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

- AI in key spheres
- Children's online safety
- Anticompetitive practices online
- Access to banking data
- Digitalization of public health
- Facilitating use of persona data

Monitoring No. 11 (23) (November 2025)

Monitoring was prepared by a team of experts of the Gaidar Institute for Economic Policy (the Gaidar Institute):
Antonina Levashenko, Senior Researcher, International Best Practices Analysis Department, Gaidar Institute.
Maria Girich, Researcher, International Best Practices Analysis Department, Gaidar Institute.
Ivan Ermokhin, Researcher, International Best Practices Analysis Department, Gaidar Institute.
Olga Magomedova, Researcher, International Best Practices Analysis Department, Gaidar Institute.
Kirill Chernovol, Researcher, International Best Practices Analysis Department, Gaidar Institute
Diana Golovanova, Researcher, Economic Policy Foundation

"Will you forgive me these November days?
Lights tremble in the Neva's canals.
Tragic autumn's sparse adornments."
Anna Akhmatova

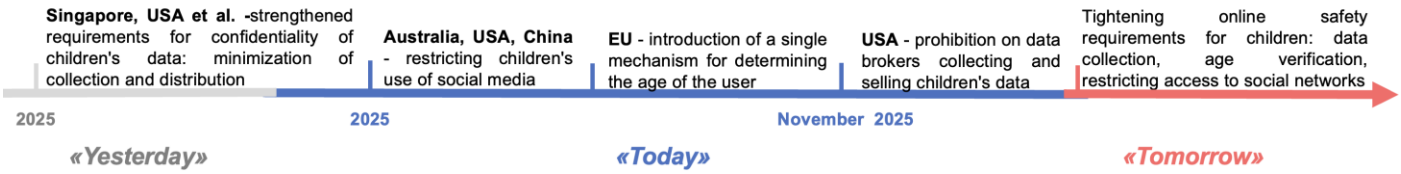
In November 2025, we can identify 6 events that define trends in the development of digital economy regulation globally.

Trend No. 1. AI in key spheres

In November 2025, the US plans to launch a government AI platform for science, energy, and defense, with companies having access to data and computing power.

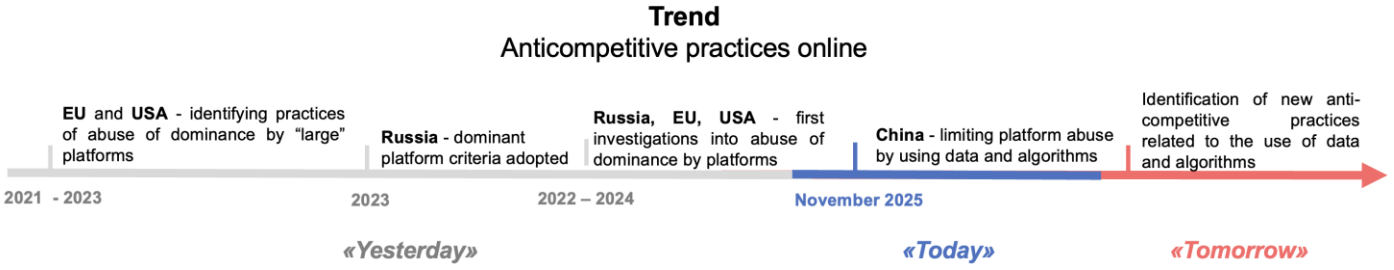
Trend No. 2. Children's safety online

In November 2025, the EU adopted a resolution to strengthen children's safety online, including monitoring child influencers. In the US, a proposal has been made to ban data brokers from collecting, storing, and selling the personal data of minors.



Trend No. 3. Anticompetitive practices online

In November 2025, China published Guidelines on Antitrust Practices of Platforms, such as collusion through the exchange of sensitive data, abuse of dominance through the use of algorithms, etc.



Trend No. 4. Access to banking data

In November 2025, the EU agreed on a new Payment Services Directive establishing rules for licensed open banking providers' access to user account data.

