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

- DFAs throw off shackles
- Big models, big bills: AI and the environment
- Dangerous connections: regulating anthropomorphic chatbots

Monitoring No. 12 (24) (December 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

GFAs throw of shackles

How the Bank of Russia is changing its attitude toward cryptocurrencies after five years

Authors: Daina Golovanova, Ivan Ermokhin

Five years after the adoption of the law on digital financial assets (DFA), it seems that in 2026, the institution of digital rights and digital currencies in Russia will undergo major changes. In the last week of last year, the Bank of Russia issued a statement that the regulator had prepared a Concept for the regulation of cryptocurrencies on the Russian market. The text of the Concept itself is not publicly available, but there is a description of the document on the Central Bank of Russia's website.

The document mainly focuses on regulating crypto exchanges in Russia. This issue has been awaiting resolution since discussions about the crypto asset market began in 2017. In particular, it is assumed that cryptocurrency trading will be carried out through the existing infrastructure—brokers and exchanges. The document does not say whether other market participants that do not have a broker or exchange license will be able to provide services after obtaining a different special license. It should be noted that most of the world's largest crypto exchanges today were created by new companies in the market, rather than existing financial organizations. Restricting new companies could lead to a decline in innovation and reduce the ability of Russian crypto exchanges to enter international markets. The document also proposes limiting the purchase of cryptocurrencies by unqualified investors to Rb300,000 per year on a single platform. However, given that users from the Russian Federation can purchase cryptocurrencies for other amounts on other foreign platforms, the ban will not reduce the investment risks of citizens but may limit the inflow of funds to Russian crypto exchanges.

As for DFAs, as well as utility and hybrid digital rights, the Bank of Russia has prepared a “quiet revolution” for them: their circulation will be permitted in open networks. What does this mean for companies and investors? It means, for example, that a Russian company can issue a DFA bond not on Russian platforms—the organizers of the issue and exchange, where the buyers are exclusively Russian users—but, in particular, on the Ethereum network. In the future, such DFA may be available for purchase on the largest crypto exchanges, as well as in DeFi protocols. Basically, after the sanctions were put in place, Russian companies will once again have access to international liquidity traded in cryptocurrencies, which means they'll be able to raise funds on more favorable terms than they could domestically. This innovation raises the question: will Russian companies be able to accept payment for DFA, for example, in Bitcoin, and pay coupon income in cryptocurrency?

The development of DFA regulation and the emergence of new legal constructs involving digital rights will be a trend in H2 2025.

In December, a law was signed that introduced regulation for debt DFA (essentially bonds). In the same month, another bill was proposed that would allow investment funds to buy DFA on the same terms as ordinary shares or bonds.

↑ In 1.6 times

went up the number of DFAs placements over first 9 months 2025 and hit Rb 972 bn

Previously, funds were virtually unable to do so because there was no convenient system for accounting for such assets.

And in the same month, another step was taken to develop the DFA market: a bill was submitted to the State Duma allowing real estate to be used as collateral for obligations issued in the form of DFA. Simply put, if a debt is issued in the form of DFA, it can be collateralized with real estate (e.g., an apartment, house, or land plot). The bill also establishes the procedure for registering such collateral with Rosreestr: it will be specified which real estate secures a particular issue of DFA, and its owners will be recognized as collateral recipients. To this end, the following rules are introduced:

- Each DFA issue will be assigned a unique number.
- This number will be indicated when registering collateral with Rosreestr.
- Such DFA can only be bought and sold after the collateral has been officially registered in the form of real estate.

What's next?

The Bank of Russia plans to present a draft of the proposed amendments as early as summer 2026. Their adoption will boost the development of DFAs in Russia, and we may potentially see DFAs being used to attract international investment and settle foreign economic transactions. This is possible in part thanks to the automation of transactions using smart contracts, which will reduce sanctions and other regulatory risks for the parties.

As for the future of digital currency payments, no changes are expected: it will still not be possible to make payments in Bitcoin either domestically or internationally.

