by 1.8 times from **1.32%** in 2019 to **2.43%** in 2024. Thus, digital sector grows faster where the state reduces excessive administrative burden and makes regulation more predictable.

YESTERDAY

1973–2025

Countries introduce personal data laws:

- 2018. – EU General Data Protection Regulation;
- 2022 – EU Digital Markets Act

Consistent establishment and expansion of consent-based rights of personal data subjects across jurisdictions

TODAY

2026

- More than 144 countries have introduced data regulation norms.
- The first federal bill on personal data protection has been proposed in the United States

There are so many regulations that it is difficult for everyone to comply with them: new regulations may lead to a decrease in data protection

TOMORROW

Targeted regulation of platforms, AI, clouds, data brokers, advertising ecosystems, etc. The main goal is not only to protect data but also to limit data monopolies.

News in **April 2026**, which we found interesting.[1]

- China introduced rules for anthropomorphic AI services: duty to notify when a person is communicating with an AI, to limit creation of "virtual relatives" and "partners" by minors, and to remind users to take breaks during prolonged, uninterrupted communication (more than 2 hours). These measures are aimed at preventing emotional dependence on AI.

- In Florida (USA), prosecutors are investigating OpenAI following the shooter attack at Florida State University. According to the investigation, the criminal used AI to receive information about campus occupancy, weapons and ammunition, though he did not directly discuss the plan of attack. Authorities are examining whether the AI developer could be held criminally liable as a possible accomplice to a crime.
- Maine (USA) put a moratorium (until November 2027) on construction of new data centers with a capacity of over 20 megawatts to assess the impact on energy costs, the grid, and the environment (including the importance of renewable energy development). Similar restrictions on data center construction have been previously introduced in jurisdictions (in Singapore, the Netherlands, and elsewhere).

[1] Since 2025, the Gaidar Institute has been developing a digital platform for analyzing news in Russia and globally on the topic of digital economy regulation – DIgiReg. The news presented has been selected by experts, in part based on an analysis of the platform's data.

DIGEST