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

- E-commerce platforms restrictions
- Data access
- Platform pricing
- Regulating crypto assets
- Responsible AI governance

Monitoring No. 7 (19) (July 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, legal counsel, Economic Policy Foundation

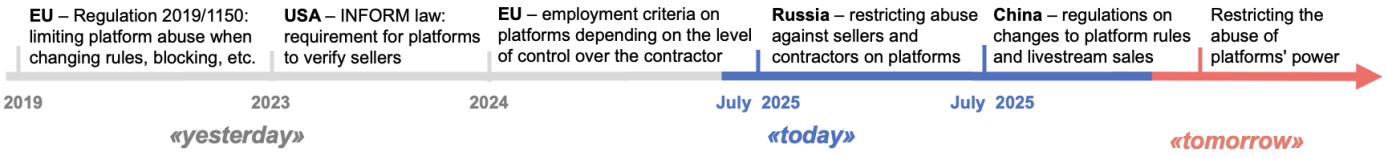
"July is the peak of summer.
The newspaper reminded me,
But before all newspapers –
The waning light of day."
Alexander Tvardovsky

In July 2025, we can identify 5 events that define trends in the development of digital economy regulation globally.

Trend No. 1. E-commerce platforms restrictions

In July 2025, Russia adopted a law regulating intermediary platforms, including employment platforms. The law establishes the right of sellers to refuse participation in platform sales, the requirement to notify platform users of contract changes, etc. In China, a procedure for gathering public opinion when changing platform rules has been introduced, and a new area of e-commerce, livestream sales, has been regulated.

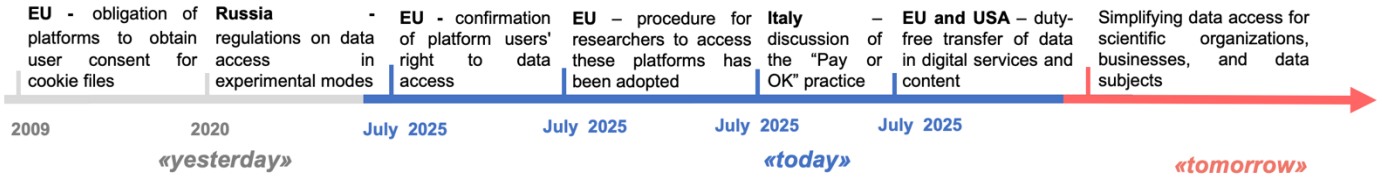
Trend
Restrictions for e-commerce platforms



Trend No. 2. Data access

The EU Court overturned the European regulator's decision to deny a user access to information about the activities of a data processor. The European Commission has developed conditions for free access to platform data for researchers. Italy discussed the practice of platforms collecting user data as payment for access to content. The EU and the US announced a trade agreement that includes zero custom duties on electronic transmissions.

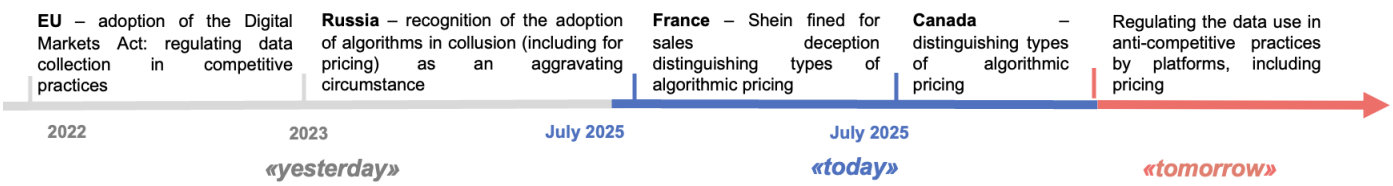
Trend
Data access



Trend No. 3. Platform pricing

In July 2025, Canada prepared an overview of algorithmic pricing practices, and France fined the Shein marketplace €40 mn for providing inaccurate information about sale prices.

