

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

- How to provide AI with power
- Restricting children's access to social media
- Benefits of data transfer

Monitoring No.1 (25) (January 2026)

Monitoring was prepared by a team of experts of International Best Practices Analysis Department at the Gaidar Institute.

Authors: researcher Maria Gririch, researcher Ivan Ermokhin, senior researcher Antonina Levashenko, researcher Olga Magomedova, researcher Kirill Chernovol, researcher Economic Policy Foundation Diana Golovanova

The reference to this publication is mandatory if you intend to use this material in whole or in part



Gigabrainsgigawatts!

Countries are making plans to ensure a stable supply of AI capacity

By: Kirill Chernovol

Countries are creating computing infrastructures for AI to operate. Large models require enormous computing power—modern processors and electric power are needed.

Therefore, regulators are accelerating the construction of large data centers and simplifying access to computing for science and business.

Therefore, regulators are accelerating the construction of large data centers (DCs) and simplifying access to computing for science and business.

Such initiatives by [China](#) and [the US](#) were further taken up by the EU, South Korea, and other countries. In 2025, the US launched the Genesis mission to create infrastructure and a platform aggregator for AI systems and data in the fields of energy, science, and defense (we wrote about the mission in [Monitoring No. 11, 2025](#)).

In January 2026, the EU adopted [Regulation \(EU\) 2026/150](#), which defines the conditions for creating “AI gigafactories”:¹ what rights to access computing resources are granted to the state and users. A pan-European co-financing scheme for gigafactories is being introduced through the Joint Program for High-Performance Computing (EuroHPC).²

The EU's contribution may amount to up to 17% of the capital costs of the computing part of the project. Projects are selected through a competition, after which access rights are established: how much computing time the EU receives and under what conditions it is allocated.

In other words, the EU, through EuroHPC participants, purchases in advance the use of computing power that can be used, for example, by government agencies or universities.

Importantly, one of the criteria for projects is requirements for sustainability, energy efficiency, and responsible water management at AI gigafactories. The regulation also lays out a plan for the development of quantum computing and the connection of supercomputers.

In South Korea, a [bill](#) was introduced in January 2026 to promote the development of AI data centers. Current regulations restrict direct transactions between power plants and large consumers. Because of this, AI data centers can be located near generation facilities but cannot obtain the required capacity. There are plans to allow power plants outside the capital region to supply electricity directly to such centers. Tax measures to support data centers and relax mandatory requirements for facilities (e.g., no need to install elevators and parking) are being discussed.

Thailand is creating conditions for data centers to obtain green energy on a long-term basis with transparent pricing. In January 2026, a pilot project was launched allowing direct contracts for the purchase and sale of electricity from renewable energy sources (RES) for data centers. [Guidelines](#) for the project were published back in October 2025. The pilot is designed for projects with a duration of at least 10 years. For data center buildings, the threshold for continuous base computing load is at least 50 MW (in the EU, this is the minimum threshold for AI gigafactories), and a backup supply from

¹ AI gigafactories are cutting-edge large-scale enterprises with sufficient capacity to support the entire lifecycle of ultra-large artificial intelligence models and applications, providing supercomputer-level infrastructure. This infrastructure consists of computing power optimized for AI tasks, data

centers, cloud-based user access environments, and specialized services focused on supporting AI operations..

² EuroHPC includes the European Commission, participating countries, and private industry associations such as ETP4HPC, BDVA/DAIRO, and others.

an energy company is also mandatory. Direct contracts are more predictable in terms of pricing than market purchases of energy, and green energy makes data centers more attractive to investors.

Today, AI regulation around the world is shifting toward energy and large investment projects.

