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

- **How antitrust authorities regulate data in the context of competition**
- **How quantum technologies become the new infrastructure**
- **Trust level for cloud systems that run public sector AI systems**

Monitoring No. 6 (30) (June 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 Soldatkina, Researcher; Kirill Chernovol, Researcher; Diana Golovanova, Researcher

Whoever controls the data controls the market

How antitrust authorities regulate data in the context of competition?

Author: Maria Girich

In June 2026, a draft bill on innovation and online choice, aimed at regulating competition in digital markets, was introduced in the U.S. for consideration. The bill covers "systemically important" platforms with annual revenue exceeding $**175** bn and an audience comprising more than **34%** of the U.S. population aged 12 and older, or **34%** of households (similar to "gatekeepers" in the EU).

The following restrictions apply to the data use:

- One may not use sellers' non-public data to promote one'' own products; for example, one may not identify sellers' best selling products and release your own similar products.

- One may not restrict business users' access to their data on the platform or prevent them from transferring and using that data on other platforms.

Mergers are one way to turn data into a source of monopoly power. In June 2026, the EU discussed a draft Merger Guidelines proposal that suggested taking into account not only companies' ability to set prices but also the impact of mergers on access to data, since in digital markets users often "pay" for free services with their data.

The company formed after the merger may abuse its position by denying competitors access to critical data or by worsening the terms of access to data. As a result, companies that relied on this data and cannot obtain it from alternative sources suffer as a result of the merger creating a data monopoly.

In Russia, an example of this behavior is the case in 2025 when Wildberries restricted access to data on products, prices, and advertising rates from third-party analytics services. This is not an example of a merger, but it illustrates how a large platform's control over data can restrict competition and the growth of companies in related markets: after Wildberries restricted access to its data, disruptions in analytics began.

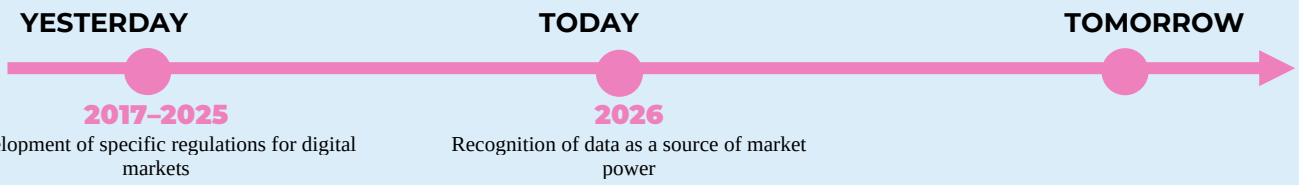
At the same time, the competitive advantages derived from access to data should be assessed not only in terms of quantity, but also by considering qualitative characteristics—such as volume, diversity, update frequency, value, and other parameters.

To reduce the monopoly of large digital platforms over data, regulators are introducing requirements to ensure data portability and are compelling them to share data with competitors.

In June 2026, the UK Competition and Markets Authority ordered Google to allow users to transfer their search data to other companies via a special API

What is next?

In Russia, there are currently no specific rules for assessing data as a factor in market power; however, the Federal Antimonopoly Service (FAS) already takes data into account as a factor in competitive advantage when evaluating mergers and abuses of a dominant position.



2017–2025
Development of specific regulations for digital markets

2026
Recognition of data as a source of market power

Rules are being introduced for dominant platforms: a ban on promoting their own services to the detriment of competitors, discriminating against business partners, and preventing users from switching to competing services

Countries are beginning to view data as a competitive factor

The introduction of measures to limit platforms' control over data, including competitors' access to data, interoperability, and data portability, as well as oversight of the consolidation of data sets during mergers

Quantum transition

How quantum technologies become the new infrastructure?

Author: Diana Golovanova

In June 2026, the U.S. passed executive order on the development of quantum innovations. The plan is to build at least one quantum computer[1] to solve scientific problems that cannot be solved on conventional computers, as well as to develop quantum sensors and networks.

$1,9 BN

accounts for the global market for quantum technologies

According to OECD, by the end of 2025, **18** OECD and EU countries were already developing quantum technologies, and since 2013, governments around the world have allocated approximately **$55.7 bn** dollars to their development.

The development of quantum technologies creates new cybersecurity risks. It will become possible to crack the cryptographic algorithms and ciphers used to protect communications, payments, and data. We discussed these risks in Monitoring No. 10 (22).

Quantum sensors are of particular interest, as they allow for highly accurate measurements of physical parameters (such as time and pressure) and are therefore used in applications where the outcome depends on measurement accuracy—for example, in mining, navigation, and space exploration.

