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

Restricting DeepSeek operations, obligating platforms to pay tips, restricting the sale of personal data, protecting intellectual property rights in AI training, anti-competitive practices online

Monitoring No. 2 (14) (February 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

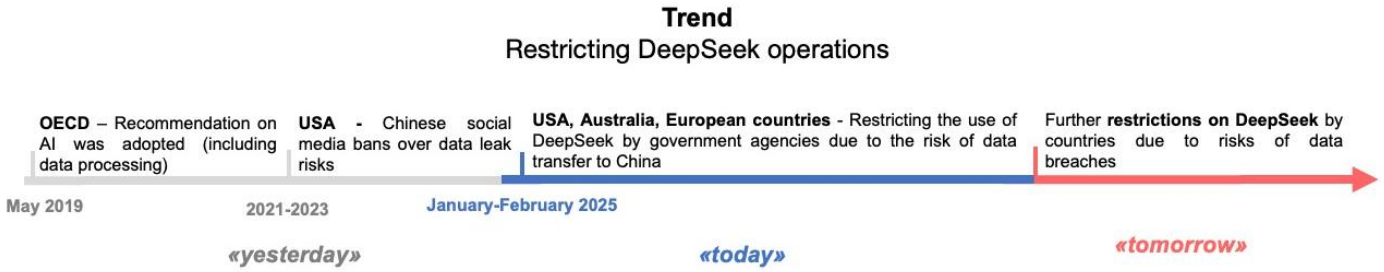
The reference to this publication is mandatory if you intend to use this material in whole or in part.

“Black spring! Pick up your pen, and weeping,
Of February, in sobs and ink,
Write poems, while the slush in thunder
Is burning in the black of spring.”.
Boris Pasternak

In February 2025, there were 5 events that define the trends in the development of digital regulation in the world.

Trend No. 1. Restricting DeepSeek operations

In February 2025, a number of countries (EU, USA, Australia) introduced measures to restrict or prohibit the use of DeepSeek (China). This is a chatbot like OpenAI ChatGPT. The main reasons for the ban are threats to digital security and abuse of personal and other data.



Trend No. 2. Obligating platforms to pay tips

In February 2025, Amazon and DoorDash were fined in the US for failing to tip their delivery drivers.

Trend No. 3. Restricting the sale of personal data

In February 2025, the state of Vermont (USA) introduced a bill that mandates large companies selling personal data to provide individuals with tools to control the sale of their data. A trend is forming in the US to restrict unregulated commercial circulation of personal data at the state level.

Trend No. 4. Protecting intellectual property rights in AI training

In February 2025, the UK proposed allowing “default” use of data for AI training as long as there is no explicit prohibition from the rights holder.

Trend No. 5. Anti-competitive practices online

In February 2025, investigations ongoing against Apple in the UK for abuses in the mobile browsing and cloud gaming market, and in Germany for manipulating data collection consent forms for advertising purposes.

February 2025 also saw a significant event in Russia's digital economy regulation - **new accreditation rules for IT companies** were proposed.

The Ministry of Digital Technology, Communications and Mass Media proposed to change the accreditation procedure for IT companies required to receive state support (e.g., reduced tax rates (5% instead of 25%) and insurance premiums (7.6% instead of 30%), etc.):[1]

1. Accreditation will be banned for companies with 50% or more share of foreign capital. Such a ban may reduce the inflow of foreign investment.

2. Companies with state participation of 50% or more will be able to obtain accreditation if 70% of the company's revenues comes from information security activities. Telecom operators will also be able to be accredited if their IT revenues exceed 50% of total revenues. This measure may contribute not to the development of the IT sector, but rather to additional legal tax optimization of certain large companies, including private companies with state participation.

3. The list of accredited organizations will include companies in the field of quantum communications and testing, attestation and certification in the field of information protection. The inclusion of quantum technologies is particularly relevant, as Russia is actively developing in this area. For example, in September 2024, Russia created a 50-qubit ionic quantum computer.[2] At the end of 2024, only 6 countries, including Russia, had such quantum computers.

4. To maintain accreditation, large IT companies (revenue of Rb1 bn or more, 100 employees or more) will be obliged to cooperate with universities in the field of IT education. This measure can help improve the quality of personnel training but will increase the administrative burden on IT companies.

5. Small IT companies (up to Rb1 mn in revenue, on the market for less than 3 years) will be exempt from inspections and confirmation of accreditation until the end of 2025. From 2026, such a privilege will be retained only for startups. As a consequence, after 2025, small IT companies without startup status may encounter difficulties in confirming accreditation and lose their benefits.

The proposed changes adjust the current accreditation rules for IT companies, expanding their scope and introducing additional requirements for companies' contribution to the social functions of business and government.

[1] https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=154642#
[2] https://nauka.tass.ru/nauka/21937207

Key aspects

1. Restricting DeepSeek operations

In February 2025, regulators in Europe, the US, and Australia[3] imposed restrictions on the use of chatbot DeepSeek, as it is unclear how the company stores and processes user data. DeepSeek also transfers foreign user data to China, which raises questions about the legality of its transfer between jurisdictions.

The OECD, in its 2019 AI Recommendations, points to the need for transparency in the collection and processing of data by AI systems. China has not joined these Recommendations. The DeepSeek case demonstrates the trend toward stricter controls over foreign digital services that handle foreigners' personal data.

The US experience

In January-February 2025, a number of US states (New York,[4] Texas,[5] Virginia, Kansas, etc.) issued bans on DeepSeek for government employees' devices and networks, as the application can transmit user data to the Chinese government. Interestingly, in 2022-2024, Texas and Virginia already imposed similar bans on TikTok, WeChat, Rednote, and Lemon8.[6]

A special bill has been proposed in Kansas to ban the use of “dangerous” AI platforms on state-issued devices and networks.[7] State employees will not be able to install or access such platforms on their issued devices, and state networks must block their use. All state agencies are required to delete existing accounts and stop working with such AI. The only exception is for law enforcement and cybersecurity investigations. “Dangerous” AI is defined as DeepSeek and any models controlled by China, Russia, Iran, DPRK, Cuba, and Venezuela.

The experience of European countries

In January-February 2025, a number of European countries banned the use of DeepSeek on government-owned devices (Italy[8]) or issued recommendations for citizens not to use DeepSeek (Poland,[9] Netherlands,[10] and Liechtenstein). Germany has launched an investigation into DeepSeek's violation of the EU General Data Protection Regulation (GDPR). The regulators have the following concerns about DeepSeek:

1. Lack of description of the purposes of user data collection, measures to ensure privacy and security of data storage (Art. 12 GDPR and Art. 50 of the EU AI Act).

2. Risk of illegal transfer of user data from the EU to China (violation of Articles 45 to 50 GDPR).[11] DeepSeek collects and stores data (IP addresses, chat history, files, keystroke patterns) on servers in China, which does not have a data protection agreement with the EU.

3. The absence of an official DeepSeek representative in the EU (Article 27 GDPR). This requirement applies to all companies collecting personal data in the EU and providing goods or services.

Russia’s experience

Russia has no special requirements for the storage of data processed by AI systems. On the one hand, China is on the list of states that provide adequate protection of the rights of personal data users.[12] That is, personal data of users from Russia can be transferred to China, provided that Roskomnadzor is notified of this.

On the other hand, DeepSeek is still obligated to comply with data protection requirements, such as localization (storage) of Russian users' data on Russian servers.

---

[3] https://www.protectivesecurity.gov.au/system/files/2025-02/PSPF-Direction-001-2025.pdf

[4] https://www.governor.ny.gov/news/governor-hochul-issues-statewide-ban-deepseek-artificial-intelligence-government-devices-and

[5] https://gov.texas.gov/news/post/governor-abbott-announces-ban-on-chinese-ai-social-media-apps

[6] For example, the risk of said applications transferring personal data at the request of the Chinese government poses a security risk under Section 620.002(1) of the Texas Government Code https://www.governor.virginia.gov/media/governorvirginiagov/executive-actions/Governor-Glenn-Youngkin-Bans-DeepSeek-AI.pdf

[7] https://www.kslegislature.gov/li/b2025_26/measures/documents/hb2313_00_0000.pdf

[8] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10098477#english

[9] https://uodo.gov.pl/pl/138/3550

[10] https://www.autoriteitpersoonsgegevens.nl/actueel/ap-pas-op-met-gebruik-chatbot-deepseek

[11] Articles 45-50 GDPR regulate the cross-border transfer of personal data outside the EU. The transfer is possible if the European Commission decides on the adequacy of protection measures, using standard contractual clauses, corporate rules or special authorizations.

[12] Roskomnadzor Order of 05.08.2022 No. 128.

2. Obligating platforms to pay tips

The US experience

In February 2025, US delivery services Amazon[13] and DoorDash[14] must pay fines for failing to tip their delivery drivers.

Back in 2019, the Federal Trade Commission (FTC) began investigating Amazon over drivers' complaints about pay wages. The Amazon Flex delivery service promised drivers earnings of $18 to $25 per hour, as well as a full tip credit. As of 2016. Amazon decided to reduce driver labor costs and lowered pay below what was promised. The rate was generated by an algorithm based on the amount of tips so that tips would cover the promised minimum hourly rate. Amazon provided drivers' total earnings information - a single amount with no separation between the minimum wage rate and tips.

That is, Amazon promised to pay 100% of the tips that customers left for delivery drivers, but in fact about one-third of the tips went to reduce Amazon's labor costs - to subsidize the drivers' hourly wage rates. In other words, these payments were not additional wages for the drivers. The FTC ordered Amazon to refund the drivers $61 mn.[15] Amazon will now pay another $3.95 mn to the District of Columbia for deceiving consumers who thought their tips were being used as additional earnings for the driver.

A similar scheme was used by DoorDash delivery, which introduced a “guaranteed payment” scheme by using tips intended for Dashers to subsidize their guaranteed pay. Before a courier accepted a delivery order, DoorDash specified a minimum amount of earnings. So, if the delivery was $10 and the customer left a $2 tip, the driver still received $10 ($8 was the hourly rate from DoorDash). And even if the customer left a $9 tip, DoorDash would then only pay $1, bringing the payment to the minimum rate of $10. As a result, in February, DoorDash signed an agreement with New York City to reimburse $16.75 mn in tips to 63,000 drivers for handling more than 11 mn orders.

Russia’s experience

There is no regulation in Russia on the distribution of tips, including on platforms. If hiring is carried out under an employment contract, in accordance with a Letter from the Ministry of Finance,[16] tips (for waiters) are considered income in the form of a gift and are not subject to personal income tax if transferred by an individual directly to a waiter.

And if tips are transferred to an organization, such income is no longer considered to be a gift. At the same time, the Ministry of Finance emphasizes that in this case, an employer may deduct remuneration (commission) for accepting tips under an agency contract. If the above approach is applied to platforms, then, for example, taxi companies operating through platforms are entitled to charge a commission for payment from drivers' tips.

If a person works on a platform under a civil law contract, platforms may charge a commission on tips, acting as agents or commissioners.

Meanwhile, the experience of foreign countries (EU, USA, France) establishes special obligations for platforms to pay tips and inform about their exact amount.

3. Restricting the sale of personal data

The US experience

In February 2025, the state of Vermont introduced a bill relating to consumer data privacy and online surveillance.[17] Since the US is now the only jurisdiction where the sale of personal data is regulated at the state level, the bill provides users with special rights when their data is sold by companies of two categories: companies that processed data from of not fewer than 25,000 consumers and companies that processed data of not fewer than 12,500 consumers and derived 25% of gross revenue from the sale of personal data.

Companies must provide the user with the opportunity to opt-out of the sale to third parties or used in targeted advertising or digital profiling. Companies must provide, upon request, a list of third parties to whom data has

[13] https://oag.dc.gov/release/ag-schwalb-secures-395-million-amazon-resolve
[14] https://ag.ny.gov/press-release/2025/attorney-general-james-secures-1675-million-doordash-cheating-delivery-workers
[15] https://www.ftc.gov/system/files/documents/cases/1923123c4746amazonflexorder1.pdf

[16] Letter of the Ministry of Finance of Russia from 04.09.2019 No. 03-04-05/67992 “On personal income tax and insurance contributions on amounts of tips transferred (paid) by customers directly to waiters or to the settlement account of the organization (restaurant, cafe)”.
[17] https://legiscan.com/VT/text/H0208/id/3116104

been shared. The practice of selling personal data is recognized as a high risk to data subjects, so companies are required to conduct a data protection assessment and disclose the results of such internal audits upon request of the state attorney general.

The bill fits in the trend of restricting the sale of personal data, set in 2018 when the state of California adopted requirements for companies to provide users with the right to opt-out of the sale of their data to third parties. Today, many states are passing personal data laws that tighten the terms and conditions under which personal data is sold, such as Virginia (Consumer Data Protection Act of 2021), Utah (Consumer Privacy Protection Act of 2022), and Colorado (Privacy Act of 2023). The requirements effectively restrict large companies from selling data against the will of the user, preventing such companies from monopolizing the market by accumulating large amounts of data.

Russia's experience

Russian legal practice does not use the concept of "sale of personal data", but this does not exclude the problem of gray schemes for trading in Russians' data. For example, in 2020, 9.2 mn records on bank customers were offered for sale in the banking sector.[18] The main source of data for sale is leaks resulting from cyber attacks: in 2023, 170.3 mn records leaked from the banking sector.[19] Thus, there is a shadow market of personal data trading in Russia, the main beneficiaries of which are fraudsters.[20]

However, user data is also of interest for legitimate business, for example, for use in marketing purposes. Therefore, working out legitimate grounds for transferring personal data between companies on a commercial basis is relevant in Russia. It is noteworthy that the national development goals of Russia until 2030 set the task of forming a data market, which could potentially include personal data.[21]

4. Protection of intellectual property rights in AI training

In 2025, the search for optimal regulation of intellectual property rights (hereinafter - IPR) in AI training continues, ensuring a balance between the protection of rights holders and the needs of developers. In Monitoring No. 5 of 2024, we have already considered approaches to addressing this issue in China, the EU, France, Italy, and the USA.

The US experience

In February 2025, a court decision was issued in the case of Thomson Reuters and West Publishing v. Ross Intelligence for copyright infringement of the legal annotations and classification system for law enforcement decisions (judicial, administrative, etc.) of the Westlaw platform.[22] Ross created an AI-based legal research tool by illegally using plaintiffs' materials to train its system.

The court found that Ross directly copied data from Westlaw in violation of the Copyright Act,[23] finding that Thomson Reuters owned the copyright not only in the texts, but also in their selection and organization. The court rejected Ross's fair use of content[24] argument because the AI was used for commercial purposes and recycled the data in whole, not in part.[25] Ross created a competing product based on illegally obtained content owned by Thomson Reuters and generated its own data from it in the same market.

The court also confirmed that Westlaw's AI-generated annotations had sufficient originality to be protected by copyright. That is, the owner of the AI system (Thomson Reuters) is recognized as the copyright holder of the generated content. Thus, the use of data in AI without the permission of the copyright holders violates the law, even with reference to fair use.

Also in February 2025, California published a bill to enhance transparency in the use of data for AI training. It is proposed to require generative AI developers to document the use of copyrighted materials in AI training,

[18] https://garda.ai/blog/news/analiz-tenevogo-rynka-baz-dannykh-bankov-za-2020-god

[19] https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A3%D1%82%D0%B5%D1%87%D0%BA%D0%B8_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85_%D0%B8%D0%B7_%D0%B1%D0%B0%D0%BD%D0%BA%D0%BE%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8

[20] https://garda.ai/blog/news/analiz-tenevogo-rynka-baz-dannykh-bankov-za-2020-god

[21] http://www.kremlin.ru/acts/news/73986

[22] https://www.lawnext.com/wp-content/uploads/2025/02/2025-02-11-Memorandum-dckt-770_0.pdf

[23] 17 United States Code Art. 410(c).

[24] Permissible use of intellectual property rights of others without explicit consent for scientific, educational, cultural and other similar non-commercial purposes.

[25] 17 United States Code Art. 107.

identify copyright owners, and keep data on the facts of such data use and its owners during the commercial use of the AI model, and 10 years after. Developers must provide a list of the materials used within 7 days upon the request of the copyright holder.[26]

The UK experience

In February 2025, public hearings were held on plans to protect IP rights in the use of AI.[27] The UK is considering four approaches to IP regulation in the context of AI training: (1) no specific regulation; (2) compulsory licensing; (3) the right for anyone to use the data for AI training; or (4) the same right, but with the right holder's option to prohibit use, and the developer's obligation to ensure transparency and accountability for the use of the data.

The UK has chosen the 4th approach - accordingly, it is planned to introduce a model where authors will be able to prohibit the use of their works in advance, and in the absence of such a ban their content can be freely used. This will allow copyright holders to earn money on licensing, and developers - to work with large amounts of data. AI developers should disclose what data their models are trained on (similar to the norms of the EU AI Act).

Existing copyright protection, such as robot bans,[28] is insufficient. They can block access to publicly accessible sites on the Internet, but do not protect individual works. Therefore, the UK is exploring ways to strengthen control over data through metadata with a ban on content collection,[29] development of standards for recording access rights, copying, etc., and centralized registries of restrictions. It is proposed to transfer rights to collective management organizations for licensing and payment distribution.

Russia's experience

Russia lacks legal regulation of IP rights protection in AI training. It was planned to approve an updated Concept of AI regulation in February 2025, but there is no information about such approval. The draft Concept sets the task of working out the issues of protection of AI rights to works created with the use of AI, labeling of such works for transparency of their origin. It is proposed that a person or organization that controls the system and makes decisions on its use should be responsible for the results of AI work.[30] In other words, there is no special regulation in Russia now, however if the plans described above from the draft Concept are implemented, the Russian approach will include granting authorizations "by default" and with information disclosure requirements, as it is accepted in the EU and planned in the UK.

5. Anti-competitive practices online

In February 2025, the investigation into Google and Apple's abuses in the mobile browsing and cloud gaming market continued.[31] The Competition and Markets Authority (CMA) uncovered abuses:

1. Apple requires mobile browsers on iOS devices to use Apple's browser engine, WebKit. WebKit does not provide the same browser extension functionality competing browsers that Apple's Safari browser does. For example, the ability of Mozilla and Vivaldi browsers to offer users additional security features such as "safe browsing mode" (warning messages are sent about potentially dangerous sites or downloads), full-screen video playback, etc. is limited.

2. Apple is limiting the functionality and reducing traffic of "progressive web apps" - a version of a website that is saved on the device's home screen as an app. This limits the launch of apps by developers, while such apps can run on any operating system and are cheaper and easier for companies to develop.[32]

3. Apple is limiting the web browsing feature in WebKit-powered apps by reducing traffic.

4. Apple has entered into a revenue sharing agreement with Google, where Google pays Apple a share of the revenue generated from traffic to Safari and Chrome on iOS from search advertising.

[26] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202520260AB412

[27] https://www.gov.uk/government/consultations/copyright-and-artificial-intelligence/copyright-and-artificial-intelligence

[28] For example, filters that detect data mining robot programs and prevent them from accessing the site.

[29] That is, markings ("flags") in metadata for AI systems or their developers that indicate whether a given set of metadata is allowed to be used for AI training.

[30] https://www.pnp.ru/social/koncepciyu-regulirovaniya-iskusstvennogo-intellekta-obnovili.html

[31] https://digitalpolicyalert.org/event/27509-cma-issued-a-summary-of-the-provisional-decision-report-pdr-response-hearing-with-google

[32] Such apps don't have to be downloaded from the App Store - you can site save to your phone screen as a regular app (mostly free).

The CMA also plans to assess the impact of Apple's actions on competition in the cloud gaming market.[33] For example, Apple requires:

– That each game is sent to the App Store as a separate app - restricting the creation of aggregator apps on iOS with access to multiple streaming games.

– Use Apple's payment systems for in-game transactions, charging a 30% fee.

The German experience

In February 2025, the Federal Cartel Office evaluated Apple's “App Tracking Transparency Framework”.[34] The ATTF is a requirement for developers to inform users about the procedures for informing about the use of their personal data, particularly for advertising purposes. Developers must obtain user consent before using data for advertising purposes, especially if they create free, ad-funded apps.

The wording and design of such consents were found to differ between Apple and third-party apps in ways that encouraged users to allow data collection by Apple's own apps and to deny permission to third-party apps. For example, third-party apps required separate consent from users to allow their data to be used and aggregated by different services within the developer for advertising purposes, which was requested in a pop-up window when the app was first launched. However, there were no restrictions on combining user data from different services in the Apple ecosystem (App Store, Apple ID, from devices) for advertising purposes, and Apple's consent requests did not disclose the methods of data processing between Apple services at all. As a result, third-party app developers are forced to offer users up to 4 pop-ups to get all consents, while only 2 for Apple apps. The investigation is still ongoing.

Russia’s experience

In Russia, the FAS Principles of Interaction of Digital Market Participants do not cover practices related to the abuse of a dominant position through various technologies, such as slowing down browser traffic, limiting operation of progressive applications, and manipulating data collection consent forms.

[33]https://assets.publishing.service.gov.uk/media/6687b9fd899a6f92e5d9cd46/WP6_-_Cloud_gaming_services__nature_of_competition_and_requirements_for_native_apps_on_mobile_devices.pdf

[34]https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2025/02_13_2025_ATTF.html?nn=52004