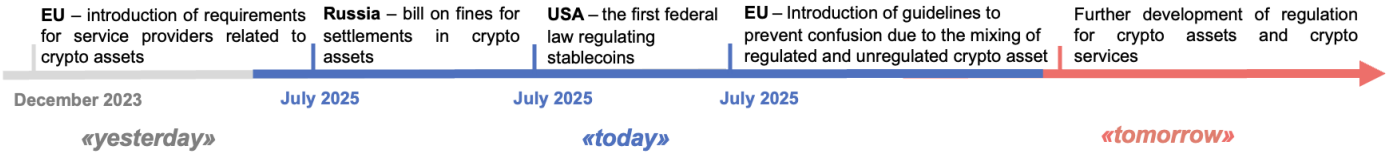
Trend
Platform pricing



Trend No. 4. Regulating crypto assets

In July 2025 ESMA[1] issued guidance for crypto asset service providers on the need to clearly distinguish between regulated and unregulated crypto assets on their platforms (in advertising, contracts, etc.). In the US the first federal law regulating payment stablecoins came into force. In Russia a bill introducing fines for the use of cryptocurrency in settlements was submitted to the State Duma.

Trend
Regulating crypto assets



Trend No. 5. Responsible AI governance

In July 2025, the EU and the UK issued recommendations on responsible AI concerning the fight against deepfakes and AI security. In the US, the AI Plan now includes support for startups, testing foreign AI systems for threats, and other topics. In Russia, the Code of Ethics for AI in the Financial Market enshrines the right of customers to refuse to interact with AI, as well as the right to know why a particular decision was made, etc.

Trend
Responsible AI governance

In July 2025, a number of innovations were introduced in Russia:

1. Criteria for online advertising approved[2]

The approval of criteria is particularly important following the introduction of a 3% levy on income from online advertising[3] in April 2025. Online advertising is defined as information on marketplaces (aggregators), classifieds, search engines, and social networks aimed at promoting a product, service, or brand. However, the following information is not considered advertising:

1) Information that is of a reference, informational, or analytical nature. For example, search results without signs of promotion; catalogs of goods/services, etc.

2) Private advertisements unrelated to business, such as the sale of personal property.

The new criteria eliminate the risk of levying a fee on non-advertising information, for example, when placing product cards on marketplaces. At the same time, the new criteria do not take into account a number of advertising features previously noted by the FAS, such as the placement of product descriptions and seller contact details on their own resources.

2. Restrictions on the use and advertising of VPN have been introduced.

[1] European Securities and Markets Authority.
2 Decree of the Government of the Russian Federation No. 1087 of July 24, 2025 "On the Approval of Criteria for Classifying Information Distributed on Certain Information Resources in the Information and Telecommunications Network 'Internet' as Advertising".
3 Resolution on the approval of the specifics of calculating and paying mandatory deductions provided for in Part 1 of Article 182 of the Federal Law "On Advertising" and the procedure for monitoring the completeness and timeliness of such deductions.

The Russian Code of Administrative Offenses[4] introduces liability for circumventing blocks and searching for extremist materials[5][6] via VPN[7] or similar services. However, there is a risk of broad interpretation of this prohibition. For example, it is unclear who will monitor access to such resources via VPN (especially if the IP address changes) and how. Will viewing content on a social network recognized as an extremist organization be a violation, or will the violation already be considered complete when photos are posted on that social network?

Advertising VPN services is also prohibited (penalty: up to Rb500,000). VPN service owners must restrict access to prohibited resources via VPN at the request of Roskomnadzor. At the same time, the use of VPN for everyday purposes remains legal. At the same time, the use of means to circumvent blocks when committing administrative offenses and criminal offenses will be recognized as an aggravating circumstance with the subsequent imposition of more severe penalties.

In order to facilitate the identification of individuals using VPN services to search for information, a ban has been introduced on the transfer of means of identification in telecommunications networks (mobile phones or accounts)[8].