However, working with such sensors involves a number of risks related to data trust: Is the sensor itself functioning correctly? Have its readings been distorted? Was the equipment manufactured securely? Are there any vulnerabilities in the software running the device?

That is why, in June 2026, Australia published Guidelines for companies working with quantum sensors. Four risks are highlighted:

Risk 1: The sensor's operation can be affected by the external environment. Sensors are highly sensitive and can pick up not only the desired signal but also interference, which reduces data accuracy. Therefore, it is important to choose the correct location for installing the sensor.

Risk 2: Data tampering. An attacker could mimic a genuine signal or inject extraneous noise to cause the sensor to transmit incorrect data. Therefore, it is necessary to verify the authenticity of the data, for example, through secure signal verification[2] and an anomaly detection system.

Risk 3: Supplier and material security. Quantum sensors require specialized materials, components, equipment, and firmware (software). Consequently, during the manufacturing or supply chain stages, there is a risk that counterfeit components or malicious software could be introduced into the device, which could compromise its operation in the future. Companies are advised to verify the origin and authenticity of equipment and components.

Risk 4: Software and firmware security. Software vulnerabilities can disrupt the sensor's operation and distort the data it transmits. Therefore, it is necessary to regularly check the software through which the sensor operates, update it in a timely manner, and fix any detected bugs.

[1] A computer that uses the properties of small particles (i.e., how atoms and other small particles behave) to perform calculations and can solve complex problems faster than a conventional computer.

[2] For example, using a digital signature that confirms that the signal was sent by the sensor itself and that the data has not been tampered with.

Quantum sensors are widely used in Russia; for example, in geological exploration, the company Geoscan uses quantum magnetometers to search for minerals; in medicine, QLU is developing sensors to measure the brain's weak magnetic fields; and in navigation, Sensor Spin Technologies is developing a quantum gyroscope that can determine where an object is moving and at what speed without satellites.

What is next?

Regulations governing quantum technologies, including quantum sensors, are still being developed in Russia. However, the state program for the development of quantum technologies calls for the development of four such devices and the deployment of two by 2030. Technical standards (GOSTs) are also being prepared for quantum communications and the quantum Internet of Things.

Therefore, it is important to develop regulations, particularly technical ones, that would specify how accurately quantum sensors must operate, how to verify their proper functioning, under what conditions they may be used, and how to confirm the accuracy of the data they provide.

Quantum computers and systems have been developed to solve problems that are too complex for conventional computers (for example, to study the structure of molecules and chemical reactions and to develop new drugs)

Countries are assessing the risks associated with the use of quantum sensors (the likelihood of collecting incorrect data due to the sensors' hypersensitivity to interference; the risk of vulnerabilities, hacking, and data leaks resulting from the use of counterfeit components or software)

Introduction of general safety regulations for quantum technologies: transition to encryption methods resistant to quantum computers; establishment of requirements for data accuracy and the protection of quantum sensors

Cloudy, with a chance of AI

The EU is developing "trust levels" for cloud services used by public-sector AI systems

Author: Kirill Chernovol

In June 2026, the EU began tightening the requirements for engaging foreign cloud service providers to operate government AI systems.

For example, a court might use AI developed in the EU but running on a foreign provider's cloud infrastructure. As a result, court data could be stored abroad or accessible to the foreign provider, creating risks of data leaks, loss of access to the service, and so on.

Consequently, the EU has presented a draft Cloud and AI Development Act (CADA). More than **70%** of the EU cloud market is controlled by just **3** companies, all of which are foreign—Amazon, Microsoft, and Alphabet. Government AI infrastructure is becoming dependent on foreign cloud services.

20%

of companies in various countries have experienced data breaches when using AI systems over which they have no control

To assess whether foreign providers should be allowed to participate in procurement, CADA introduces **4 "trust levels"**: the higher a provider's level, the more significant the functions for which it provides cloud services are to the state and society:

Level 1—for non-critical functions (AI does not use sensitive data, and a service outage does not pose a threat to society). Example: AI systems for document management. The provider and cloud infrastructure must be located in the EU.

Level 2—for functions posing a risk to public order (if sensitive data is involved or the service is critical to the operations of a government agency). Example: medical data management services in public hospitals. The provider's staff, facilities, and equipment must be located in the EU. A foreign parent company must not be able to order its EU-based "subsidiary" to shut down the service.

Level 3 – for more critical functions (law enforcement, judicial activities, where data constitutes a state secret). Staff must be EU citizens. Companies controlled by foreign entities cannot be assigned Level 3 or higher.