In Russia, data centers are regulated by law as infrastructure facilities. In

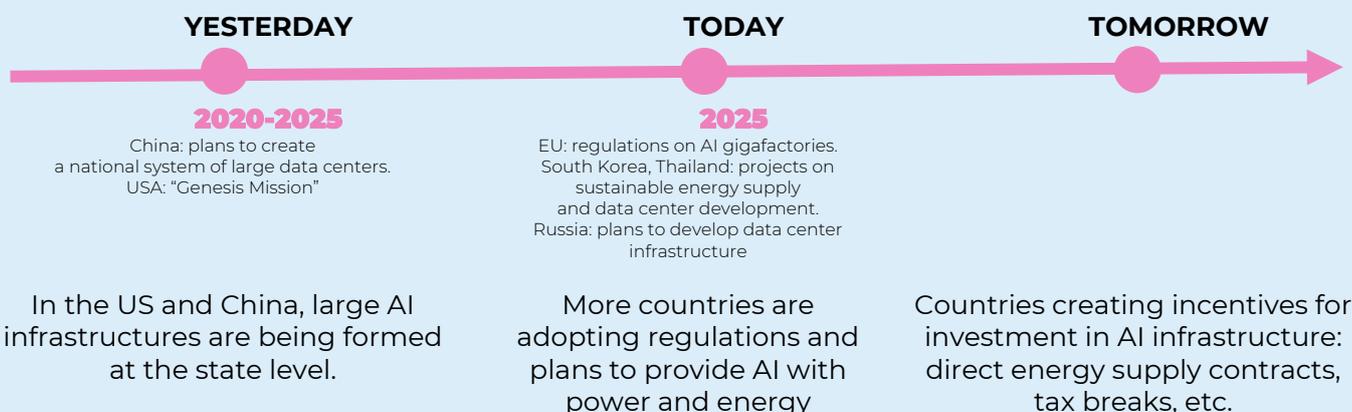
January 2026, the President of the Russian Federation instructed that a plan of measures for the development of data center infrastructure be drawn up by June.

What's next?

The EU [forecasts](#) initial capacity of 50 MW per gigafactory, with an increase to 150 MW. This is 1.3 terawatt-hours¹ of energy per year for one gigafactory in the EU.

In Russia in 2025, excess energy production [amounted to](#) 5.2 terawatt-hours (within the Unified Energy System).² This “surplus” energy would be enough to power three AI gigafactories. There is also a surplus of energy resources—for example, excess coal production³ in 2030 is [estimated](#) at a minimum of 14 million tons,⁴ which would be enough to power another 20 AI gigafactories.⁵

However, supplying 20 gigafactories with coal-based energy per year will result in emissions of 50.1 million tons of greenhouse gases⁶ (equivalent to the emissions of [11 million passenger cars](#)).



¹ 150 MW * 8760 hours = 1,314,000 MWh

² In 2025, electricity generation by power plants in the Russian Unified Energy System amounted to 1,166.4 billion kWh, while consumption amounted to 1,161.2 billion kWh, 1,166.4 – 1,161.2 = 5.2 billion kWh = 5.2 TWh.

³ The assessment of the potential of AI gigafactories for Russia was made on the basis of excess coal production as a benchmark for the theoretically available volume of energy resources. Factors such as (1) the territorial location of resources and infrastructure constraints for building gigafactories in these locations, and (2) the climatic consequences of coal use today are not analyzed here.

⁴ Conservative scenario of the Russian Ministry of Energy: production – 341 million tons, domestic demand – 134 million tons, exports – 193 million tons.

⁵ Approximately 0.52 million tons of coal [are required](#) to generate 1 terawatt-hour of energy, i.e., 0.67 million tons for one gigafactory with a capacity of 150 MW, 14/0.67 = 20.89.

⁶ Calculation based on: URL: <https://sro150.ru/kalkulyator-vybrosov-dioksida-ugleroda-so-pri-ispolzovanii-energeticheskikh-resursov-prilozhenie-7-energopasporta>

Digital Adulthood

How countries restrict children's access to social media

By: Maria Girich

In January 2026, France [discussed an initiative to ban](#) children under the age of 15 from using social media. Existing accounts would be blocked. The only exceptions would be non-commercial online encyclopedias and educational or scientific reference resources.

The trend to restrict children's access to social media took shape in late 2023–2024. France was one of the first to take action ([the law](#) was passed, but it never came into effect). Then Australia, China, New Zealand, the US, and others joined the initiative. In 2025–2026, the measures began to take effect.

Companies are trying to challenge the ban policy. For example, [Australia](#) introduced a minimum age for using social media of 16 years old in December 2025. However, the social network Reddit [filed a lawsuit](#) against the unfairness of the law, arguing that information on social media can be accessed by children without creating an account, so it is necessary to restrict the types of public information, rather than the ability of children to use social media. In addition, if a child registers on a social network, it is easier to track the content they view.