In addition, in order to facilitate the identification of people using VPN services to search for information, a ban has been introduced on the transfer of one's mobile phone number or account to another person for use.

3. RuStore's technical limitations are recognized as a product defect.

Back in 2022, the Russian government developed RuStore (a national unified app store), which became mandatory for pre-installation on electronic devices (phones, computers). And in July 2025, the Consumer Protection Law prohibited manufacturers of technically complex devices from restricting the ability to install programs and applications through RuStore, as well as the use of such programs (e.g., restrictions on search, updates, management of their settings, etc.), and from restricting payment methods for applications in RuStore.[9] The introduction of regulation is due to the fact that certain device manufacturers (primarily Apple) restrict the ability to download applications from third-party websites, competing app stores, etc. in their license agreements.

Now, restrictions on the functioning of RuStore and downloaded applications will be considered a defect in the product, so consumers will be able to return it to the seller for repair, replacement, or a refund.

[4] Code of the Russian Federation on Administrative Offenses (Art. 13.53).
[5] According to the federal list of extremist materials of the Russian Ministry of Justice.
[6] Federal Law No. 281-FZ of July 31, 2025, “On Amendments to the Code of the Russian Federation on Administrative Offenses.”
[7] Software and hardware for accessing information resources and information and telecommunications networks with restricted access.
[8] Code of the Russian Federation on Administrative Offenses (Art. 13.29).
[9] Federal Law No. 194-FZ of July 7, 2025, “On Amendments to the Law of the Russian Federation "On the Protection of Consumer Rights."

Key aspects

1. Restricting e-commerce platforms

Experience of China

In July 2025, a draft Regulation[10] concerning agreements for the provision of services to business users and consumers on platforms, including marketplaces, classifieds, social networks, etc., was put up for discussion.

If a platform changes its terms of service, public consultations must be held. The draft amendments must be published and opinions must be collected within seven days. All opinions must be taken into account, and if they are not accepted, the reasons must be stated. The new rules must then be published seven days before they come into force (in Russia, 15 days' notice of changes is required). As in Russia, China requires all versions of platform rules to be stored for at least three years.

It is prohibited to impose unfavorable conditions on business users:

1) Unreasonable after-sales obligations without the seller's consent – an obligation to refund the buyer without returning the goods (this restriction does not exist in Russia).

2) Compulsion to participate in the platform's advertising campaigns at the seller's expense (a similar restriction exists in Russia).

3) Unreasonable fees:

– Passing on costs to sellers if goods are sold at a price lower than that set by the seller due to a technical failure on the platform.

– Charging sellers for access to their own business data.

– Forcing sellers to purchase additional services, such as requiring a paid subscription under threat of reduced visibility of their goods.

Today, a new trend in e-commerce is developing worldwide - livestream sales - live broadcasts (streams) during which goods and services are sold. Livestream sales are growing by 20–30% annually worldwide.

In July 2025, China proposed regulations for livestream sales[11] for discussion. Streaming rooms are created on platforms through which the broadcast is conducted. The broadcast is conducted by a streamer who advertises the goods or services of sellers. Advertising agencies responsible for planning, setting up, etc. for live broadcasts also connect to the broadcasts. Responsibilities are established for each type of participant.

Streaming rooms are created through the platform, so the platform must verify the identity of the streamer, who is verified at the beginning of the live broadcast and during the broadcast through dynamic verification systems. The platform is required to provide training for streamers and advertising agencies.

The platform must establish a stream room management system: grade stream rooms based on their compliance with legal requirements, as well as the number of subscribers and views, sales volume, transaction amounts, etc. For stream rooms with a large number of visitors and sales volume, additional measures are implemented, such as technical monitoring for violations in real time, increasing the storage period for video recordings of broadcasts, etc.

The platform must prevent streamers from using deepfakes, etc.

Stream room operators are required to:

1) Post information about sellers' goods and services. Information must be provided without imposed checks (captcha), donation requests, etc.

2) Verify streamers (identity, qualifications, status, etc.).

