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

- Regulating cryptocurrencies
- Platform pricing
- Personal data regulation
- Development of openness of AI models and rights to AI generated content
- Data on competition

Monitoring No. 8 (20) (August 2025)

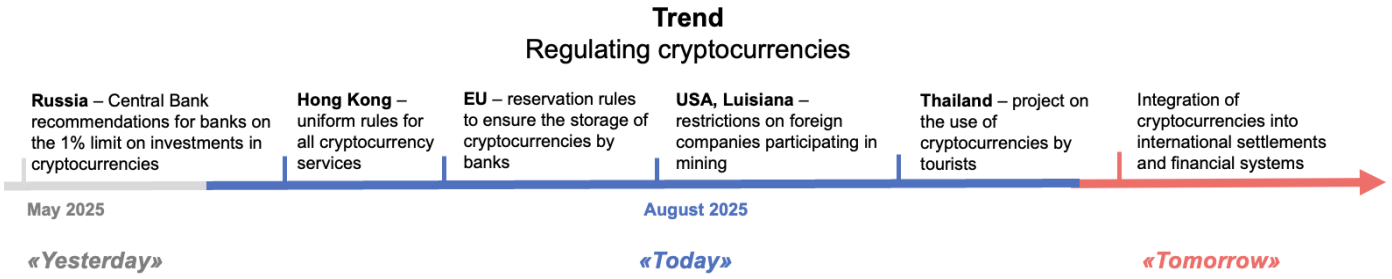
Monitoring was prepared by a team of experts of the Gaidar Institute for Economic Policy (the Gaidar Institute):
Antonina Levashenko, Senior Researcher, International Best Practices Analysis Department, Gaidar Institute.
Maria Girich, Researcher, International Best Practices Analysis Department, Gaidar 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

"Hello, August, crowned with hops,
Dark-skinned satyr youth!
We spread carpets under the oak tree,
We prepare a feast in the forest!"
Valery Bryusov

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

Trend No. 1. Regulating cryptocurrencies

Hong Kong has proposed mandatory licensing for all companies working with cryptocurrencies, the EU has established risk requirements and limits for bank investments in cryptocurrencies, Louisiana (USA) has banned foreign companies from participating in mining, and Thailand has launched a pilot project for tourists to convert cryptocurrencies into baht.

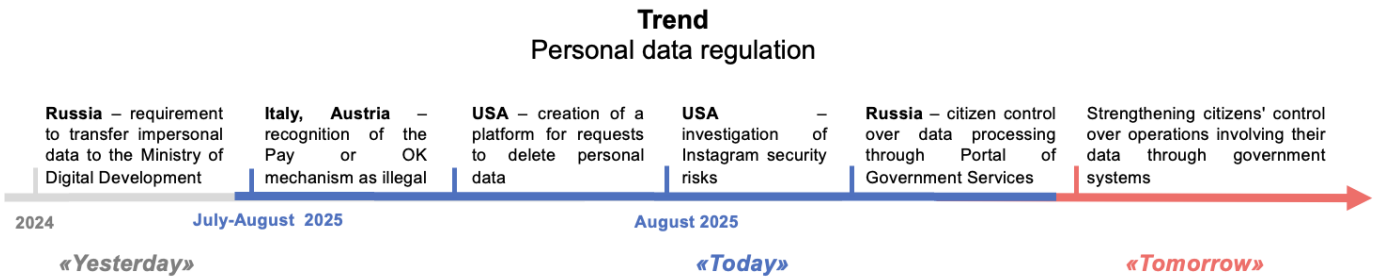


Trend No. 2. Platform pricing

China has proposed a draft regulation on platform pricing practices, including seller participation in sales, data-driven algorithmic pricing, automatic write-offs, price parity restrictions, etc.

Trend No. 3. Personal data regulation

California discussed launching a centralized platform for consumer requests to delete their data from data broker databases. In the U.S. the Attorneys General of some states launched an investigation into the legality of Instagram's new service, which allows users to publish geodata in real time.[1] In Austria, court ruled that collecting user data using the “Pay or OK” mechanism is unlawful.