Trend
Access to banking data

Trend No. 5. Digitalization of health care

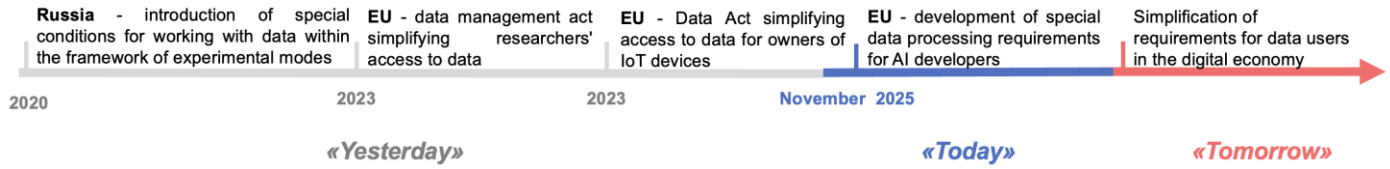
In November 2025, the OECD presented a report on best practices in countries regarding the digitization of public health. In the US, for example, it was proposed that digital service providers be required to protect health data, an obligation that previously applied only to hospitals and insurers.

Trend
Digitalization of public health

Trend No. 6. Facilitating use of personal data

In November 2025, the EU presented a package of amendments aimed at simplifying data handling requirements.

Trend
Facilitating use of personal data



Also in Russia, in November 2025, Roskomnadzor began a phased **blocking of WhatsApp**[1] due to the service's refusal to provide information at the request of Russian regulators, including information about data leaks and the use of the messenger for fraud and other criminal activities[2] – a formal violation of Article 10.1 of the Information Law, which requires messengers to cooperate with state authorities.

[1] Owned by Meta. Meta's activities are recognized as extremist and are prohibited in the Russian Federation.
[2] From the official statement of Roskomnadzor to TASS. https://tass.ru/ekonomika/25764077

Key aspects

1. AI in key spheres

The US experience

From November 2025, the Genesis Mission[3] was launched in the US to create an "American Science and Security Platform" for scientific data for the purpose of training fundamental models and "AI agents" that test hypotheses and automate research in priority areas: energy, scientific research and development, and defense. The platform was developed as part of the "American AI Plan"[4] (see review in Monitoring No. 7 (19) (July 2025)).

The platform should provide computing power, modeling and analysis tools, secure access to data, etc. There are plans to develop AI in the fields of advanced manufacturing,[5] biotechnology, critical materials, nuclear energy, quantum computing, semiconductors, and microelectronics.

It is planned to develop model agreements on data and models, rules for licensing and commercializing intellectual property created using the platform, as well as uniform procedures for accessing data, models, and calculations, and cybersecurity standards for non-governmental participants.

Currently, 53 companies are planning to participate in the Genesis Mission in the fields of cloud technologies and general-purpose AI platforms (5 companies), hardware and data center infrastructure for AI (10), semiconductors, lithography, and critical materials for AI infrastructure (12), energy, including nuclear energy (6), quantum computing (2), and others. The Genesis initiative involves businesses in the development of AI solutions, including through budgetary funds. There are plans to involve startups.

The experience of China

In August 2025, opinions were published on deepening the implementation of the Artificial Intelligence+ initiative on the formation of programs, standards, and legal regulation of AI. The document contains the following directions:

- For science and technology – the development of scientific models and the creation of open and shared high-quality scientific data sets.

- Introducing AI into business strategies and processes and applying AI in design, production, and maintenance.

- Improving the system of data rights and copyrights as they apply to AI, opening access to data created within the framework of government-funded projects, and in parallel, developing national computing infrastructure (AI chips, supercomputing clusters, etc.).

- Establishing rules for monitoring AI systems, preventing risks, and responding to incidents, taking into account the level of risk. Here, China's approach to AI regulation is similar to that of the EU.

Unlike the US, China's approach is not built around a single specific state platform with a strict partner admission regime.[6] Instead, China is implementing AI "in all sectors" of the economy and government, while simultaneously planning to "fine-tune" the framework rules: data rights and copyrights, standards, security assessment and registration systems, as well as monitoring and responding to AI risks.

Russia's experience

In November 2025, Russia's Ministry of Digital Development, Communications and Mass Media discussed launching a pilot project on labeling AI-generated content, which would make it possible to distinguish between content created by humans and machines, as well as mechanisms for verifying the identity of users who post materials. It was proposed to analyze the current regulation of AI, assess the extent to which existing norms protect the rights of citizens when using AI in healthcare, education, and social support, and where gaps remain—to reconsider the basic norms of the law on AI.

In the future, laws on AI will be developed in Russia and around the world, defining the principles for using the technology and distributing responsibility for the correct operation of AI systems in critical areas (social services, healthcare, etc.) between the state, developers, and digital service providers. On average, in developed countries, about 15% of

[3] https://www.whitehouse.gov/presidential-actions/2025/11/launching-the-genesis-mission/

[4] https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf

[5] Manufacturing using AI, the Internet of Things, 3D printing, etc.

