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

- New responsibilities for platforms to combat fraud
- International data protection practices for web parsing

Monitoring No.10 (34) (October 2026)

Monitoring has been prepared by a team of employees of the International Best Practices Analysis Department at the Gaidar Institute.
Associated authors: Maria Girich, Researcher, Ivan Ermokhin, Researcher, Antonina Levashenko, Senior Researcher, Olga Soldatkina, Researcher, Kirill Chernovol, Researcher, Diana Sinelnikova-Muryleva, Researcher

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

Deception all around!

New responsibilities of platforms to combat fraud

Author: Kirill Chernovol

Fraudulent schemes often evolve alongside technology. Regulators have begun to entrust platforms with responsibilities to combat fraud.

In October 2026, the EU published a study on 6 types of financial schemes related to investments, dating, e-commerce, easy money, employment and charity.

Fake product or seller listings are being created on marketplaces, and AI can create more of these listings than humans can "sift through." A customer visits such a listing, for example, on a classifieds site (like Avito), communicates with an AI chatbot posing as the seller, transfers money for the product or service, and then the fraudster disappears.

To combat such practices, in October 2026, the European Commission launched an investigation into Booking.com to assess the effectiveness of the platform's measures to mitigate the risks of fake accommodation listings and the misuse of guest and booking data. The Commission is reviewing the data transfer procedures to hotels and the internal communication processes at Booking.

$ 3.2 mn

on average, fraudsters steal from blockchain networks in one transaction using AI

Another example is dating sites and social media. Here, fraudsters beguile victims into giving up money and payment information under the guise of online relationships, romantic correspondence, or sexting. Such correspondence can be conducted by AI chatbots. Another scheme involves posing as a friend of the victim's and asking for money, supposedly for help. By the way, sexting is prohibited or restricted by law in at least 5 countries around the world[1] and in China such ban has been approved exactly for generative AI.

In this context, in October 2026, the United States passed a law requiring dating platforms to notify users of contact with fraudsters. If a service blocks a fraudster's account, it must notify all users who received messages from that account.

Deepfakes. Fraudsters impersonate the face and voice of, for example, a company's top manager, to convince victims, the company employees, to transfer money. Thus, in 2024, an employee of the British company Arupa in Hong Kong office received a letter purportedly from the head office's CFO, instructing him to carry out a confidential transaction.

He was then invited to a video conference where the "CFO" and other "colleagues," whose images and voices had been spoofed by AI, convinced him to transfer about $25.6 mn to them. It is unknown if fraudsters were caught.

Criminals can attack not only humans but also AI agents. The European Commission has highlighted the threat of attacks on AI using "prompt injections." The problem is that AI, when analyzing text, doesn't always distinguish between the information it should process and the commands it should execute. For example, when viewing a user's social media messages, AI might detect a hidden instruction ("prompt") in one of them and mistake it for a command from the user, such as to transfer sensitive data or transfer money to an intruder's account.

Thus, in June 2026, code for the Microsoft Azure cloud platform was discovered in the open GitHub repository, which was supposed to help users set up their projects on this platform. However, the project's documentation contained instructions for the Cursor AI agent to collect and transmit to the fraudsters the users' access keys for various services (GitHub, AWS cloud platforms, Azure, Google Cloud, and others). In total, 73 Microsoft repositories were targeted.

[1] Nigeria, Oman, UAE, India, Bangladesh.

The European Commission recommends combating such practices by conducting checks on platform participants (sellers, advertisers, performers, etc.), identifying keywords in correspondence and creating systems for reporting fraudulent activity. It is proposed to develop exchange of information about fraudsters between platforms, banks, telecom operators, and law enforcement agencies. Warn users about potential fraud before transferring funds, use additional confirmations, and "cooling-off periods" where funds for a suspicious transaction can only be transferred after a certain period of time, so that the victim has the opportunity to seek help.