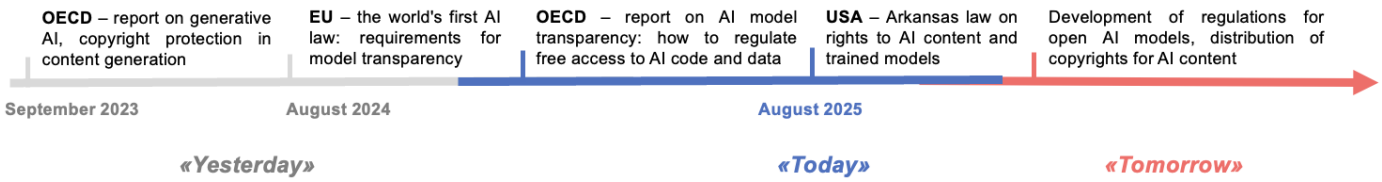


Trend No. 4. Development of openness of AI models and rights to AI generated content

In August 2025, the OECD released a report, and Arkansas (US) passed a law explaining how to regulate open AI models and who owns the rights to AI-generated content: it depends on whose data was used to train the model.

[1] Meta's activities have been recognized as extremist and banned in the Russian Federation.

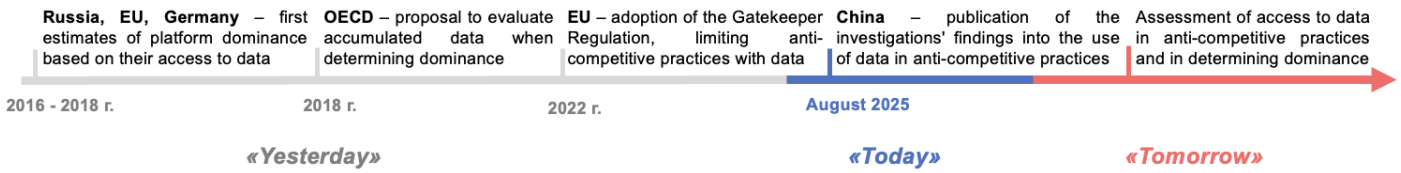
Trend
Development of openness of AI models and rights to AI generated content



Trend No. 5. Data on competition

In August 2025, the Supreme Court of China published a collection of cases on data protection issues, including the use of data in anti-competitive practices by platforms, such as restricting the transfer of data between platforms, etc.

Trend
Data on competition



In August 2025, a number of new practices were introduced in Russia.

1. Special AML/CFT requirements introduced for miners and mining pools

The Russian government[2,3] has approved AML/CFT[4] standards for miners and mining pool organizers.[5] Internal AML/CFT control rules must be developed before any operations in digital currency can begin, including its distribution after mining.

The rules cover the organization of internal control, customer identification and verification, risk management, detection of suspicious transactions and reporting them to Rosfinmonitoring, freezing (blocking) assets, staff training, annual internal audits, and storing data for at least 5 years after the end of the relationship with the customer.

2. New rules for anonymizing personal data introduced

The government has approved new requirements and methods for anonymizing personal data to enable data operators to comply with the requirement to transfer anonymized data to the Ministry of Digital Development, Communications and Mass Media GIS.[6] Operators are required to store personal and anonymized personal data separately; exclude from anonymized data information to which access is restricted by law (including non-anonymized PD); use anonymization techniques for the purpose of further transferring anonymized data to the GIS of the Ministry of Digital Development, Communications and Mass Media; and ensure the technical capability to modify anonymized data without restoring it.

There are five methods proposed for anonymization: introducing identifiers (in foreign practice, for example, in the EU GDPR, this method is known as pseudonymization); changing the composition or semantics; decomposition; mixing; transformation (including aggregation of data arrays).[7] Although this set of methods is consistent with international practice in regulating the de-identification of personal data, the list of methods is closed, which limits data operators in their choice of alternative methods.

3. Out-of-court blocking for profanity proposed

The State Duma is considering a bill on the use of extrajudicial blocking (under Article 15.1-1 of the Federal Law “On Information”[8]) for obscene language. This significantly simplifies the process of

[2] RF Government Decree of August 7, 2025 No. 1180
[3] https://www.consultant.ru/document/cons_doc_LAW_511974/9d0f569c0eb594c99074582e750e82d845f13d2d/
[4] AML/CFT -_ Anti-money laundering and countering the financing of terrorism.
[5] An association of miners who jointly mine cryptocurrency and divide proceeds proportionally to the power contributed.
[6] In accordance with amendments to the Federal Law No. 152 of August 8, 2024.
[7] Previously, the last 4 methods of depersonalization were already provided for in the methodological recommendations of Roskomnadzor from 2013.. URL: https://10.rkn.gov.ru/docs/10/Metod.rekomendacii-Ob_utverzhdenii_trebovanij_i_metodov_po_obezlichivaniju_personal6nykh_dannykh.pdf
[8] https://sozd.duma.gov.ru/bill/989488-8

users filing complaints with the Prosecutor General's Office for extrajudicial blocking of content, since any swear words can be used as grounds.