The introduction of additional child protection mechanisms entails direct costs for platforms. [According to estimates](#) by the British regulator Ofcom,¹ verifying the age of already registered users costs approximately £5,000 per 100,000 accounts.

For this reason, some countries choose time limits rather than a complete ban. For example, in January 2026, the state of Virginia (USA) introduced regulations against addictive algorithmic feeds: children under the age of 16 should be limited to one hour of social media use per day, and this limit can only be

increased with the confirmed consent of their parents.

In [California](#), the risks of addiction are combated through mandatory warnings. If the platform is not sure that the user is over 17 years old, it displays a notification for 10 seconds (at least 25% of the screen) about the risks to mental health when the user first logs in for the day. When 3 hours of active time are reached, a warning appears for 30 seconds (covering at least 75% of the screen, with no option to close it). It is then repeated at least once an hour.

Age restrictions are being introduced not only for social media, but also for all apps. For example, in January 2026, Turkey [proposed](#) limiting the use of platforms and games for children under 16 to 55 minutes per day and introducing a “night ban” on access from 10:30 p.m. to 9:30 a.m. (except for educational content).

In Virginia (USA), [it has been proposed](#) to introduce requirements for the use of app stores (App Store, Google Play, etc.) only under parental control. A child's account must be linked to a verified parental profile. Downloading apps and in-game purchases (e.g., virtual currency) are only allowed with parental consent. Parents must be informed of the age rating of the app/purchase, information about the data collected by the developer, and measures to protect it. There is also a mechanism for withdrawing parental consent with notification to the developer; and if fraud or “age-inappropriate” purchases are suspected, the store has the right to request confirmation and data from the parents again.

¹ Based on calculations of employee salaries (engineers, IT specialists, etc.).

It is worth noting that the OECD has been compiling reviews of social media and applications in terms of child safety for several years. Thus, in its [2023 review](#) of Russian social media (risks of sexual exploitation), the OECD noted that VKontakte (VK) uses a more advanced system: hybrid moderation with proactive monitoring and automated detection, rapid response to complaints, and elements of public accountability.

Odnoklassniki relies solely on user complaints, discloses fewer details about the detection of violations, and does not

has no mechanisms in place to protect children: no special privacy policies, advertising and content restrictions, or parental control features. Therefore, the age threshold seems rather declarative: the OECD has recorded the use of Telegram by groups targeting minors.

Whats' next?

In Russia, there is no ban on social media for children and teenagers. VK and its affiliated social network Odnoklassniki formally do not allow users under the age of 14 to register. TikTok allows users aged 13 and older. Telegram and Reddit do not verify age during registration. YouTube has no age limit, however offers a children's account with parental controls.

According to estimates by [Mediascope](#), teenagers as young as 9 actively use Telegram (36% of their time spent on social media) and TikTok (49%). Potentially, 5.7–6.4 million Telegram accounts¹ in Russia may belong to children aged 10–14.² And if Russia bans the use of social media for children under 15, Telegram could lose³ between 176 and 198 million rubles per year when the accounts of children aged 10–14 are closed.⁴



publish transparency reports.

In its [report from 2025](#), the OECD analyzed the rules of Telegram, the only service in the EU with a minimum registration age of 18+. However, Telegram

¹ Calculations are based on the fact that children aged 10–14 make up 6.12% of Russia's population ([Rosstat data](#)). Telegram's average monthly audience [is estimated](#) at 93–105 million unique users. If we apply the specified proportion of children to this audience, the approximate number of children's accounts could be around 5.7–6.4 million.

² Since the available demographic statistics from Rosstat are published in broad age groups (e.g., 5–9 and 10–14 years old) and do not allow us to identify the number of 9-year-old children specifically, for the sake of simplicity in comparison with Mediascope's estimates, we have conditionally adopted 10 years as the minimum threshold for "active age" (as the closest available threshold in Rosstat data).

³ Telegram's potential losses entail a certain amount of potential savings for users of this resource from subscriptions, paid content, etc. (no assessment was made).