In Russia, according to the Federal Law "On the Platform Economy," operators of intermediary digital platforms are required to verify partners, i.e., sellers, contractors, etc., through state registries, as well as verify information on product cards (such as permits and labeling). The Antifraud State Information System (GIS) is used in Russia to facilitate interactions between government agencies, banks, telecom operators, and messaging apps. It helps obtain information about known fraudsters and block their activities promptly. Marketplaces will be obliged to hook into this system from March 2027.

What is next?

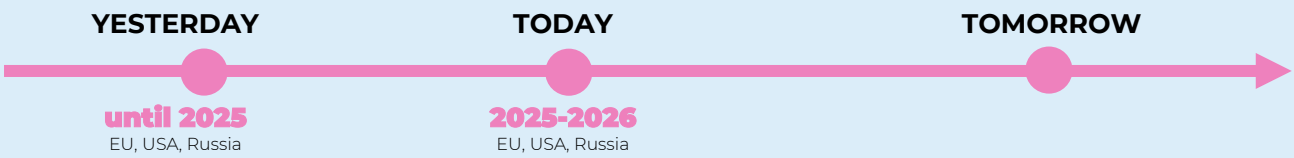
Russia has already implemented general regulations to combat fraud on platforms. There are no specific regulations for AI-based fraud.

How much will it cost marketplaces to secure transactions from fraud? According to Data Insight findings, in 2026, the number marketplaces' online-orders in Russia will account for about **8.1** bn, thus, its growth since 2025 will reach **20%**. At this rate, even if the verification of one order costs Rb 1, marketplaces will have to spend Rb **52.18** bn to combat fraud in 2027-2030.[1]

However, the cost of damage is much greater: according to the Bank of Russia, the amount of client transfers to fraudsters in 2024 amounted to Rb **26.86** bn, and in 2025 – Rb **28.25** bn. Thus, between 2027 and 2030, fraudsters could extract at least Rb **135** bn from Russians.[2]

[1] If the number of orders on Russian marketplaces grows by 20% annually, and one check of each order costs Rb1, then Rb 8.1 bn in 2026 * 1.2 for each subsequent year, we get Rb 9.72 bn in 2027, Rb 11.66 bn in 2028, Rb 14.00 bn in 2029 and Rb 16.80 bn in 2030. Total for 2027-2030 – Rb 52.18 bn..

[2] If the amount of thefts from individuals registered by banks grows by 5.16% annually, as between 2024 and 2025, then the estimated Rb 29.71 bn in 2026 * 1.0516 for each subsequent year, we get Rb 31.24 bn in 2027, Rb 32.86 bn in 2028, Rb 34.55 bn in 2029 and Rb 36.33 bn in 2030. Total for 2027–2030 – Rb 134.99 bn.
.



Combating fraud by blocking fraudulent websites and monitoring suspicious payments, protecting personal and payment data

Responsibilities for platforms to prevent fraud before damage occurs

Expanding platform responsibilities: stricter requirements for user authentication on platforms, increased platform control over AI agents' access to data and funds: protection against "prompt injections," additional confirmation of transfers, human actions, etc.

Secure data parsing: all or nothing

International data protection practices for parsing

Authors: Olga Soldatkina

17% *of websites have already launched restrictions for data parsing for training, according to Cloudfare estimates*

Data parsing (or web scraping - the automated collection of data from web pages) not only adds "fuel" (data) to the AI technologies' race, but also challenges the privacy of personal data. Traditionally, data protection focused on ensuring control of their data by individuals and that companies obtain user consent to use it. But how can data use be controlled if it is collected by AI beyond human control?

In October 2026, the OECD published a report on enhancing user control in the context of AI. The OECD noted that AI bots often collect data not for training, but rather to respond to a one-time user request (using RAG technology – augmented generation), so data parsing settings are not applicable.

In this regard, the South Korean Personal Data Protection Commission recommends filtering data both during collection and during model output when AI accesses external databases through RAG.

The OECD recommends addressing AI risks at multiple levels.

Clarification is needed at the regulatory level on how to apply current data requirements. For example, in the EU, the EDPB's ChatGPT task force is clarifying how to interpret the GDPR[1] in the context of the use of large language models. The key conclusion is that the developer cannot shift responsibility to the model's user through user agreements, for example, by warning against entering sensitive health data into a chat.