[6] Standard agreements on data and models, uniform access procedures, cybersecurity requirements, user verification and authorization.

all AI projects will be funded by governments in the coming years. Today, this share ranges from 3% (US[7]) to about 50% (China[8]).

2. Children's online safety

The EU experience

In November 2025, the EU adopted a resolution[9] to strengthen the protection of children on the Internet due to their sensitivity to destructive content created by AI, gaming addiction, mental disorders caused by social pressure on the Internet, etc. Back in October 2025, the European Commission launched an investigation[10] into violations by Snapchat, YouTube, the App Store, and Google Play regarding the protection[11] of minors in terms of age verification mechanisms, setting stricter default privacy settings for accounts, ensuring that the service design does not cause addiction, etc.

The EU plans to develop:

1) A uniform method for verifying the age of users within the EU. The method should ensure minimal collection of children's data, for example, obtaining only an affirmative or negative answer to the question of whether the user is 16 years of age[12] in order to use the platform, without collecting data for personal identification.

2) Requirements for device manufacturers and AI application developers to implement data collection control mechanisms to ensure that AI applications do not collect children's data without the consent of a parent or guardian.

3) A ban on platforms financially supporting "child influencers" (e.g., paying for advertising), and the creation of a way to distinguish between content and advertising in applications for children.

4) Requiring platforms to prohibit games that include "lottery" mechanisms (such as "wheels of fortune," "pay to advance in the game" mechanisms, exchanging game currency for real money, etc.).

5) Requiring platforms and apps to create parental control tools during the development stage (e.g., parents receiving reports on their children's activities on the platform).

The US experience

In November 2025, a bill[13] was introduced to prohibit data brokers[14] from collecting, using, storing, and distributing (selling, disclosing) data belonging to minors.[15] The only exception is the collection of data by a broker to determine a person's age. Any data about a person must be deleted after their age has been established, and a mechanism must be created for requesting the deletion of a child's data (e.g., by a parent, guardian, or the teenager themselves).

Russia's experience

In Russia, Law No. 436-FZ "On the Protection of Children from Information Harmful to Their Health and Development" establishes age qualifications for restricting destructive content and defines the obligation of platforms and telecommunications operators to restrict access to content. The trend toward measures to protect children will expand, especially with the development of access to new technologies. For example, it is predicted that the use of AI in children's education alone will grow by 38.5% per year until 2030.[16]

3. Anticompetitive practices online

The experience of China

In November 2025, China issued Antitrust Guidelines for Platforms.[17] Platforms are required to implement compliance systems and manage risks.

The following rules have been established:

1. Prohibition of horizontal agreements (between platforms or platform users) on price fixing, sales volume restrictions, or restrictions on the introduction of new technologies or products by:

[7] https://www.nitrd.gov/pubs/FY2025-NITRD-NAIIO-Supplement.pdf
[8] https://techwireasia.com/2025/06/china-ai-investment-98-billion-2025-us-rivalry
[9] https://www.europarl.europa.eu/doceo/document/TA-10-2025-0299_EN.pdf
[10] https://ec.europa.eu/commission/presscorner/detail/en/mex_25_2353
[11] Compliance checks with the EU Digital Services Act 2022.
[12] The Parliament recognizes 16 as the age at which a teenager can use social media independently without parental supervision.
[13] https://www.congress.gov/bill/119th-congress/house-bill/6292/text
[14] A data broker is a legal entity that sells, leases, trades, transfers, discloses, or otherwise provides to third parties personal data obtained from an individual, but which the organization did not collect directly from that individual.
[15] The bill distinguishes between different age categories of minors: children (under 13 years of age) and adolescents (13 to 18 years of age). Adolescents may submit a request to delete their PD, but children cannot do so independently without a parent/guardian.
[16] https://www.applify.co/insights/gen-ai-for-k12
[17] https://www.samr.gov.cn/hd/zjdc/art/2025/art_8e05960782204036af6b9583f1413378.html

- Forming common data pools, agreements on interoperability between systems, using cloud storage, AI to coordinate intentions to exchange information.

- Exchanging sensitive information (about pricing, commissions, discount terms, customer bases, traffic distribution mechanisms, etc.).

- Using data, algorithms, and platform rules for coordinated uniform behavior for user segmentation, dynamic pricing, traffic distribution, and product ranking.

2. Prohibition of vertical agreements (between the platform and sellers) on setting resale prices using:

- Big data analysis, AI, and other means for automatic price setting.

- User profiles, predictive algorithms, etc. to directly or indirectly restrict resale prices.

The platform should not facilitate such agreements between platform participants.