4. New measures proposed to combat cybercrime

The Ministry of Digital Development, Communications and Mass Media has presented a draft law on the obligations of telecommunications operators to combat telephone and online fraud.[9] Subscribers have the right to block calls from non-Russian numbers, and operators are obliged not to allow such calls through, inform users about the status of the call, forward recordings of conversations with signs of illegal activity to government agencies, identify suspicious numbers, and forward information about them to the GIS to combat crimes involving the use of ICT.

To distinguish between permitted and prohibited communication devices, a central database of user equipment identifiers is being created, to which operators enter data from their corporate databases. Calls from phones registered to legal entities or individual entrepreneurs are only allowed if the information is available in the database. Security agencies may prohibit the operation of specific equipment on the Russian network. The proposed measures are aimed at establishing state control over telephone communications, including virtual systems, in order to ensure the economic security of citizens, but may result in costs for operators.

[9] https://regulation.gov.ru/projects/159652

Key aspects

1. Regulating cryptocurrencies

The experience of Hong Kong

In August 2025, Hong Kong discussed a draft regulation on virtual asset trading.[10] It provides for mandatory licensing of companies engaged in transactions with virtual assets (such as cryptocurrencies) and the extension of AML/CFT requirements to them. The proposed rules expand on existing regulations, which previously only covered crypto exchanges and the issuance and circulation of stablecoins. Now, all companies that help clients buy, sell, or store cryptocurrencies will be subject to regulation, from crypto exchanges and crypto brokers to crypto wallets, consultants, and crypto asset managers.

The EU experience

The European Banking Authority (EBA) has published draft rules[11] requiring banks to account for their investments in crypto assets and determine the amount of reserves needed to cover the risk of crypto asset volatility in accordance with the EU Capital Requirements Regulation (CRR 3).[12] Banks may acquire crypto assets (e.g., cryptocurrencies, stablecoins) as part of their own investment portfolio or to serve their customers.

According to the draft, different categories of cryptocurrencies are assigned different risk weights, which determine how much capital a bank must reserve for such investments. For example, tokens backed by real assets (e.g., gold) (ARTs[13] under MiCA regulations[14]) have a 250% weighting, while unbacked cryptocurrencies (such as Bitcoin) have a maximum risk weighting of 1250%.

For comparison, the risk coefficient for gold is 100%, and for stocks it is 250%. In other words, a coefficient of 250% makes even secured tokens riskier than conventional assets, while a coefficient of 1250% for unsecured cryptocurrencies equates them to the riskiest investments, effectively prohibiting banks from holding such assets.

Thus, if, for example, a bank buys Bitcoin for €100bn, a risk weight of 1250% is applied to such an asset. This means that to calculate the risk-weighted assets,[15] the amount is multiplied by 12.5 times and amounts to €1.250 bn. However, since banks are required to hold capital equal to at least 8% of their risk-weighted assets, in this case, the bank would be required to reserve €100 m of its own capital. In other words, for every €1 invested in Bitcoin, the bank must hold another €1 in capital.

Quantitative restrictions are also being introduced: the total volume of unsecured crypto assets on a bank's balance sheet must not exceed 1% of its Tier 1 capital.[16] These measures are effectively aimed at limiting the large-scale accumulation of volatile cryptocurrencies by banks.

The US (Louisiana) experience

The Blockchain Basics Act[17] has come into force in Louisiana, prohibiting certain foreign companies from acquiring or owning cryptocurrency mining businesses in the state, namely citizens and organizations from countries under US sanctions[18][19] (e.g., Russia, Iran), as well as companies that the US State Department has identified as entities of particular concern. Such companies are prohibited from engaging in mining, otherwise they will face a fine of up to $1 m or up to 25% of the value of the share owned by the violating company in this business.

The law also prohibits Louisiana authorities from accepting payments in central bank digital currencies and participating in their testing. However, in Louisiana, it is possible to participate in maintaining the blockchain — to maintain computers that help the network operate, as well as to engage in mining at home.