At the level of data source (on websites), for example, restrictions on automated data collection can be established, as well as technical barriers can be implemented, such as the use of "robots.txt" files (the standard by which a website tells search robots which sections they can visit) or Cloudflare features (blocking AI bots at the network level with a single setting).

Data control tools can also be applied at the developer level. For example, multi-stage filtering allows developers to filter out personal and sensitive data before it is included in the training dataset. Data origin tracking techniques can also be used, where each piece of information is tagged with the website from which it was collected. For example, the French data protection regulator CNIL has introduced a tool for tracking the sources of data produced by AI, a technique that allows for the extraction of data fragments from an existing dataset for AI training, if necessary.

It is also important to maintain transparency in the data processing: the datasets being collected must indicate the sources of collection, exclusion criteria, and filtering methods.

In the context of parsing, the focus needs to shift from protecting data from breaches (which a person may never know about) to the fair handling of data when working with AI.

In October, the EU discussed the Web Scraping Guidelines for generative AI, specifically regarding the application of the GDPR to parsing. Safe web parsing is based on the principle of "no longer seeing the user," meaning not collecting data that is not visible to the user on the website but is discernible by the AI parser.

Publishing data publicly does not constitute consent for its parsing. However, since individual consent is difficult to obtain for large-scale scraping, a developer may collect data without consent if it is necessary for a clear and legitimate purpose (for example,

1 GDPR (General Data Protection Regulation) 2016

training a model)—this basis for processing is known as "legitimate interest."

At first glance, data parsing and data collection minimizing seem mutually exclusive. However, with parsing, the minimization principle begins to be applied even before data collection, when the developer defines the data filtering criteria.

Moreover, data "culling" is also performed during the training dataset formation stage, meaning that data used for AI is minimized after parsing. The principle of minimization refers to the order in which it is selected rather than to the volume of data.

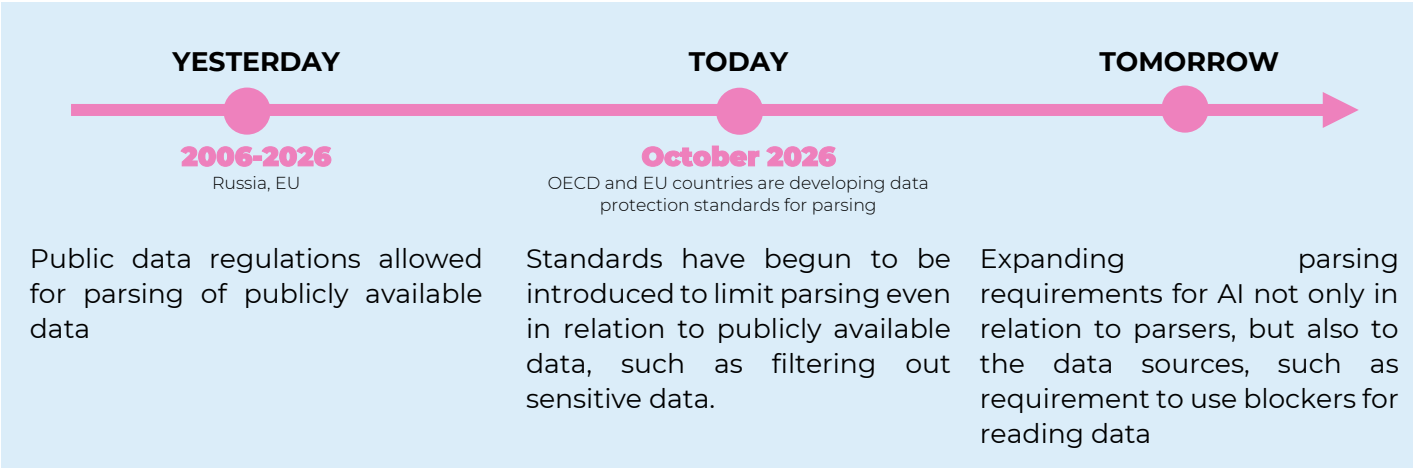
In Russia, the legality of parsing is based on publicly available information regulations. However, the court ruling in VKontakte v. Double (2021) case found that, although VKontakte user data is publicly available, parsing it for analytical products and commercial sales violates VKontakte's database rights.