3. Prohibition of abuse of dominance through practices such as:

- Unfairly high fees, service charges, marketing.

- Hidden price inflation (fragmentation of service packages, additional types of paid services).

- Unfairly low purchase prices (paying sellers prices for goods that are significantly lower than the prices paid by other platforms).

- Sales at below cost (e.g., subsidizing sellers' prices) to restrict competition (after forcing competitors out of the market, a sharp increase in prices).

- Refusal to deal with counterparties, restricting competition: removing goods from sale, blocking accounts, establishing excessively complex procedures for conducting transactions, restricting traffic, terminating data exchange, including through the use of algorithms for traffic distribution, product placement, etc.

- Restricting transactions, for example, including in the platform rules requirements for sellers not to work with other platforms, including under threat of exclusion from promotions, loyalty programs, blocking, lowering positions in search results, traffic restrictions, creating technical obstacles, etc.

- Requiring the purchase of certain goods (tied sales) and imposing unreasonable terms and conditions on transactions, such as the use of pop-up windows that are mandatory for completing steps in the interface, imposing costs on sellers for participating in platform promotions, restricting the methods of conducting transactions, payment, charging unreasonable fees (technical fees, traffic promotion fees, etc., which were not known in advance).

- Discrimination against platform users – different rules for connecting to the platform, charging fees for both sellers and buyers (e.g., based on preference data, transaction history, devices used, solvency analysis, etc.).

Platforms are required to implement an antitrust compliance system and conduct follow-up risk management (e.g., special assessment after marketing campaigns, investment transactions, etc.).

Russia's experience

In Russia, the Platform Economy Act will come into force in October 2026, regulating certain anti-competitive practices of platforms, such as prohibiting marketplaces from forcing sellers to participate in sales, and ensuring equal access for all sellers to service opportunities (promotion in search results, etc.). However, competition legislation does not yet contain a specific list of practices characteristic of online markets, such as abuse of a dominant position through various technologies, such as slowing down browser traffic, restricting the operation of progressive applications, manipulating data collection consent forms, etc.

There has been an increase in the attention paid by authorities to anti-competitive behavior by platforms: the average annual number of antitrust cases in the digital sectors has grown from 4 cases per year in 2015 to 29 cases per year in 2015–2022.[18]

4. Access to banking data

The EU experience

In November 2025, the EU agreed on a new Payment Services Directive (PSD3),[19] which regulates the activities of payment service providers (banks and non-bank fintech companies) and the procedure for accessing

[18] https://www.cresse.info/wp-content/uploads/2024/09/2024_ps20_pa3_POIRIER_GARNEAU.pdf

[19] https://oeil.europarl.europa.eu/oeil/en/procedure-file?reference=2023/0209(COD)

users' payment account data within the framework of open banking.[20]

With the user's consent, open banking providers (services that the user authorizes to receive account data or make payments) must have access to the user's payment account data, and banks are required to provide such access on a non-discriminatory basis (providing it to all licensed providers on equal terms).

Users will have more control over access to their data: a permissions dashboard is planned, which will allow payment service users to see in one place which providers they have granted access to their payment account data and to manage the consents they have given.

In addition, PSD3 addresses the technical side of payment services: mobile devices and digital services must not create technical restrictions for the operation of payment applications. Smartphone manufacturers (who control the device and its operating system) and electronic service providers (services that provide applications with access to device functions) will be required to ensure that such applications can store and transfer the data necessary to make payments.

Russia's experience

In Russia, a similar mechanism for open access to banking data is still under development. Back in 2022, the Bank of Russia presented a concept for the introduction of open APIs[21] (tools for the secure exchange of data between banks and other financial companies) in the financial market, and in 2024 published a plan that would require the largest banks to connect to APIs starting in 2026 (and other participants starting in 2027).[22] For now, the largest banks exchange data via APIs within the framework of individual partnerships. By the end of 2025, the Central Bank of the Russian Federation plans to prepare and publish draft unified standards for information exchange for open APIs.

According to forecasts, access to financial data will continue to expand: By 2030, the global open banking market will grow from $31 bn in 2024 to $135 bn.[23]

5. Digitalization of public health

The OECD experience

In November 2025, the OECD presented a report on the digitization of public health,[24] highlighting best practices in four areas:

1. Ramping up human resource capacity. Australia has launched a program to improve the digital literacy of medical professionals, where doctors are trained to work with hospital medical information systems.