Big models, big bills

How regulators are learning to calculate the "price" of AI in kilowatts and CO_2

Author: Maria Girich

Today data centers around the world consume up to 1.5% of electricity, and by 2030 consumption will double.

The French antitrust authority has released a Report on competition issues related to the impact of AI on energy and the environment. According to the IEA, while a typical data center has a capacity of 10–25 MW, an AI-focused data center has a capacity of over 100 MW. This is comparable to the annual electricity consumption of 100,000 households.

It is evident that AI has an impact on the environment. Energy for data centers is often produced from fossil fuels. However, there is a trend toward investing in decarbonized energy sources, such as renewable energy and nuclear power, especially in areas with high electricity demand. For example, in 2024, Microsoft agreed with Brookfield to supply 10.5 GW of green power in the US and Europe. Tech giants Amazon, Google, and Oracle have announced the introduction of small modular reactors.

The EU AI Act (Regulation 2024/1689) already sets the task of developing codes of conduct to minimize the environmental impact of AI systems.

When it comes to competition, the French antitrust authority highlights three issues.

Difficulties represent *the first issue* in accessing power grids and uncertainty about energy prices (energy costs account for 30–50% of a data center's operating costs).

The growth of data centers has led to an increase in the number of applications for technological connection to high-power grids. The risk of network overload in areas of high demand has increased: data centers are often organized as clusters with redundancy (i.e., the installation of several technical resources designed to replace each other in the event of a failure). There is also a risk that large players will "take over" profitable sites to the detriment of smaller ones.

In France, in particular, a number of measures have been taken. For example, an accelerated procedure has been introduced for connecting energy-intensive industrial consumers (0.4–1 GW). The state selects several areas in advance where it is possible to connect large consumers and reserves capacity there for potential projects so that investors can then come in and quickly connect to the electricity grid. There is also the problem of some energy consumers having "predatory" strategies. For example, enormous capacity is reserved in the grid so that competitors cannot obtain this capacity, but in fact it is not used, which creates an artificial shortage. In this regard, a rule has been introduced: it is not possible to reserve capacity without confirming the rights to use the land on which the project is planned to be located. And if the requested capacity is not used, it can be reduced. The idea of "dynamic" capacity allocation is being discussed: capacity is reserved not for those who applied first, but for those who build and commission the facility faster.

The second issue is related to the emergence of the concept of "frugal AI"—the prioritization of solutions that minimize material and energy costs and

↑ 91%

of water consumption occurs during training and AI inference

environmental footprints to assess the "necessity" of AI use (i.e., AI solutions are only used when they are indispensable), and which are optimized throughout the entire chain (development, implementation, use) to minimize resources. In fact, the question has arisen of developing smaller AI models that help to "save" on computing power. For example, open-source helps: if a model has already been trained, it can be reused, saving resources, rather than having to train it from scratch every time.

In this regard, the state and companies are beginning to introduce "green" parameters into procurement and tenders. This creates the risk that companies may overstate the environmental benefits of their AI solutions and data centers due to the lack of scientifically sound calculation methods, gaining an undeserved advantage in procurement. Also, large operators may refuse to disclose data on their environmental footprint and frugality, reducing transparency.

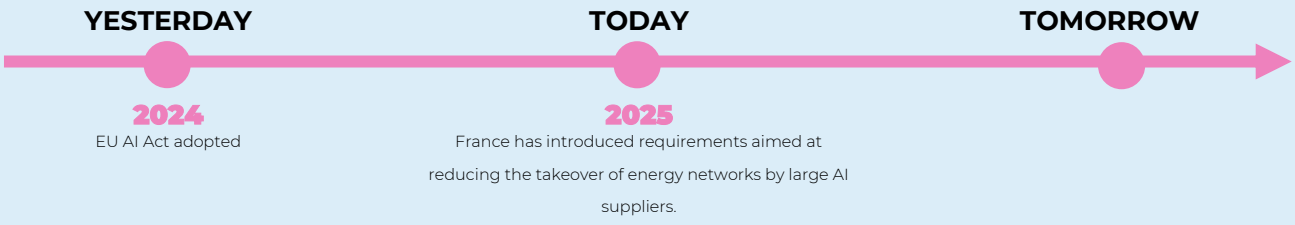
The third issue is the need to develop uniform methods for assessing the environmental impact of AI. Currently, there are many different methods that are not always sufficiently scientifically sound. Alternatively, the standard may be developed by major players who lobby for their own interests without offering environmental improvements.