3) Moderate the chat during the stream, removing prohibited content.

Russia's experience

In July 2025, the Platform Economy Act was adopted, regulating "intermediary platforms" that allow users to place orders, list goods and services, make transactions, conduct payments, etc. The regulation covers relations between platforms (such as marketplaces, classifieds, taxi platforms, courier services, etc.) and their partners (service providers, workers, sellers of goods, and delivery points).

Intermediary platforms, including foreign ones, will be included in a special register. Foreign platforms must also comply with the so-called "landing" law.

Foreign individuals and self-employed persons may be partners of platforms.

[10] https://www.samr.gov.cn/hd/zjdc/art/2025/art_ed7d047de7cd423e981890d4ece9e974.html

[11] https://www.samr.gov.cn/hd/zjdc/art/2025/art_da63265146f741cd8bc80d2bba4e1e37.html

Firstly, the new Law establishes the following obligations of platforms in relation to sellers of goods and services:

– Provide the opportunity to include information about the seller, their goods/services, licenses, certificates, etc., including information on compliance of goods with technical regulations and labeling requirements, including in the Honest Mark system, in the product description.

– Verify the information in the product description to ensure that the goods have not been withdrawn from circulation.

– The government will establish a procedure for accessing information systems containing the above information so that the platform can verify it.

– Separate goods and services sold by the platform from those sold by its partners.

Rules have been established to limit platform abuse:

1) The platform does not have the right to force sellers to offer discounts during sales at their own expense. The platform must notify sellers of the introduction of a discount 5 days in advance and obtain written consent from the partner, in which the partner sets the minimum price, the quantity of discounted goods, and the duration of the discount. The platform may introduce discounts without the partner's consent only at its own expense. It is prohibited to punish sellers for refusing to participate in sales, for example, by lowering their rating, changing the position of the product card in search results, etc.

2) The platform has the right to unilaterally amend the agreement with the partner, the pick-up point, but subject to 15 days' notice (similar to the EU). And 45 days in advance if the platform changes the partner's liability measures, increases commissions, reduces the pick-up point's remuneration, or changes the terms of acceptance, storage, delivery, issuance, and return of the seller's goods.

3) The platform can restrict the ability to post product cards and access to the personal account only upon 3 days' notice, or on the day of notification if the personal account has been hacked.

The logistics infrastructure of platforms (warehouses, distribution centers, pick-up points, etc.) must comply with fire safety and sanitary and epidemiological requirements, including food safety requirements. The contract with the pickup point should specify the rules for distributing the risk of damage or accidental loss of goods.

Moreover, the Law introduces regulations governing platform employment – couriers, taxi drivers, and other workers and service providers on platforms under civil law contracts (CLCs). Criteria for working under CLCs have been established:

– Performer provides individual services without being tied to a schedule or having to comply with internal work rules.

– Performer can refuse an order, and the platform can't punish them for it.

– Performer gets paid separately for each order.

– Contractor may not involve third parties in the work/services – only independent performance.

– Platform is not obliged to provide social guarantees, weekly days off, vacations, etc.

Interestingly, the platform is obliged to enable performers to apply for a contract with an insurance provider (medical, pension, etc.) through the platform, as well as to provide preferences to performers who voluntarily join insurance schemes (the government will set the minimum level of such preferences). For example, the platform may fully or partially reimburse performers' insurance costs.

The platform must monitor:

– Working hours for jobs and services involving increased danger or risk to life, health, or property (e.g., limiting taxi drivers' working hours to 12 hours).

– Risks of involving minors in work that minors are not permitted to perform.

– Maximum permissible standards for physical and other types of stress.

– Compliance with legislation on the legal status of foreign nationals.

The platform may use automated decision-making technologies (such as AI algorithms) to form orders, determine remuneration (the order and terms of payment), publish ratings of performers, provide opportunities for additional professional education, provide the performer with tools and materials for the execution of the order (e.g., clothing), verify the contractor's experience and qualifications, and assess the risks associated with the safe performance of work and services.