⁴ The calculations are based on [an estimate by the Financial Times](#): in 2023, the publication calculated that Telegram earns up to \$0.4 per user (approximately Rb31). We then multiply \$31 by the estimated number of accounts belonging to children aged 10–14 on Telegram — 5.7–6.4 million — to obtain an approximate estimate of the potential revenue attributable to this audience.

Saving on data

On the effects of introducing the right to transfer personal data in the health insurance sector

By: Olga Magomedova

The right to change service providers only becomes a reality when users can transfer the personal data necessary for the service to the new provider. Therefore, many jurisdictions, such as the EU, the US, Brazil, Japan, China, New Zealand, Saudi Arabia, and the UAE, enshrine the right to transfer personal data, i.e., the right to request that one provider transfer data to another provider.

Canada also plans to enshrine the right to data portability in the Personal Information Protection Act 2000 ([Bill C-15](#)). In 2024, [Quebec](#) became the first province to require data operators to transfer data to third parties at the request of the data subject within a reasonable time frame (in practice, 30 days).

What effects are expected from the innovation?

In January 2026, the Canadian Competition Bureau [calculated](#) how much time and money the right to transfer personal health data between insurance companies would save users of health insurance services in Canada. The total savings for the population could range from \$810 million to \$2.78 billion per year. The [calculations](#) took into account the cost of different insurance programs and the time spent by 3,000 Canadian consumers searching for a suitable insurance company.

Canada also plans to enshrine the right to data portability in the Personal Information Protection Act 2000 ([Bill C-15](#)). In 2024, [Quebec](#) became the first province to require data operators to transfer data to third parties at the request of the data subject within a reasonable time frame (in practice, 30 days).

What effects are expected from this innovation?

In January 2026, the Canadian Competition Bureau [calculated](#) how much time and money the right to transfer personal health data between insurance companies would save users of health insurance services in Canada. The total savings for the population could range from \$810 million to \$2.78 billion per year. The [calculations](#) took into account the cost of different insurance programs and the time spent by 3,000 Canadian consumers searching for a suitable insurance company.

Where do these huge sums come from?

In Canada, the public health insurance system, [Medicare](#), does not cover a number of medical expenses for patients, which is why the private health insurance market is well developed in the country.

According to the Canadian Health Insurance Association, there are currently 145 companies operating in the market, whose insurance services cover [74%](#) of the population. Moreover, [83%](#) of insurance contracts are concluded on the basis of individual insurance plans.

However, the cost of such an individual plan depends on the insurer's access to the patient's health data. If the company does not have access, the plan will be calculated based on maximum risks, increasing the cost of private insurance for the patient. Therefore, when a patient changes insurance companies, their accumulated health data must be transferred to the new provider.

At the same time, companies are not required by law to transfer the collected data to third parties, even at the client's request, which is why insurance companies refuse to transfer data, not wanting to share it with competitors.

Because of all this, it is difficult for customers to change insurance providers: new insurance, calculated without health data, is very expensive, and the customer is tied to one provider.

The issue of health data portability first arose in practice in the United States, where there is essentially no public health insurance system, and a person's inability to pay for private insurance effectively means no access to medical care. Therefore, the US was the first to enshrine the right to data portability in the 1996 Act. In countries where the population is guaranteed access to the public healthcare system, the right to data portability appeared much later, and in the context of other industries. For example, in the EU, the right to data portability was first enshrined in the General Data Protection Regulation only in 2016. The reason for this was the need to regulate markets that are vulnerable to the risk of user data being concentrated on large platforms.

According to OECD estimates, [25%](#) of users refuse to switch providers due to

difficulties with data transfer. Therefore, in highly competitive segments, companies voluntarily provide all the technical conditions for data transfer.

For example, in the EU, [72%](#) of banks implement open APIs.¹ Therefore, in order to make services more accessible to users in markets with increased risks of monopolization (e.g., telecommunications services), states need to establish obligations for data operators to transfer data to other parties at the user's request.