Level 4—for the most critical functions (defense, national security, etc.). The provider must not be controlled by foreign entities, and all service support and data access must be provided exclusively within the EU.

Despite the stricter requirements, Amazon, Microsoft, Alphabet, and other foreign cloud providers can participate in Level 1–2 procurements through their European subsidiaries—Amazon Web Services and Google Cloud both have them.

In Russia, in June 2026, a draft federal law on supporting the development of AI was submitted to the State Duma (and adopted in July), in which the approach differs from that of the EU: data from state AI systems must be stored in data analysis centers owned by Russian legal entities. However, the Russian bill does not classify government systems by criticality, which would require different "trust levels" as in the EU.

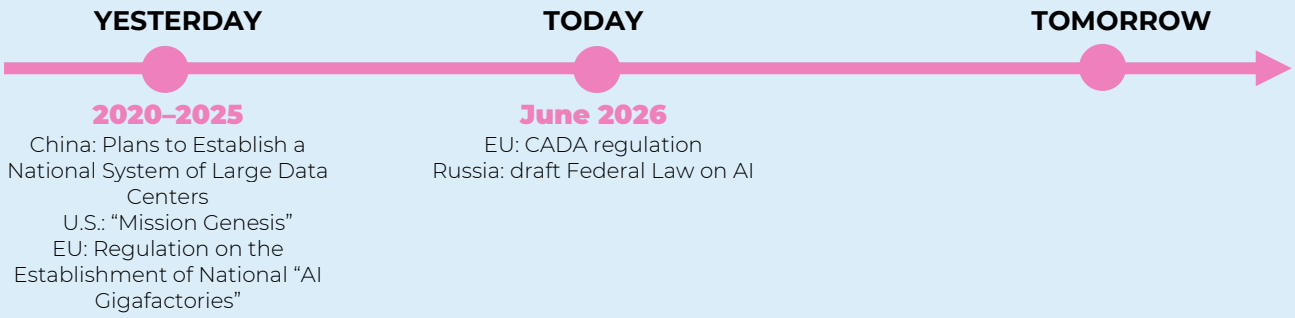
The definitions of control also differ. In Russia, foreigners are not permitted to own more than 50% of a company. In the EU, control is defined as the ability to exert a "decisive influence" on a company's operations, including through key contracts or foreign top managers. This approach is broader than in Russia.

What is next?

There are approximately **59** cloud data center clusters operating in the EU,[3] with **83%** of them belonging to providers based outside the EU.

By 2030, the EU plans to triple its data center capacity and fully meet its AI cloud computing needs by 2035.

In Russia, plans for the development of data centers have not yet been adopted, but there are plans to bar companies with foreign ownership from providing infrastructure services for government AI initiatives.



Countries develop standards and plans to ensure self-sufficiency in computing power for AI

Countries restrict access by foreign cloud computing providers for AI systems in the public sector and for critical infrastructure

Protecting digital sovereignty by restricting the use of foreign cloud services for government AI systems: requirements for localization and the placement of equipment within the country, etc.

.

[3] AWS – 6, Microsoft Azure – 12, Google Cloud – 11, Oracle – 9, Exoscale - 6, IBM Cloud – 2, Alibaba Cloud – 2, Tencent Cloud – 1, OVHcloud – 7, Hetzner – 3.

DIGEST

News **in June 2026** that we found interesting[1].

- In the UK, the Competition and Markets Authority is forcing Apple to share the NFC technology[1] in the iPhone. Previously, Apple had restricted access to NFC exclusively to its own services. Consumers were forced to use only Apple Pay and Apple Wallet on the iPhone for contactless payments. It is expected that once NFC access is granted, services supporting payments with digital currencies and stablecoins will emerge.

- In Russia, website owners will be fined Rb500,000–700,000 if they allow users to register or access the site in any way other than as permitted by law—for example, a fine will be imposed for registration via Gmail.

- South Korea's antitrust authority has published a report on the impact of algorithmic self-preferencing by platforms on consumer choice. The report found that if a platform artificially boosts its own product in search results, the likelihood of that product being purchased increases by **34%**, while the likelihood of a competitor's product being purchased decreases by **32%.**

[1] Since 2025, the Gaidar Institute has been developing DIgiReg, a digital platform for analyzing news in Russia and around the world on digital economy regulation. The news items featured are selected by experts based, in part, on analysis of the platform's data.

[1] Near Field Communication (NFC) is a set of short-range wireless communication protocols widely used in mobile devices, such as when making payments with a phone at a payment terminal