2. Data access

The EU experience

In July 2025, the EU Court of Justice ruled on the case of Lisa Ballmann v. European Data Protection Board (EDPB).[12] Ballmann requested the EDPB to provide documents from its investigation into Meta,[13] which was the data processor for the plaintiff on Facebook. The EDPB refused, arguing that Ballmann was not a party to the investigation and could not request access to the investigation materials.

However, the EU Court recognized that it is not necessary to be a party to the proceedings in order to have the right to access investigation materials. According to Article 77 of the GDPR,[14] every user has the right to lodge a complaint with a supervisory authority regarding a breach of the Regulation and to be informed about the progress of the complaint, including the investigation materials. The EU Court gave a broad interpretation of the rule: the data subject has the right to access information not only about the processing of their own data, but also about the data processor's activities in general.

Also in July 2025, the European Commission approved rules on free access for researchers to data from very large platforms. Back in 2022, the EU adopted the Digital Services Act (DSA),[15] which imposed obligations on such platforms to provide researchers with public access to their data on systemic risks related to the design, architecture, functioning of platforms and their algorithmic systems.[16] Now, the EU is creating a special portal for the exchange of such data, where researchers will be able to submit requests for specific platform data. Access to data will be granted only to organizations whose research is independent of commercial interests and whose findings will be made publicly available. Researchers' requests are not addressed directly to the platforms , but to national digital services coordinators (bodies authorized to implement the DSA), which review the requests and formulate technical requirements for platforms to provide access to the requested data.

The experience of Italy

In July 2025, public consultations concluded on business practices that force users to choose between agreeing to data collection through tracking technologies ("ok option") or paying for resources or services ("pay option").[17] In other words, either surrender your data or pay to use the content or platform – what is commonly referred to as the "consent wall" scheme. This scheme deprives users of freedom of choice: users should have the right to decide to pay or not, but the "pay or ok" scheme forces them to pay either with money or with data. It violates the rule of specific consent: under current regulations, users provide data for a specific purpose of processing, whereas access to content is not the purpose of data processing, but in fact a service in exchange for data. It may also be unclear to users who and why is collecting their data, how their data will be used, and when their processing will cease. If, following consultations, the practice is found to be unlawful, the government will be able to prohibit platforms from using the "pay or ok" scheme, which will restrict platforms' unlawful access to users' behavioral data.

The US and EU experience

In July 2025, the US and the EU announced the conclusion of a Trade Cooperation Agreement,[18] including the removal of barriers to digital trade. The countries agreed to maintain zero customs duties on electronic data transmissions (e.g., audiovisual content). Thus, the parties agreed not to complicate the conditions for digital trade, which is important for European companies amid the tightening of US trade policy (increased customs import duties).

Russia's experience

Unlike the EU, Russia has little tradition of upholding users' rights to information. For example, under current legislation on personal data, users have only the right to access information about the processing of their personal data, but not about activities of the data

[12] European Data/Case T-183/23.
[13] Meta's activities have been recognized as extremist and banned in the Russian Federation.
[14] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data
[15] https://digital-strategy.ec.europa.eu/en/library/delegated-act-data-access-under-digital-services-act-dsa
[16] Par. 3 Art. 40 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services
[17] https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/10126652
[18] https://www.whitehouse.gov/fact-sheets/2025/07/fact-sheet-the-united-states-and-european-union-reach-massive-trade-deal/

controller. Therefore, in Russia, users do not have the right to access information about the outcomes of audits on security measures taken by platforms (as in the EU). Given Russia's national goals for developing the data economy, it is necessary to develop practices for providing researchers with access to data from the largest platforms, including through a separate portal.

3. Platform pricing

Canadian experience

In July 2025, a document entitled "Algorithmic Pricing and Competition"[19] was discussed. Algorithmic pricing is the process of using automated algorithms to set or recommend prices for goods and services, often in real time, based on a set of input data.

The data can be obtained from consumers (online behavior, demographic information, transaction history) or may contain information about market conditions (supply and demand, competitors' prices, inventory levels). With the development of AI, it has become possible to continuously train algorithms based on data, especially if the data is constantly updated ("reinforcement learning"[20]). However, the decision-making process of such algorithms is often opaque and difficult to understand (the "black box" problem). Therefore, human oversight is important to control such algorithms.

Depending on the type of data, there are different types of algorithms:

1) Dynamic pricing algorithms – setting prices based on market conditions (demand, supply, competitors' prices, etc.). The main goal of such an algorithm is to maximize the company's profit.

2) Personalized (or controlling) pricing algorithms – setting prices based on the personal characteristics of an individual or group of individuals. The main goal is to determine consumers' willingness to pay in order to maximize profit.

This leads to price discrimination, where a company charges different prices for the same product or service depending on a customer's willingness to pay. There are several degrees of price discrimination:

1) First degree: the company sets the exact price that the consumer is willing to pay (i.e., personalized pricing).

2) Second degree – setting different prices depending on the terms of sale (e.g., price reduction for bulk purchases, subscription plans).

3) Third degree – setting different prices for different consumer groups depending on age, location, and other characteristics (e.g., price reductions for students or seniors).

Algorithmic pricing leads to anti-competitive practices:

1) Cooperation between competitors for price fixing, market division, etc. For example, companies enter into a hub-and-spoke agreement — several companies use the same algorithm (identical software) that processes data provided by competitors and sets prices simultaneously for all competitors. If there is direct interaction between competitors, this is explicit collusion; if there is no interaction, tacit collusion is possible.

2) Use of anti-competitive practices involving algorithms. For example, in predatory pricing, when a dominant company deliberately lowers its price below cost in order to drive competitors out of the market (predatory phase) and raises prices after competitors leave, compensating for the price reduction (recovery phase).

Companies use algorithms to target customers: they identify customers who are most likely to switch to another seller in order to retain customers with low prices.

French experience

In July 2025, the Shein marketplace was fined €40 million for price fraud: it advertised "crossed-out prices" (defined as "discounts").[21] However, in 57% of cases, there was no price reduction, in 19% of cases, the discount offered was less than promised, and in 11% of cases, prices were found to have increased. At the same time, the French Consumer Rights Code stipulates that when posting information about price reductions, it is necessary to indicate the minimum price at which the product was sold during the 30 days preceding the promotion. This price is the reference price from which the discount should be calculated. There is no such rule in Russia.

Russia's experience

In Russia, the use of algorithms to implement anti-competitive agreements,

[19] https://competition-bureau.canada.ca/en/how-we-foster-competition/education-and-outreach/publications/algorithmic-pricing-and-competition-discussion-paper

[20] reinforcement learning

[21] https://www.economie.gouv.fr/files/files/directions_services/dgccrf/media-document/cp-dgccrf-SHEIN-sanctionne-amende-40millions.pdf

including for pricing, particularly in the context of an explicit collusion, is recognized as an aggravating circumstance.

4. Regulating crypto assets

The EU experience

In July 2025 the European regulator ESMA issued Guidelines for providers of crypto asset services (CASP), such as crypto wallets, crypto exchanges, crypto converters, etc. The guidance is aimed at marketing practices that mislead consumers as to whether the assets traded are regulated under MiCA[22] or not.

ESMA warns that if a platform with a CASP license issued under MiCA to provide crypto asset services simultaneously offers both MiCA-regulated crypto assets (e.g., stablecoins) and unregulated (e.g., NFT[23]), this creates a risk of misleading consumers about the level of protection for each asset. The presence of a CASP license creates a "halo effect": consumers mistakenly believe that all of the platform's products are reliable and regulated. ESMA prohibits the use of the MiCA license as a marketing tool to promote products that are not covered by MiCA regulation, and also provides recommendations to CASPs:

– At every stage of interaction with the consumer – in advertising, on the website, and in the contract – it is necessary to indicate whether a specific product is subject to MiCA regulation, with non-regulated services being identified as such and information about them being provided separately.