[10] https://www.fstb.gov.hk/fsb/en/publication/consult/doc/VADEALING_consultation_paper_en.pdf
[11] https://www.eba.europa.eu/sites/default/files/2025-08/616d6b06-cdcf-4246-a7cc-2173dfd32fa6/Draft%20RTS%20on%20crypto%20asset%20exposures%20Article%20501d-5.pdf
[12] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401623
[13] Asset Referenced Tokens
[14] Markets in Crypto-Assets Regulation — European regulation establishing rules for the regulation of crypto assets and related services, adopted in 2023
[15] Risk-Weighted Assets (RWA)
[16] Tier 1 capital - the bank's core capital, including share capital, retained earnings, and other reserves used to cover losses and ensure the bank's stability.
[17] https://www.legis.la.gov/legis/BillInfo.aspx?s=24rs&b=HB488&sbi=y
[18] https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=24d528fddbfc930044f9ff621f961987
[19] US International Arms Trade Regulations

The experience of Thailand

In August 2025, the Thai Securities and Exchange Commission proposed a regulatory sandbox concept for cryptocurrencies[20] to enable foreign tourists to exchange cryptocurrencies for Thai baht to pay for purchases in the country. The TouristDigiPay pilot project was launched,[21] allowing tourists to convert cryptocurrencies into baht through licensed cryptocurrency platforms and wallets. After the exchange, the funds are credited to a special tourist e-wallet, from which goods and services can be paid for using QR codes at local merchants. The project is scheduled to run for 18 months and is intended only for foreign tourists temporarily residing in Thailand. At the same time, limits have been set on transactions, for example, no more than 50,000 baht ($1,500) per month for small purchases. The project is particularly relevant for Russian tourists, who face restrictions when paying with bank cards abroad.

The experience of Russia

Russia has already adopted measures similar to the EU's approach, providing for a quantitative limit of 1% of capital for cryptocurrencies: in May 2025 the Bank of Russia published Information Letter recommending that credit institutions independently assess the risks of transactions with digital currencies, ensure full coverage of such investments with their own funds (capital), and set a limit of no more than 1% of their own funds.

Also, unlike Hong Kong and Thailand, where attention is focused on regulating service providers and creating “sandboxes” to stimulate tourism, there are no such initiatives in Russia yet. However, there is a law on mining: only companies and individual entrepreneurs registered in the Federal Tax Service registry can engage in it. This approach is comparable to measures in the US, where the participation of foreign companies in the mining business is restricted.

2. Platform pricing

The experience of China

China has published draft pricing rules for e-commerce platforms and sellers.[22]

Platforms are prohibited from: raising fees, imposing penalties, canceling price subsidies or discounts for sellers, restricting traffic, blocking sellers, reducing the visibility of their products, or imposing other restrictions for the purpose of:

1) Forcing sellers to participate in sales or discounts.

2) Restrict the seller's ability to offer optimal prices for goods and services on different platforms (restricting the practice of price parity).

3) Connect a system of automatic price matching, automatic price reduction, etc.

4) Otherwise restrict the sellers' right to set prices.

The exception is platforms with uniform pricing methods, such as taxi platforms.

If a platform changes its commission, it must take into account the financial situation of sellers in order to set reasonable rates; unreasonable payments are prohibited. If rates change, public discussions must be held (for at least 7 days), and if sellers are not satisfied with the new rates, the platform must allow them to terminate the contract without consequences.

If different prices are applied to different categories of consumers depending on the terms of the transaction, the pricing rules must be disclosed publicly in advance. It is also necessary to disclose the rules for time-differentiated pricing (dynamic pricing) with an explanation of the factors affecting price formation.

When conducting promotions and sales, it is necessary to publish the rules of the promotion and its duration in a place visible to consumers, and to indicate the base price from which the discount is calculated. If the platform subsidizes sellers' prices, information about the rules and terms of the subsidy must be disclosed. If goods or services are promoted through paid ranking (e.g., a seller pays to increase visibility), it must be clearly indicated that this is “advertising.”

Anti-competitive practices are prohibited:

1) Selling goods or services at a price below cost in order to drive out competitors or monopolize the market (predatory pricing).

