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

Strengthening of AI regulation, anti-competitive practices online, protection of consumers online

Monitoring No.12 (December 2024)

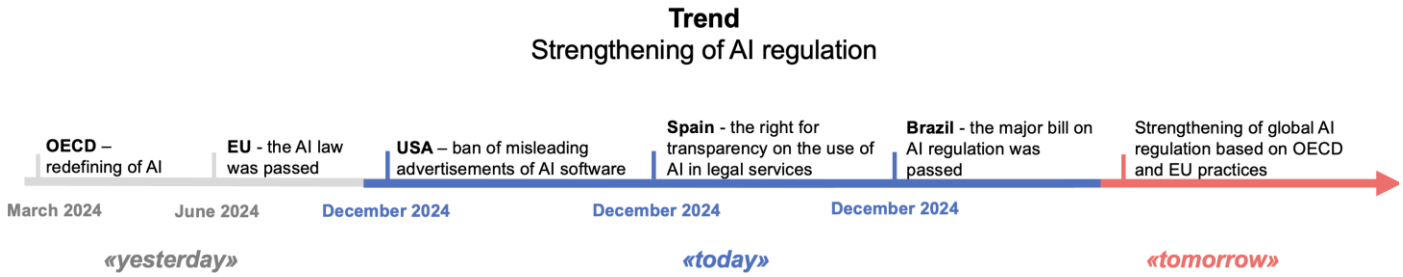
Monitoring was prepared by a team of experts of the International Best Practices Analysis Department at the Gaidar Institute for Economic Policy (Gaidar Institute): *Antonina Levashenko,* Senior Researcher. *Maria Girich*, Researcher. *Ivan Ermokhin*, Researcher. *Olga Magomedova*, Researcher. *Tatiana Malinina*, Senior Researcher.

“With cheerful heart the new year revives
And a new joy in Russia claims.”
Mikhail Lomonosov

In December 2024, we can identify 3 events that define trends in the development of digital economy regulation in the world.

Trend No. 1. Strengthening of AI regulation

In December 2024, the US Federal Trade Commission banned the circulation of misleading advertisements for facial recognition software that uses AI. Spain introduced the right of defense for the use of AI in legal services. Brazil adopted a basic law on the use of AI.

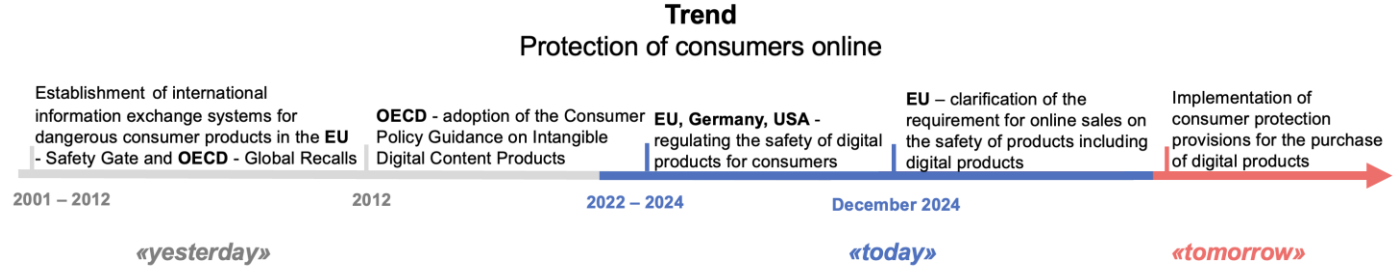


Trend No. 2. Anti-competitive practices online

In November 2024, China's antimonopoly regulator launched an investigation into US graphics processor manufacturer Nvidia over alleged violations of the terms of acquisition of Mellanox Technologies (a manufacturer of network interconnect products). In South Korea, the antitrust regulator fined the taxi-hailing services Kakao Mobility for illegally collecting information on competing franchisees, resulting in the aggregator's monopoly on the market. In Italy, an analysis of dynamic pricing of airfares showed that there was no discrimination against consumers, including using their data.