In Russia, the Ministry of Digital Development, Communications and Mass Media projects a 2.5-fold increase in energy consumption by Russian data centers by 2030, which may also drive up electricity prices amid energy shortages in Russia.

.

What's next?

With energy demand on the rise, regulation will move toward "energy allowances" for AI and data centers (as well as other areas such as mining) in Russia and abroad, especially in regions with energy shortages. Countries will encourage the transition to nuclear and low-carbon energy. At the same time, we can expect the introduction of mandatory reporting by companies and the development of methodologies for comparing resource efficiency data. At the same time, there may be an increase in long-term energy contracts, which will create antitrust risks, for example, due to discrimination and the closure of access to energy networks for smaller suppliers of data centers, AI services, etc.



The idea of developing environmental standards for AI

Rules for AI environmental standards to reduce risks to competition are being discussed.

Introduction of green procurement AI, environmental reporting for suppliers AI as a competitive advantage

Dangerous connections

How countries are seeking to regulate the security of anthropomorphic chatbots

Author: Kirill Chernovol

Regulators around the world are paying increasing attention to “human-like” chatbots. This type of generative AI designed to mimic human communication for various purposes. If used improperly, they can cause harm, and developers are usually held responsible. Regulators want chatbots to have built-in measures to keep users safe.

On December 9, 2025, US states attorneys general sent a letter to 13 companies that develop generative AI-based chatbots, including OpenAI, Google, Meta, xAI, and others. The attorneys general highlight two problems.

The first is “agreeability”: the bot agrees excessively, confirms the user's fears and misconceptions, and may push them toward dangerous decisions. Retraining based on human ratings and quick “like/dislike” buttons reinforce this effect.

The second is misleading responses, including instances where the bot writes as if it were a real person. Particular emphasis is placed on chatbot interactions with children: references are made to sexualized “romantic” dialogues, requests to hide correspondence from parents, encouragement to take drugs, harm oneself, etc. Around 72% of US teenagers have communicated with a chatbot at least once.

In the US, there have already been a number of lawsuits against AI developers for violating the rights of minors and causing harm to users' mental health—at least seven cases since 2020.[1] For example, in Garcia v. Character Technologies Inc., the plaintiff claimed that the platform's developers did not take “sufficient measures” to prevent irreparable consequences for her 14-year-old son. After the dispute, the companies implemented automatic chat termination when certain topics were raised.

Chatbots can also give medical or psychological advice, which violates laws requiring counseling licenses to provide such advice.

Companies are asked to improve the safety measures of their products, such as safety testing prior to launch; persistent warnings on the input screen; disabling the chatbot if dangerous responses cannot be stopped; independent audits and assessments of the impact on children; a public incident log and a target response time (e.g., within 24 hours for the most dangerous cases); age-based dialogue settings and protocols for reporting cases of threats of violence, drug use, and self-harm to specialists, police, parents, etc. The actual responsibility for user safety falls primarily on chatbot developers.

China has taken the path of stricter regulation. In December 2025, a draft of Temporary Measures for Regulating Human-like AI Services was presented. It prohibits practices that most often lead to harm: encouraging suicide and self-harm, using manipulation, misleading users, etc. Providers must issue messages urging users to seek help, and in cases of statements of intent to harm oneself, connect the person with their parents or legal representatives.

A special regime for the use of AI is also being introduced for minors, and if the chatbot's function is to provide “emotional support,” then the child can only use it with the express consent of a guardian. In other words, under China's approach, the responsibility for the safety of vulnerable users (children) will fall on both providers and the child's legal representatives. This eliminates the risk that claims will be made against the provider based on the logic that “the child was harmed, so the provider failed to ensure safety.”