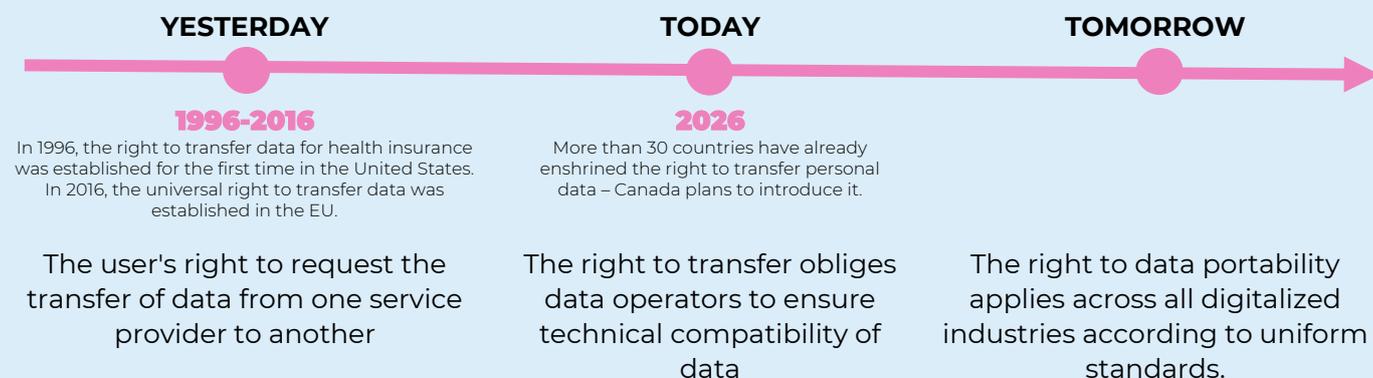
In Russia, users have the right to access their data and therefore, in theory, they can transfer data themselves by obtaining it from one provider and transferring it to another. However, the right to transfer data directly from one provider to another is not enshrined in law.

API (Application Programming Interface) is a set of rules, protocols, and tools that allows one computer program to interact with another.

Securing the right to transfer in Russia can have positive effects.

What's next?

According to OECD estimates, access to and exchange of data can increase the value of data for users by 10-20 times, and for the economy as a whole by 20-50 times. The OECD has calculated² that access to and exchange of data generates social and economic benefits ranging from [0.1% to 2.5%](#) of GDP (in some studies up to 4% of GDP).



¹ API (Application Programming Interface) is a set of rules, protocols, and tools that allows one computer program to interact with another.

² The OECD's economic calculations of the impact of data freedom on GDP take into account a variety of factors, including cross-border data transfer requirements, data storage requirements, and industry-specific data

handling requirements. Moreover, the weight of the factors taken into account may vary depending on the structure of the country's economy (the more digitized sectors there are, the more significant the impact of regulatory conditions on data circulation). Consequently, data portability in a jurisdiction is considered only as one of the factors, the weight of which in the overall result depends on the ratio with other factors.

News from **January 2026** that we found interesting.¹

- The European Parliament [has announced](#) a resolution on the protection of intellectual property rights in the training and operation of generative AI. It proposes establishing two basic requirements: transparency and remuneration. AI providers must disclose what materials were used in training and ensure that remuneration is paid to rights holders. The European Commission proposes to introduce a single form for rights holders to refuse the use of their works by AI, and refusals will be stored in a special EU register. It is noted that works created by AI should not be protected by copyright.
- Poland's Ministry of Digital Affairs [has proposed](#) introducing a tax on digital services: it will apply to targeted advertising on digital interfaces, the operation of online platforms (such as social media and marketplaces), and the commercial trading of user data. The tax will be levied on revenue at a rate of up to 3%. Only large companies with global revenues of more than €1 billion and revenues in Poland from services of more than €5.9 million will be liable to pay the tax.
- The European Data Protection Board (EDPB) [has published](#) its opinion on the draft amendments to EU legislation to simplify access to data for operators of AI systems and models (Omnibus Package). The EDPB points out that the processing of sensitive data (e.g., health data) using AI systems is only permitted for specific purposes and only in relation to data that is “strictly necessary” for such purposes. The regulator thus rejects the proposal to simplify the conditions for processing sensitive data for operators of AI systems.



¹ Since 2025, the Gaidar Institute has been developing a digital platform for analyzing news in Russia and around the world on the topic of digital economy regulation – DIgiReg. The news presented is selected by experts based on, among other things, analysis of the platform's data.