2) Setting different prices for the same goods or services under equal conditions of

[20] https://www.sec.or.th/EN/Pages/News_Detail.aspx?SECID=11899&NewsNo=173&NewsYear=2025&Lang=EN

[21] https://www.nationthailand.com/business/digital-assets/40054107

[22] https://www.samr.gov.cn/hd/zjdc/art/2025/art_65b6620cb5114ea49c72494b084d3e42.html

sale, based on the consumer's willingness to pay or preferences, using data and algorithms without the consumer's knowledge. This limits discrimination in algorithmic pricing.

3) Use expressions that fuel expectations of price increases, such as false information about product shortages, high demand, etc.

4) Attract consumers or sellers with low prices and then charge high prices, promise false discounts, fail to indicate or deliberately understate price conditions, mislead, etc.

Platforms and sellers are required to provide consumers with the option to cancel automatic debits, including contactless (password-free) payments, insurance and other additional services, automatic subscription renewals, etc.

The experience of Russia

In Russia, the Platform Economy Law does not regulate platform pricing, but a platform has the right to offer a discount on a seller's goods only after receiving the seller's written consent specifying the price, quantity of goods discounted, and the duration of the discount. Without the seller's consent, the platform can only offer discounts at its own expense.

3. Personal data regulation

The US experience

The California Privacy Protection Agency held consultations on the implementation of the unified "DROP" portal (under the 2023 Deletion Act[23]). Previously, California consumers could only opt out of the sale of their data to third parties at the time their data was collected by companies. At present, a centralized state platform is created to enable consumers to find data brokers to whom companies have already transferred their data and request that they delete their data.[24] At the DROP a data broker must process requests for data deletion at least every 45 days. After processing the request, a data broker notifies the requesting consumer whether the user's data is found in the broker's database and deleted. At the same time, it is prohibited to use the DROP portal to contact consumers beyond the data deletion procedure.

In the US, Attorneys General from 37 states sent a letter to Meta[25] regarding the introduction of a new location sharing feature on Instagram[26]. By displaying the exact location of users in real time on a map the feature is expected to increase the risk of stalking and harassment, especially for minors. The companies are advised to restrict the use of this feature for minors, introduce warnings for adults about the risks of sharing their location, and ensure that users can opt out of using the feature.

The experience of Austria

In August 2025, the Federal Administrative Court of Austria [27] found that Austrian media group Der Standard had violated the EU General Data Protection Regulation (GDPR) requirements regarding the collection of consent through a "Pay or OK" mechanism.[28] This practice of charging for access to content was discussed in the previous issue of Monitoring.[29]

Earlier, following a complaint from the human rights organization Noyb, the Data Protection Authority, found that the news publication Der Standard forced users to either agree to all data processing purposes, including automated data analysis, targeted advertising, and access to social networks, or pay for a subscription to the publication in order to access the platform's content. In the proceedings, Der Standard argued that it had the right to collect user data, citing the exception for media freedom (Article 85(2) of the GDPR).[30] However, the Court pointed out that blanket consent mechanisms violate the GDPR (the principle of clear consent (Article 5), the condition of lawfulness of processing based on consent (Article 6)), as users must be able to choose the specific purposes for which they give their consent. Clicking an "OK" button is not voluntary, as it does not allow the user to choose a purpose of data processing and, therefore,

[23] https://digitalpolicyalert.org/change/13671-california-privacy-protection-agency-rules-on-data-broker-registration-and-accessible-deletion-mechanism

[24] https://www.skadden.com/insights/publications/2023/12/californias-new-data-deletion-law-imposes

[25] Meta's activities have been recognized as extremist and banned in the Russian Federation https://digitalpolicyalert.org/event/32796-attorneys-general-of-37-states-announced-investigation-into-instagram-over-location-sharing-feature

[26] https://illinoisattorneygeneral.gov/News-Room/Current-News/Protect%20Instagram%20User%20Privacy%20Multistate%20AG%20Letter.pdf?language_id=1

[27] https://digitalpolicyalert.org/event/32858-federal-administrative-court-issued-ruling-against-publishers-of-derstandardat-over-pay-or-consent-mechanism-violations

[28] https://noyb.eu/sites/default/files/2025-08/20250818145608738p_Redacted.pdf

[29] See Monitoring No.7 (19) (July 2025).

[30] According to Article 85(2) of the GDPR, EU Member States must provide for exemptions from data protection requirements for journalistic activities in their national legislation.

such consent is invalid. The GDPR exemption for journalism does not apply in this case, as the data is processed for targeted advertising, which cannot be considered journalistic activity. The court ordered the processing of previously collected data to be stopped and the data to be deleted.

The question arose as to what data Der Standard should delete. The court confirmed that all behavioral user data, including so-called "transparency and consent strings" – records of user choices when giving consent (e.g., cookie settings) – must be deleted. The court considers such data as personal because, in combination with Internet Protocol addresses, TC strings make users identification possible.

The experience of Russia

In August, the Ministry of Digital Development, Communications and Mass Media presented draft requirements for the collection and processing of personal data by data operators.[31] The purpose of the amendments is to expand the control of data subjects over their collected data by providing the ability to track who and how processes their data by means of the "Gosuslugi" government services portal.

Data subjects are enabled to give their consent to data processing using a standard form developed by Roskomnadzor and to manage their consent through the Gosuslugi portal (for example, receive information about data processing or submit complaints to Roskomnadzor against actions of data operators). This obliges data operators to transfer the information requested by the data subject to the Gosuslugi system. As a result, the proposed regulations establish a centralized mechanism for public control over the relationship between individuals and companies in regard of personal data processing.

4. Development of openness of AI models and rights to AI generated content

The OECD experience

In August 2025, the OECD presented a report on "AI openness", describing how countries can implement frameworks for freely distributed components of AI models. The OECD recommends that regulators define the concept of "open-source AI" or "AI source code"[32] in AI regulation by introducing levels of openness for AI systems into legislation.[33] The OECD notes that the term "open-source AI" does not accurately describe which components of AI are open: model weights,[34] code, or data. For example, disclosing only the weights can be labeled "open source," but in fact provides little practical value without the underlying source code. Disclosing these components is a key tool for transparency enabling third parties to verify a model's quality and risks, identify errors and biases, and better explain its outputs. The OECD suggests describing levels of openness based on the accessibility of components: "open model" (weights and basic description), "open tools" (training and evaluation codes, key datasets are added), "open science" (the entire development cycle and materials are disclosed).

It is important to introduce "open licenses" into regulation, allowing the free use of intellectual property (including AI systems). Licenses vary in purpose. For example, permissive licenses allow the use of open AI elements when the developer is specified. These accelerate development and implementation by enabling free experimentation and the sale of solutions, provided the license terms are met. However, due to the risk of abuse, they need to be supplemented with checks for malware distribution, copyright infringement, or illegal data use. Another type is copyleft licenses, which require that any product using open-source AI elements must be distributed under the same conditions.

In introducing such licenses, the OECD emphasizes that regulators must ensure the legality and security of published AI components and data. Requirements for descriptions are recommended: what elements are published and what data sources are used. Components must be tested for security and compliance with their declared properties.

[31] https://regulation.gov.ru/projects/159652

[32] There is no commonly accepted definition of "open-source AI," but it is generally understood to refer to AI models whose key components are publicly available and freely usable: source code (how the model is trained and how it works), trained "weights," and data information.

[33] https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/08/ai-openness_958d292b/02f73362-en.pdf

[34] "Weights" are numerical parameters of an AI model that it 'learns' during training. Open-weight models are AI models where weights can be freely downloaded and run, but not necessarily the entire rest of the "set": training data, part of the code, or tools may be closed.

The US experience

In August 2025, a law on AI content rights[35] came into force in the state of Arkansas. By default, if a person gives instructions to a generative AI system, supplies data, and receives content (text, images, code, etc.), they hold the rights to the output. If they provide data for training, they become the owner of the version trained on that data, provided the data was obtained legally and the rights must not be transferred to the developer/provider by contract. In the case of employees, if working with AI is part of their job responsibilities, the rights to the content belong to the employer.

The law specifies that it is not possible to appropriate anything that infringes on the copyright or other rights of others. If someone else's copyrighted material or personal data is used when requesting or transferring data, the person does not acquire intellectual property rights to the generated content. The question of who owns a model trained on data from many individuals remains open: the law does not resolve this issue.

The law clarifies rights concerning generated content, the user's prompt, the provided data, and the model trained on that data. If a company legally provides data for training, it obtains ownership rights to the trained model. The law reduces the risk of conflicts in joint projects: the parties can establish a different ownership order in advance—the terms of the contract apply. For example, when retraining a supplier's model on customer data, rights can be divided: the “weights” and their updates remain with the supplier, and the customer receives a license for internal use.

The user owns the copyright to the content if the data used belongs to them on a legal basis. This resolves the issue of rights to AI content in the event of copyright infringement by the user. IP rights to such content do not arise, and fragments (e.g., text or code) similar to someone else's IP object will belong to the copyright holder in the event of a proven infringement.

The experience of Russia

Russia has introduced certain measures to stimulate the development of open-source AI. For example, expenses incurred in developing open-source platforms for “smart assistants” can be counted twice toward reducing corporate income tax. However, Russia has not adopted regulations that take into account the specifics of open AI licensing. When developing such regulations, it is worth paying attention to the OECD's recommendations on the requirements for descriptions of AI components distributed under open licenses, as well as on indicating data sources and ensuring that such components can be verified for security.

Russia also lacks specific regulations on intellectual property rights for AI-generated content and AI models trained on data belonging to third parties. Discussion of these issues in the State Duma is scheduled for fall 2025.[36] During the discussion, attention should be paid to the following questions: whose data was used to train the AI model that generated the content; does the user who formed the request for the AI to generate content provide their own data?

5. Data on competition

The experience of China

The Supreme People's Court presented a selection of competition cases related to the use of data.[37] In one case, Company A (the defendant) copied more than 50,000 videos from Company B's (the plaintiff) application, which contained Company B's application code, user nicknames, and avatars. Company A actually used the data posted on platform B and transferred it to its own platform for public distribution. Company A referred to the fact that Company B did not have intellectual property rights to user content, so such a transfer did not violate Company B's rights.

The court ruled that Company B had aggregated data posted by users who uploaded their videos based on the platform's user agreement and through its technical support. Therefore, the data uploaded by users has high commercial value. In addition, Company B invested significant resources (human and financial) in the formation and accumulation of data and attracted user traffic, which gave the data set additional economic value. Therefore, Company B's commercial interest in owning and commercially exploiting the data set is subject to legal protection even if Company B does not own

[35] https://arkleg.state.ar.us/Bills/Detail?id=HB1876&ddBienniumSession=2025/2025R

[36] https://iz.ru/1944845/2025-08-29/v-gosdume-khotiat-zakrepit-avtorskoe-pravo-na-proizvedeniia-s-ii

[37] https://eastlawlibrary.court.gov.cn/court-digital-library-search/page/portal/newsDetail.html?id=44aad9946d2b414a9ee1b59b965192e6&utm

the IP rights to such data. The court found a violation of competition, since the transfer of data from platform B to platform A led to the content offered to users being identical, i.e., company A attempted to “replace” the services of company B's platform, thereby violating its economic interest.

In another case, Company A (the plaintiff) operated a website for job seekers, including providing employers with the ability to search for employees by resume, download and forward resumes, etc. At the same time, Company B (the defendant) provided resume processing and recruitment management services for employers, etc. On Company B's website, it was possible to link external accounts, such as accounts on Company A's website or other websites, so that employers could centrally process resumes from all websites. To do this, the employer had to log in with their username and password from their account on Company A's website (or other websites), after which the systems automatically synchronized, and resumes from Company A's website were sent to the employer's personal account on Company B's website for further processing. However, by linking the accounts of the two platforms, resumes from company A's website were transferred to company B's information systems. As a result, a lawsuit was filed against company B for unfair competition, alleging that by linking accounts, company B used employers' logins and passwords, bypassed company A's data protection mechanisms (e.g., captchas) and automatically obtained, stored, and used the resumes collected by Company A.

However, the court found that there was no act of unfair competition, recognizing such behavior as a matter of the employer's right to transfer the data it had collected (including resumes) from one platform to another. In addition, the transferred resumes were stored exclusively in the employers' accounts and did not enter Company B's general resume database.

The experience of Russia

In Russia, the use of data in anti-competitive practices is currently not regulated.[38] However, the Federal Antimonopoly Service (FAS) takes into account the issue of access to data from large platforms, for example, when determining a dominant position. For example, the FAS assessed this factor in its 2019 investigation against HeadHunter,[39] where the company created a difficult barrier to entry for other platforms that need to ensure a large base of job seekers and employers.

[38] For example, within the framework of the Principles of Interaction between Participants in Digital Markets 2022

[39] https://br.fas.gov.ru/ca/upravlenie-regulirovaniya-svyazi-i-informatsionnyh-tehnologiy/8e4961ce-3f9c-4b37-9f4b-b2804deeec88/