The era of AI is changing our understanding not only of how data is collected but also of the very categories of data that can be processed. For example, human neural data, i.e., data on the functioning of the human nervous system. On the one hand, data about human physiological and mental state is considered health data, i.e., personal. On the other hand, can machine interpretations or calculations of nervous system signals (so-called "inferred data") be considered personal data? After all, here the line between what a human produces (his nervous system) and what technologies record as his data (his nervous system) is blurred.

In a report on neuro-data governance, the OECD analysts note the need to adapt data regulation to a new type of AI. i.e., fundamental models of the brain (Brain Foundation Models) based on the analysis of neuro-signals. Moreover, the inferred data may be more sensitive than the original. However, AI conclusions about emotions, intentions, and cognitive patterns may drop out from the protection of data laws, even though such data is no less sensitive than health data, and therefore may require a comparable level of protection.

What is next?

While rules are being discussed, data on Russians is already being collected. In the global web-aarchive Common Crawl, Russian is the second language after English in terms of the amount of data that can be parsed for AI training. Of the 160 identified languages Russian accounts for **6,3%** web-pages (**136.1 mn** pages). However, even this supply is not infinite. Epoch AI estimates that there are approximately 300 trillion human-created texts available for AI training. There's an **80%** chance that models will completely exhaust this supply between 2026 and 2032. This means that future generations of AI will increasingly be trained not on human-created data, but on generations of previous AI models.



Public data regulations allowed for parsing of publicly available data

Standards have begun to be introduced to limit parsing even in relation to publicly available data, such as filtering out sensitive data.

Expanding parsing requirements for AI not only in relation to parsers, but also to the data sources, such as requirement to use blockers for reading data

News **in October 2026** that we found interesting.[1]

- The US proposed to ban large grocery stores and their online platforms from setting individual prices based on the personal data of customers (age, income, etc.), using biometrics for pricing, and raising prices depending on the expected time of purchase.

- The EU proposed to increase by a factor of **50** (from Euro 6 bn to 300 bn) the limit of the value of tokenized stocks and bonds that can be traded on blockchain platforms, and also allow crypto exchanges licensed under the MiCA (Markets in Cryptoassets Regulation) to participate in such trading.

- The US proposed to facilitate fundraising through the issuance of crypto assets (ICO): exempt companies from mandatory registration under securities laws when raising up to $5 mn over 4 years or up to $**75** mn per year subject to additional reporting requirements.

- In Russia, the Central Bank determined the digital currency accounting rules for banks: a reduction in its value must be recognized as a loss, even if the currency has not yet been sold, and a gain from an increase in value must be recognized only after the sale. For example, if a bank purchased digital currency for Rb 1 mn and its value declines to Rb 800.000, it must record a loss of Rb 200.000. If the value increases to Rb 1.2 mn, the gain of Rb 200.000 can only be recorded after the sale. This approach is already used in commodity accounting.

- The Ministry of Digital Development, Communications and Mass Media of the Russian Federation proposed measures to combat ICT crime: citizens will be able to use Gosuslugi to check who they have consented to the processing of their personal data to and revoke that consent. The list of data collected and the purposes for which it is processed will be determined by the relevant ministries.
- Norway plans to restrict the use of AI-powered smart glasses in public places (parks, beaches, museums, schools, etc.) to prevent people from being filmed without their consent.

- Roskomnadzor took up the trend of restricting children's use of social media, proposing mandatory identification of children on social media and limiting the time children under 14 can spend online.

[1] Since 2025, the Gaidar Institute has been developing a digital platform for analyzing news in Russia and globally on the topic of digital economy regulation – DIgiReg. The news presented has been selected by experts, in part based on an analysis of the platform's data.