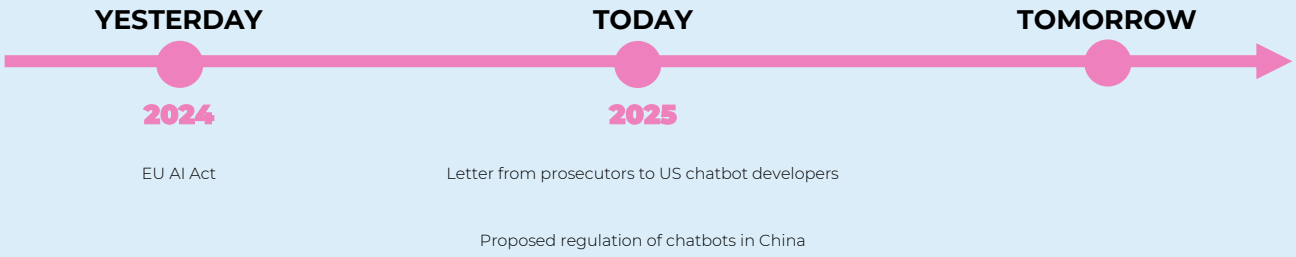
---

[1] ES v. Character Technologies, Inc., PJ v. Character Technologies, Inc., Montoya v. Character Technologies, Inc., Garcia v. Character Technologies, Inc., Christopher “Kirk” Shamblin, et al. v. OpenAI, Inc., et al., Hannah Madden v. OpenAI, Inc., et al., Jennifer “Kate” Fox, et al. vs OpenAI, Inc., et al.

The trend towards protecting vulnerable user groups was set by the OECD in its 2019 AI Recommendations. The EU's 2024 AI Act contains increased requirements for the safety of generative AI systems, and in 2025, the EU published guidelines on data protection in generative AI systems. The current initiatives are a continuation and elaboration of the global trend towards more sophisticated protection for users interacting with generative AI. In Russia, regulation of such systems is currently limited to industry recommendations on AI ethics. In December 2025, the government instructed the Ministry of Digital Development, Communications and Mass Media to develop proposals for regulating AI, which may include security requirements for humanoid chatbots. The results will be announced in March 2026.

What's next?

The trend toward special security requirements for chatbots will spread across countries in the coming years as their use grows: Gartner projects that by 2029, up to 80% of everyday communications with AI will be conducted through human-like agent systems. The key issue here will be the distribution of responsibility. Most countries are likely to choose to establish a closed list of security measures, risk management, and disclosure requirements. The general logic will be the same: chatbots should not engage in behavior that would be considered illegal if a human being behaved in the same way in correspondence.



For the first time, standards have been established for the safety of generative AI and the protection of vulnerable users.

Regulation of generative AI systems is becoming more sophisticated, with specific requirements emerging for chatbots that mimic human communication.

Stricter regulation of chatbot manufacturers and providers, especially with regard to child protection

News from December 2025 that we found interesting.[1]

- The Dubai International Financial Centre (DIFC) has announced the introduction of special tools for resolving disputes related to crypto assets: a mechanism for the temporary judicial storage of crypto assets has been introduced, and courts have been given the ability to use services to track the movement of crypto assets.

- Companies associated with cryptocurrencies (such as Circle and Ripple) have begun to receive preliminary approvals for banking licenses. This will allow them to connect to the US payment infrastructure.

- The Hong Kong Insurance Authority has introduced draft rules allowing insurance companies to invest their own capital in crypto assets.

- In New York (US), the trend towards increased government control over the safety of AI models released to protect consumers continued with the passage of the Responsible Approach to AI Safety Act (RAISE Act). Developers must publish safety protocols when releasing the most powerful advanced AI models to the state market. Developers must report all AI security incidents to the state attorney general within 72 hours.

DIGEST

[1] From 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.