2. Technological equipment. The OECD recommends using cloud solutions for data storage in healthcare (reducing the load on hospital IT infrastructure); establishing criteria for ensuring data confidentiality in public procurement procedures for hospital software; ensuring the scalability of IT solutions for hospitals; using open source software with built-in compatibility standards for hospital interaction.

3. Formation of health data architecture. New Zealand has approved standards for the interoperability of data and information systems for the exchange of the most frequently requested health data between hospitals.

4. Organizing public participation in data management. Canada has adopted a standard for self-governance of health data for indigenous peoples, who can independently regulate the collection of and access to data in medical organizations.

The US experience

In November 2025, a reform of medical information privacy protection was proposed in the United States:[25] it was recommended that digital service providers for medical services (such as SberZdorovye, SmartMed, etc.) be assigned obligations similar to those of data operators. These obligations are established by the Health Insurance Portability and Accountability Act (HIPAA) only for hospitals and insurance companies. Organizations such as platforms are not obligated to protect health data.

[20] A mechanism whereby users can transfer data about their payment accounts to licensed financial companies through standardized interfaces.

[21] Software interfaces that allow financial institutions to securely transfer data to external participants.

[22] https://www.cbr.ru/Content/Document/File/142114/concept_09-11-2022.pdf

[23] https://www.grandviewresearch.com/industry-analysis/open-banking-systems-market

[24] https://www.oecd.org/en/publications/digitalisation-of-public-health_97204768-en.html

[25] https://www.congress.gov/bill/119th-congress/senate-bill/3097/text?s=1&r=6

The rights of personal data subjects to access, delete, and transfer data, to refuse to sell their data to third parties, and to receive notifications in clear language and in an understandable form are also enshrined in law. Previously, such rights were enshrined at the state level, but now they are enshrined at the federal level.

Singapore's experience

Singapore is continuing[26] to develop a national electronic record system for the collection, storage, and disclosure of health data. Hospitals are required to upload specific types of patient data to the system and comply with technical requirements. Access to the information in the system will be granted to the data subjects themselves and to healthcare providers, including pharmacies. Two types of data can be accessed in the system:

1) Health information that directly identifies an individual (used to provide medical services to patients).

2) Anonymized and aggregated data from hospitals for researchers. To obtain data, researchers must specify the purpose of the information request and their intentions regarding the further disclosure of the information obtained to third parties.

Russia's experience

Back in 2024, Russia approved its "Strategic Direction for Digital Transformation of Healthcare until 2030," which included providing patients and medical organizations with access to health data through the Unified State Information System for Healthcare (EGISZ).[27] Since 2025, all medical organizations have been required to maintain medical records in electronic format. However, the economic potential of such health data collection is not being fully realized—there is no centralized access to the data collected for researchers or medical technology developers. Opening up access to such data would reduce research costs by up to 9% by reducing the amount of duplication in research.[28]

6. Facilitating use of personal data

The EU experience

In November 2025, the European Commission presented a package of amendments to EU legislation aimed at simplifying data management to support innovation, particularly AI.[29] The initiative includes adapting the General Data Protection Regulation (GDPR) to the needs of AI system developers:

1) It is proposed to introduce a separate legal basis for the processing of personal data for the purposes of developing and testing AI systems and AI models: developers no longer need to obtain separate consent for data processing for AI training purposes in order to anonymize this data and include it in the AI training database.

2) A solution is proposed to the problem of re-identification of anonymized data during its analysis using AI. Whereas previously this led to the need to take measures to remove re-identified data from databases, now AI developers only need to take measures to prevent the disclosure of restored personal data to third parties. It is important to prevent the language model from responding to a query by revealing personal data.

Russia's experience

In Russia, the task of simplifying access to data for participants in the digital economy, such as developers of new technologies, is being addressed at the level of experimental legal regimes (ELRs). The ELRs mechanism has been in place since 2020 and involves the development of special conditions for accessing and working with data within each ELRs that is launched. However, the EPRs has a limited scope of participants, so simplifying the conditions for accessing personal data within a single ELRs does not stimulate the development of data-based technologies throughout the country. In Russia and around the world, new modes of centralized data access will be developed with a wider range of participants from different sectors of the economy. Today, the European data space is already being organized in this format in certain sectors, such as healthcare.

[26] https://www.parliament.gov.sg/docs/default-source/bills-introduced/health-information-bill-20-2025980b6831-a710-4386-bb27-f7b7f53d1f95.pdf?sfvrsn=95b05d08_1

[27] Unified State Information System for Healthcare.

[28] https://handbook.pathos-project.eu/sections/0_causality/open_data_cost_savings.html

[29] https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal