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

- **Responsible AI governance**
- **Right to data portability**
- **Cross-border flows of non-personal data**
- **Regulation of tracking pixels**

Monitoring No.6 (18) (June 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

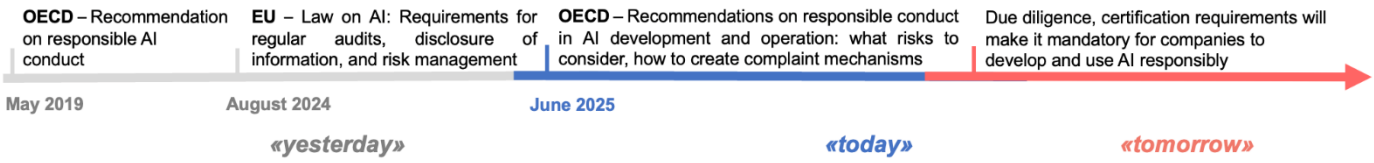
"What is there to do in the city in June?
No lanterns are lit;
On a yacht, on a Chukhonian schooner
I want to leave soon!"
Osip Mandelstam

In June 2025, we can identify 4 events that define trends in the development of digital economy regulation globally.

Trend No.1. Responsible AI governance

In June 2025, the OECD issued recommendations for the responsible AI governance: disclose information about how algorithms work, discuss risks with employees, users and regulators, etc.

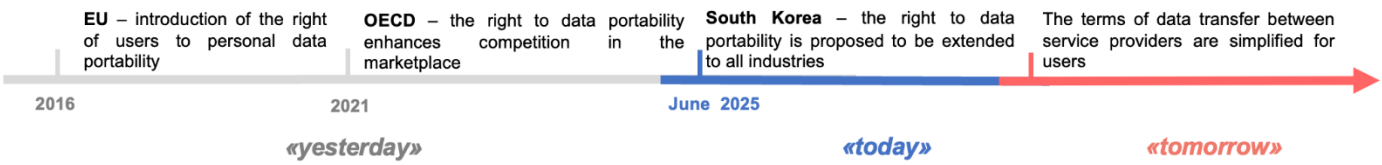
Trend
Responsible AI governance



Trend No.2. Right to data portability

As of June 2025, South Korea is expanding the right of citizens to transfer their personal data from one organization to another in any industry.

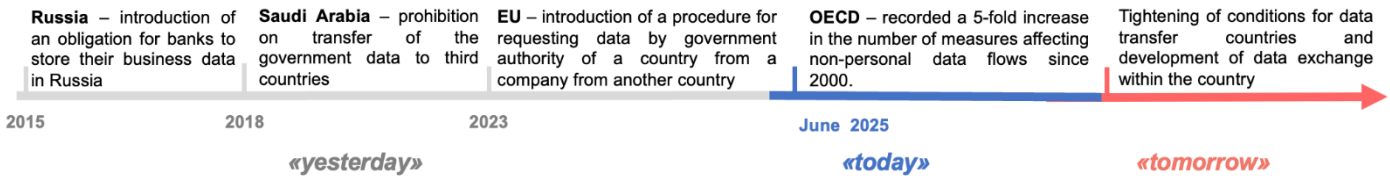
Trend
Right to data portability



Trend No.3. Cross-border flows of non-personal data

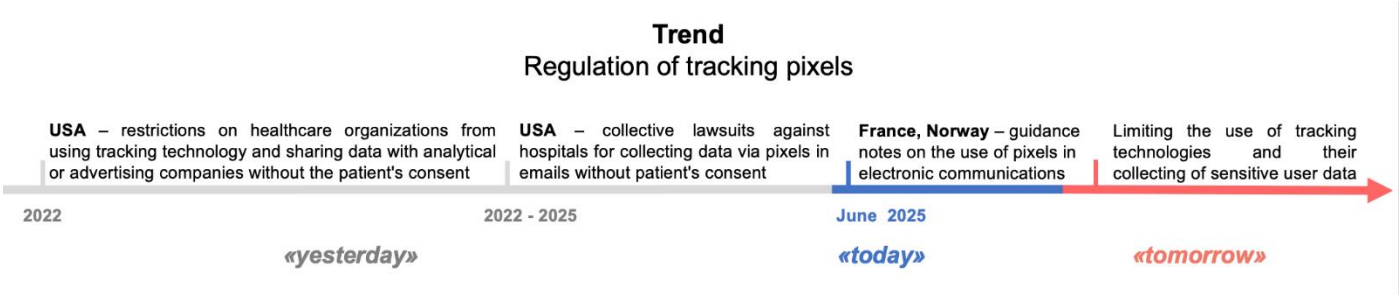
In June 2025, the OECD submitted a report noting a fivefold increase in the number of measures regulating cross-border flows of non-personal data between 2000 and 2024. Measures include requiring data localization, mandatory transfer of fata from companies to government agencies, facilitating cross-border data sharing, etc.

Trend
Cross-border flows of non-personal data



Trend No.4. Regulation of tracking pixels

In June 2025, France and Norway issued guidances on the use of pixels, a tracking technology for collecting user behavior data, including its use in email communications (email opening rates, geolocation, IP address, etc.).



There are a number of innovations introduced in June 2025.

1. A national messenger will be developed

In June 2025, Russia adopted a Law[1] on the creation of a multifunctional information exchange service - actually a national messenger both for personal messages to other users and for communication with authorities and institutions. The national messenger will be connected to the infrastructure of Gosuslugi, providing several opportunities unique to citizens:

1) Use of an enhanced electronic signature to sign documents.

2) Interact with participants of educational institutions (participation in school chats) and use educational services.

3) Submission of personal documents via messenger. For example, it will be allowed to present documents to confirm age, eligibility for benefits, to present documents for general and vocational education institutions, hotels and other organizations.

If a citizen presents documents via messenger, paper copies may not be requested. In fact, the messenger will work as a digital ID through which a citizen can provide information about himself or herself.

The developer of such a service will be chosen by the Government's decision. An important criterion for the selection of the developer organization will be that it has a social network with more than 500,000 users per day. The creation of such a messenger, on the one hand, advance digitalization of some processes (such as paperless presentation of documents), but on the other hand, there are risks of monopolization on the work of such a messenger in the hands of a single operator. In such a case, the messenger may need to ensure interoperability with other social networks, messengers, etc.

2. The procedure for filling in the GIS OPD has been determined

In June 2025, the Government of the Russian Federation approved the rules[2] for the formation of compositions of anonymized personal data to be transferred by companies to the State Information System of Anonymized Personal Data (GIS OPD).[3]

Data should be provided not on a regular basis, but at the request of Roskomnadzor. In accordance with the rules, when forming data compositions, Roskomnadzor assesses the risks of restoring anonymized data to the original state, which is necessary to ensure the safety of further use of this data in the system. Roskomnadzor also checks the quality of data to exclude repetitive or inaccurate data. In this case, access to the data is carried out in accordance with the procedure of sending a request by a company or an individual to the authorized body.

This tool is aimed solely at developing the quality of public administration and does not address the task of developing the data market in Russia, since the state, not the market, will determine the composition of the data to be opened, and the data will become available at the request of private organizations (if they meet the requirements of the law) only one year after their transfer to the state.

3. Regulatory measures for drones introduced

[1] Federal Law No. 156-FZ of 24.06.2025 "On the Creation of a multifunctional information exchange service and on amendments to certain legislative acts of the Russian Federation".

[2] Decree of the Government of the Russian Federation of 26.06.2025 No. 961 "On the formation of the composition of personal data obtained as a result of depersonalization of personal data, grouped according to a certain characteristic, provided that the subsequent processing of such data will not allow to determine the belonging of such data to a particular subject of personal data, and providing access to the composition of such data".

[3] Decree of the Government of the Russian Federation No. 740 dated 28.05.2025 "On the state information system of the federal executive body that performs the functions of elaboration and implementation of state policy and normative-legal regulation in the field of information technologies, specified in Article 13.1 of the Federal Law "On Personal Data".

In June 2025, the Ministry of Industry and Trade issued an order[4] that clarifies how the so-called C2 channels - the routes along which operator commands and drone telemetry are sent - should be constructed. The essence of the innovation is simple. The drone owner decides whether he will send signals to control the drone directly via radio or through an external provider, who will provide the infrastructure for the signals and make sure that there are no dropped connections to the drone. The owner installs the necessary hardware, obtains permission to use a certain radio frequency for control,[5] logs every flight and record instances of lost communication channel with the drone during flights. The provider, in turn, is obliged to keep the communication line without failures, maintain the equipment and immediately notify the owner in case of malfunctions. The state operator (not yet officially defined)[6] distributes radio frequencies, sets the zones where drones can catch the signal, and stores their telemetry[7] as “black boxes”.

According to the order, responsibility for the operation of unmanned aircraft systems lies with: the owner is responsible for the device itself; the provider is responsible for the quality of the signal: the state-appointed organization is responsible for frequencies and safety.

This order is a continuation of the history with the introduction of drone regulation in Russia. Back in 2023, the Air Code was supplemented with requirements on special aviation regulations for drones (mandatory certification of unmanned aviation systems, rules for drone control infrastructure, etc.). In 2024, Russia launched the national project “Unmanned Aviation Systems”.

[4] Order of the Ministry of Industry and Trade of Russia No. 2266 dated 14.05.2025 “On Approval of federal aviation rules ”Procedure for organization and maintenance of unmanned aircraft systems control lines and unmanned aircraft systems control for unmanned aircraft systems of aviation enterprises and experimental aviation organizations".

[5] frequency of electromagnetic oscillations, established to designate a single component of the radio frequency spectrum.

[6] Government provider of unmanned aircraft system control lines and unmanned aircraft system monitoring services.

[7] Data on communication and control line status, volume and speed of transmitted information required for safe control of the drone

.

Key aspects

1. Responsible AI governance

The OECD experience

In June 2025, the OECD described[8] how to extend responsible business conduct due diligence (hereinafter RBC)[9] to the regulation of AI. The OECD's RBC principles address human rights, labor, environment, anti-corruption, consumer interests and taxes. They apply to any area of business.

The OECD recommends that companies building and implementing AI systems apply the Six-Step procedure:

– Integrate risk management into corporate policies. For example, in 2025, Microsoft revealed in reporting that each of the company's AI projects undergoes more than 30 mandatory internal reviews before launching.

– Identify and rank potential and actual negative impacts of algorithms on human rights, security and the environment. In June 2025, Google described[10] how its "red team" preemptively attacks the Gemini 2.5 model with malicious requests to teach the system how to respond correctly.

– Take measures to prevent and minimize risks at all stages of the model's lifecycle. For example, YouTube, starting from May 2025, obliges authors to label videos created with the help of AI.[11]

– Provide independent auditing and public reporting on the plan's progress. For example, in December 2024, OpenAI invited the AI Security Institutes to test the new ChatGPT model prior to release and published their findings.[12]

–Engage in meaningful dialog with stakeholders and provide a grievance mechanism with effective redress. For example, in March 2025, OpenAI promised to pay up to $100,000 to anyone who finds a serious vulnerability in its AI systems, thereby encouraging users to report glitches.[13]

–Track the effectiveness of measures and disclose findings in public reports. For example, in April 2025, Google disclosed that its AI had blocked 5.1 bn malicious ads and disabled 39.2 mn fraudulent accounts.[14]

Due diligence is based on risk assessment: the depth of scrutiny should be commensurate with the likelihood and severity of possible harm. For "high-risk" systems, such as those identified in the EU AI Act 2024, due diligence should be ongoing and include internal and external controls. For AI developers and suppliers, due diligence is a system for identifying and mitigating threats to human rights, consumer safety and the environment. Its implementation will reduce a company's legal and reputational risks in the event of failures and make it easier to comply with AI laws.

This is especially true for generative AI. In the new report, the OECD notes[15] that generative AI research expanded beyond the IT sector, with more than 71,000 generative AI patents published worldwide in 21 sectors between 2000 and 2023, including more than 32,000 in software. In addition to software, the key sectors in terms of number of patents are life sciences, medical sciences, business solutions, document management, and industrial manufacturing.[16] In 2024, the adoption of generative AI in companies remains low, with only 5.4% in the EU using chatbots and 9.3% in Canada. In the US, 22% of workers use AI on a weekly basis. At the same time, over 50% of global usage is in middle-income countries. According to the

[8] https://www.oecd.org/en/publications/responsible-business-conduct-and-anticipatory-governance-of-emerging-technology_1308a723-en.html

[9] Responsible business conduct means measures that enable a company to recognize which of its decisions and operations may harm people, the environment or fair competition, and to take timely action to prevent or compensate for such harm. This includes treating employees and suppliers fairly, respecting human rights, caring for the environment, paying taxes transparently, combating corruption, and so on.

[10] https://security.googleblog.com/2025/06/mitigating-prompt-injection-attacks.html?

[11] https://ppc.land/youtube-introduces-mandatory-disclosure-for-ai-content

[12] https://www.aisi.gov.uk/work/pre-deployment-evaluation-of-openais-o1-model

[13]https://www.forbes.com/sites/daveywinder/2025/03/29/hack-openai-win-100000-what-you-need-to-know

[14]https://services.google.com/fh/files/misc/ads_safety_report_2024.pdf

[15] https://www.oecd.org/en/publications/is-generative-ai-a-general-purpose-technology_704e2d12-en.html

[16] In particular, in the EU, US states, UK, Canada, Australia and others.

OECD, this indicates a deeper integration of AI into economies with growing digital maturity.[17]

Russia's experience

In Russia, there are initiatives that promote the implementation of RBC principles in the development and use of AI. For example, a voluntary Code of Ethics in the field of AI.[18] In June 2025, the Bank of Russia also published an AI Code of Ethics for financial institutions.

There are currently no real regulatory measures to ensure responsible conduct in the use of AI, including generative AI, beyond strategies and instructions in Russia.

2. Right to data portability

The experience of South Korea

In June 2025, the South Korean government proposed to extend the "right to portability" from certain fields (medicine, telecom) to all sectors of the economy. That is, a citizen can demand the controller (organization) to transfer his or her personal data to him or her or, at his or her direction, to any third party. The organization will be obliged to implement the user's request to transfer his personal data if:

– It has over $110 mn in revenue and over 1 million users.

– It has more than 5,000 users and accumulates sensitive[19] or unique data of such users.

– Universities with more than 20,000 students or operators of public administration systems (e.g. outpatient clinics).

However, data that the operator compound with other data or analytics, such as a database of users' likes aggregated by gender and age and combined with data on users' music preferences, is exempt from regulation. In this way, the law protects the right of companies to create databases and other products based on user data.

Notably, the user can request to transfer personal data both directly to himself (e.g., to download a data file to his computer) and to third parties - specialized intermediary organizations. Such organizations act as agents for data subjects, so they have the right to receive and store data on behalf of the user, provide access to his data, and transfer them to third-party organizations at his request, but they cannot process the data received. Organizations must comply with information security requirements, technical and organizational measures to prevent data leakage, etc.

The EU experience

In foreign legislative practice, the right to data portability first appears in the EU General Data Protection Regulation in 2016. The right was introduced to enable users to freely transfer between companies, primarily digital platforms competing with each other.[20]

The Korean initiative to establish the institution of specialized user data management organizations is similar to the institution of data intermediary in the EU. However, in the EU, such an intermediary can provide services not only for personal data but also for non-personal data.

Russia's experience

In Russia, the right to data portability is currently not established - there is no right to receive a copy of the processed data, nor is there a right to request the transfer of processed data to another data controller. There is also no special regulation for providers of data intermediation services.

3. Cross-border flows of non-personal data

The OECD experience

In June 2025, the OECD released a report on the classification of measures affecting cross-border flows of non-personal data (i.e. data that does not identify specific individuals - hereinafter – NPD).[21] From 2000 to 2024, the number of measures to regulate NPAs has increased five times, both incentivizing and restricting data flows. According to the OECD measures affecting data flows include not only measures regarding cross-border data transfers but also measures affecting the accessibility of data between countries (e.g. the ability to view and use data stored in one country by users in another country). OECD experts estimate that

[17] https://www.oecd.org/en/publications/is-generative-ai-a-general-purpose-technology_704e2d12-en.html
[18] https://ethics.a-ai.ru/
[19] Sensitive data - data on ideology, political views, criminal record, biometrics data, etc. Unique data - passport number, driver's license number, etc.
[20] https://iapp.org/news/a/data-portability-in-the-eu-an-obscure-data-subject-right
[21] https://www.oecd.org/en/publications/a-preliminary-mapping-of-measures-affecting-the-cross-border-flow-of-non-personal-data_0825c57c-en.html

cross-border data sharing can increase GDP by up to 2.5%

Based on the analysis of 124 measures, OECD experts identify 3 categories of measures:

1) Measures that encourage cross-border access to NPD and data sharing (17% of measures). For example, open government data initiatives that are accessible to foreign users, among others, fall into this category. For example, the US Open Government Data Act of 2019 sets out requirements for the publication of open data by federal agencies, including the availability of data to an unlimited number of people, including foreigng users.

2) Measures requiring companies to provide cross-border access to their NPD to the government and other companies. For example, in the US, the Foreign Lawful Use of Data Act of 2018 (CLOUD Act) obliges US electronic communications service providers to provide US government agencies with access to information, including information stored outside the US. In this category, 84% of measures require data disclosure to government agencies and only 16% - disclosure to third parties.

3) Measures prohibiting cross-border access to and sharing of NPD such as restrictions on cross-border data transfers (obtaining the authority's approval for each data transfer, the security risk assessment of data transfers abroad by the authority, etc.) and data localization requirements, which limit the ability of companies to transfer data for the purpose of storing it on servers in third countries. In total, localization requirements account for 35% of all identified NPD regulatory measures worldwide.

The largest number of measures are adopted for manufacturing data (e.g., data from internet devices in a factory), business data (e.g., transportation of goods), and government data (e.g. budget management data). It is noteworthy that for government data, 50% of measures have restrictive effects for public access, and only 40% are open data initiatives, including for foreign users.

Russia's experience

In Russia, most measures are aimed at regulating personal data.

There are few initiatives regarding non-personal data. For example, from 2012 Russia has been developing the concept of open government data, but the published data are little involved in the domestic digital economy. Russia does not have the principle of "open government data by default" (i.e., the principle "publish everything that is not prohibited for publication"). As a result, only those data that are required to be published by law are disclosed.

Public data are collected and published to different degrees: the government publishes detailed financial data (e.g. tax data) but does not collect data on quality of life. Data are opened without regard to user demand for specific data compositions.

4. Regulation of tracking pixels

Experience of France and Norway

In June 2025, France launched a public debate on a draft recommendation regarding the use of tracking pixels in electronic communications.[22] Similar guidance has also been published in Norway.[23]

A tracking pixel is a special tracking technology representing an image (1x1 pixel in size) that is embedded in emails (as well as advertisements, browsers, etc.) and allows collecting data on user activity (e.g., whether the email was read, time the email was opened, IP address, device and browser from which the email was opened, geolocation, etc.). Pixels are placed not in the email itself, but on remote servers (outside the site where the user is located), which makes it possible to collect user data on a remote server with further processing of such data.

When a user opens an email, an image of the pixel is automatically downloaded, sending a request to the server where the pixel is located. The request contains technical data, including IP address, device and browser information, timestamp, and so on. - at which point the user activity data is received by the server. That is, the pixel itself does not collect any information, but the fact that it is downloaded allows the sender of the email to receive information that a particular email was viewed by a certain user, the time of viewing, geolocation, and so on.

Regulators are focusing on developing rules specifically for this technology due to the

[22] https://www.cnil.fr/fr/consultation-publique-projet-recommandation-pixels-de-suivi

[23] https://www.datatilsynet.no/personvern-pa-ulike-omrader/internett-og-apper/bruk-av-sporingsverktoy-pa-nettsteder-og-i-apper/

rise in lawsuits. For example, in 2022, lawsuits were filed against a one-third of the 100 largest US hospitals that sent sensitive data to Facebook[24] via pixels on their websites.[25]

Technology enables the collection of data about the recipient of the email, so regulators in France and Norway recommend the following:

1. Consider that the sender of the e-mail message becomes the controller of the data collected through the tracking pixels, as it is the sender who decides whether to use the technology to collect the data, as well as determining the goals of data processing.

The email service provider ensures that users' emails are received and displayed, it does not affect senders' use of pixels (although it may block automatic image uploads), so it is neither a data processor nor a data controller.

2. Embedding tracking pixels in emails will require prior consent from the recipient:

– When analyzing the opening of emails. For example, if a sender is evaluating their marketing strategies (how often recipients read emails, how attractive the email headers are, etc.) to improve email readability, adjust the frequency of sending emails, etc.

– When individually analyzing the recipient's interest in emails to personalize content, e.g., customizing the content of emails depending on the identified preferences and interests of the recipient; personalizing the sending channel (email, SMS, push notifications, etc.) depending on which channel the recipient uses more often.

Consent is not required for:

– Using pixels for security and user authentication. A pixel allows you to make ensure that an email with a password reset link is opened on a device that belongs to a specific user.

– When measuring the statistics of opened emails. In this case, you should use pixels for anonymous statistics, without individually tracking individual users.

3. The purpose of using pixels should be disclosed. For example, recipients could be warned to the recipient that when they open the email, information about their actions may be used to display personalized ads or content on other platforms.

4. Consent to use pixels can be requested at the time of consent to send emails, warning that pixel tracking will occur when the email is opened.

5. There should be a simple procedure for withdrawing consent to the use of tracking pixels. For example, it is recommended that a link to withdraw consent be included in every email containing the pixel. This link should lead to a site where consent can be withdrawn without additional steps (e.g., entering an email address).

Russia's experience

Today in Russia, Roskomnadzor does not issue special guidelines on the use of tracking technologies, including such technologies as cookies. However, behavioral data collected by such tracking technologies fall under the definition of personal data provided for in Federal Law No. 152 "On Personal Data". In particular, Russian courts qualify cookie data as personal data.[26] Thus, data collected through tracking pixels is subject to the same legal protection as other personal data.

[24] Meta's activities are recognized as extremist and banned in the Russian Federation

[25] https://www.infosecurity-magazine.com/opinions/website-tracking-tech-risk-analysis?utm_source=twitterfeed&utm_medium=twitter

[26] Ruling of the Nineth Arbitration Court of Appeal in Case No. 09AP-17574/2016.