– Before connecting a customer to an unregulated service, you must warn them about this and obtain confirmation that they have read and understood the information.

In July 2025, ESMA released a brief expert assessment report on how the Maltese regulator MFSA issued the first CASP license under MiCA.[24] ESMA notes that the MiCA licensing procedure for CASPs was too rushed: plans for onboarding new clients, the quality of CASPs' corporate governance, AML/CFT[25] procedures, and other aspects were not properly verified. Since a CASP license issued in one EU country allows the provider to offer services throughout the EU, the uniformity and quality of the licensing review process is important. Therefore, ESMA recommended that the assessment of these risks be refined in the future and emphasized the need to disclose information to clients when offering MiCA-regulated and non-MiCA-regulated services together.

The US experience

In July 2025, the United States passed the Payment Stablecoin Act (GENIUS Act).[26] The Act establishes licensing requirements for stablecoin issuers, requirements for stablecoin reserve backing (e.g., through fiat currencies) and regular reporting to the regulator on the composition of these reserves, as well as compliance with AML/KYC. The Act also prohibits charging interest to stablecoin holders and using marketing statements that create the impression of a government guarantee. The key provisions of the GENIUS Act were analyzed in the May Monitoring Report No. 5 (17), and in July, the law came into force at the federal level.

Russia's experience

In July 2025, a bill was introduced in the State Duma on fines for payments in cryptocurrency[27] from 2026 to Rb 200,000 for individuals, and up to Rb 1 mn for legal entities, and the cryptocurrency used will be confiscated. The head of the Duma committee called crypto payments a "gray area" and clarified that the bill would enshrine the ruble as the only legal tender.

Currently, Law No. 259-FZ[28] on digital financial assets prohibits the use of digital currencies as a means of payment, but does not provide for any penalties for doing so. However, since September 2024, the Bank of Russia has been granted the right to launch an experimental legal regime (ELR) under which foreign trade settlements in digital currency are permitted.[29]

It should be noted that in Russia, tokens falling under MiCA (ART/EMT[30]) may be classified as digital financial assets (DFAs) in accordance with 259-FZ.[31] Russian law, like the ESMA clarification, imposes requirements on

[22] EU Regulation No. 2023/1114 on the regulation of the crypto asset market.
[23] Non-fungible token.
[24] https://www.esma.europa.eu/sites/default/files/2025-07/ESMA42-2004696504-8164_Fast-track_peer_review_on_a_CASP_authorisation_and_supervision_in_Malta.pdf
[25] Anti-money laundering/countering the financing of terrorism.
[26] https://www.congress.gov/bill/119th-congress/senate-bill/1582?q=%7B%22search%22%3A%22GENIUS+Act%22%7D&s=9&r=1
[27] https://iz.ru/1922846/taibat-agasieva-anton-belyj/postavit-na-bit-s-2026-goda-rossiyan-nachnut-shtrafovat-za-oplatu-kriptoj
[28] https://www.consultant.ru/document/cons_doc_LAW_358753/
[29] https://www.garant.ru/hotlaw/federal/1746698
[30] Asset-backed tokens/Electronic money tokens.
[31] https://www.consultant.ru/document/cons_doc_LAW_358753/

the advertising of DFAs: the issuer and the website with the decision on the issue must be indicated, a warning about risks/possible loss of funds must be included, promises of returns and price growth forecasts must be prohibited, and advertising must be placed before the decision on the issue of DFAs is published. There are currently no regulations governing stablecoins in Russia.

5. Responsible AI governance

The UK experience

In July 2025, a report was released on practices for countering deepfakes[32] including methods for labeling content so that users can recognize and flag deepfakes: invisible watermarks[33] file origin metadata, content labels ("made with AI"), etc.

Rather than shifting the burden of recognition onto the audience, platforms should use watermarks and metadata to prioritize their moderation efforts. It is recommended to explicitly **establish** distinctions between fully and partially generated content, where AI has only edited the original content (applied filters, changed elements in the image, etc.).

The EU experience

In July 2025, the European Commission published a Code of Practice for General Purpose AI.[34] The Code provides for:

1) Transparency. The Code contains "model documentation" — a universal reporting form that companies can use to disclose information about AI: what the system does, what it was trained on, how many resources it consumes.

2) Safety and systemic risks (for models with systemic risk.[35] Responsibility may lie with company management, teams that develop and maintain AI, and auditors. Shifting responsibility to the user is not advised.

3) Protection of intellectual property rights. For example, it is recommended to implement rules for "crawling" — the automatic collection of data for training. Data in this process should only be collected on a legal basis. General-purpose AI systems should recognize prohibitions on the use of content for training.

Meta[36] has refused to join. However, OpenAI, Amazon, Google, IBM, and others (more than 25 companies) have announced their intention to join the Code.[37]

The US experience

In July 2025, the American AI Plan was released.[38] The plan outlines measures to:

1) Support startups developing open AI models[39] and models with open "weights".[40] A National AI Research Resource is being created to give startups access to computing power, models, and data without expensive contracts with private companies.

2) Combating deepfakes in the judicial system. False videos created by AI can end up in court as fake evidence and deprive people of their right to justice. Therefore, it is proposed to develop mandatory standards for the recognition of deepfakes in courts.

3) State testing of foreign models for "propaganda and bookmarks." The Ministry of Industry and Trade will check foreign AI models for censorship, the ability to secretly transfer data or control the AI system without the user's knowledge, and threats to critical infrastructure. At the moment, the US is the only country where such rules are planned to be introduced.

Russia's experience

In July 2025, the Bank of Russia published a Code of Ethics for AI in the financial market.[41]

---

[32] https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/deepfake-defences-2/deepfake-defences-2---the-attribution-toolkit.pdf?v=399908&__cf_chl_tk=_NpxVdIesx1t_BvJLNhgja0MEbGCtbbw.MA8VxcJEjk-1754490847-1.0.1.1-KvTusrBRDmHDEap6ht4r1YLweNiu9q2rVBfoKo3X5gM

[33] Programmatically detectable signals in an image/audio that indicate that the content was created using AI.

[34] General-purpose AI is an AI model that is trained not for a single function, but on very diverse data so that it learns general patterns of language/images/sound and can solve many tasks without separate reprogramming: answering questions, writing texts and code, translating, summarizing, analyzing images, etc. An important distinction: this is not a ready-made application, but a component — like a universal engine that can be run "as is" via prompts or adapted to an industry through fine-tuning.

[35] "System risk model" is a general-purpose model whose high capabilities could potentially cause large-scale harm due to its scope or predictable negative effects on health, safety, individual rights, and society as a whole.

[36] Recognized as an extremist organization in Russia.

[37] https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai

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

[39] Open models are AI models in which all key components (source code, architecture, training scripts, etc.) are publicly available. Such models can be freely used, modified, and distributed by anyone (sometimes with minimal conditions, such as crediting the authors).

[40] "Weights" are numerical parameters of an AI model that it 'learns' during training. Models with open weights are AI models where the weights can be freely downloaded and run, but not necessarily the entire "set": training data, exact recipes, part of the code, or tools may be closed.

[41] https://www.consultant.ru/document/cons_doc_LAW_509514/

The Code identifies five guiding principles: human-centricity, fairness, transparency, security, and responsible risk management. For example, customers must be given the right to refuse to communicate with a bot and request that decisions made by AI be reviewed by a human (e.g., in the event of a loan refusal). To prevent bias, AI algorithms must exclude nationality and religion from customer assessments, and their data sets must be proactively screened for these attributes. Companies will be required to indicate that recommendations made by robot advisors are generated by AI. The measures provided for in the Code should make AI more transparent and understandable to bank customers and increase public confidence in AI technology as a whole.