Trend No. 3. Protection of customers online

Since December 2024, the General Product Safety Regulation has been in force in the EU defining the requirements for digital and online products, namely, cybersecurity characteristics for safety assessment, e.g., a mobile application is not considered a safe product if it is not protected from cyberfraud messages. There are also special requirements for e-commerce platforms: facilitating the blocking/removal of content with unsafe products; informing customers about the purchase of products with identified security issues.



In December 2024, Russia also saw significant developments in the regulation of the digital economy:

1. New advertising taxes

In December 2024, amendments to the Law on Advertising were adopted[1]:

1. From April 2025, mandatory contributions will be imposed on Internet advertising distributors and operators of Internet advertising systems in the amount of 3% of the income received from the sale of Internet advertising distribution services aimed at Russian customers.

Moreover, Russian advertisers will have to make a 3% deduction if they place advertising through foreign companies. The deductions must be withheld directly by the advertiser on the basis of the cost of services under a contract with a foreign advertising distributor. At the same time, mandatory deductions are not payable, for example, if advertising on their websites is distributed by TV or radio channels, news agencies, large print media, as well as media owned by state or municipal bodies or receiving state funding during the year. Roskomnadzor will determine the amount of deductions and monitor payment. Such innovations will increase the cost of advertising placement.

2. Advertising distributors (with more than 200,000 users per day), classifieds and aggregators of information about goods (services) (marketplaces) are obliged to distribute social advertising aimed at achieving charitable and other socially beneficial goals and ensuring the interests of the state, in the amount of 5% of all advertising distributed by them on the Internet in a year. Aggregators and classifieds may also distribute social advertising within the limits of 5% corresponding to the total number of users for the year, i.e. so that at least 5% of users from Russia viewed this advertising.

3. New rules are established for advertising on the extension of credits (loans). For example, an advertisement must contain the warning “Study all the terms and conditions of the loan (credit)” with a reference to the section of the creditor's official website where detailed terms and conditions affecting the full cost of a consumer loan are presented. If the advertisement contains information on interest rates, information on the full cost of the loan should also be available. In radio programs, the duration of the warning must be at least 3 seconds; in TV programs and in film and video services - at least 3 seconds and at least 5% of the frame area. The measure is aimed at reducing cases of impulsively taken retail loans without realizing the consequences and assessing the financial burden for the borrower and his family.

2. New penalties for leaking personal data

In December 2024, amendments were adopted to parts 12-17 of Article 13.11 of the Administrative Offenses Code to tighten sanctions for companies for personal data leakage.[2] Now for the first-time leak, the fine can reach Rb15 mn, but depends on the scale of the leak, for example: for the unlawful transfer of personal data from 1 to 10,000 people the fine can hit Rb 5 mn, from 10 to 100,000 people – Rb10 mn, and more than 100,000 people - up to Rb15 mn. In case of a repeated offense, the company will face a fine of 1 to 3% of annual revenue for the previous calendar year. Penalties are also introduced for the leakage of certain types of data, for example: sensitive data (such as health data) - a fine of up to Rb15 mn, biometric data - up to Rb20 mn. By toughening penalties for leaks, the government hopes to encourage companies to strengthen data protection measures in view of the growing number of cases of data misuse - in the first 10 months of 2024, Rb158 bn were stolen from Russians using personal contact data.[3]

3. Prohibition of forcing goods or services on consumers

In December 2024, a draft law (N 787328-8) was submitted to the State Duma prohibiting the forcing of additional goods (works, services) on consumers before the conclusion of a contract for the purchase of basic goods, including as a condition for the purchase of basic goods or services.[4] The prohibition applies to both sellers and aggregators (marketplaces). The sale of such goods or services must be made with the consumer’s written consent, and if the consumer was charged for additional goods or services, it must be refunded. In addition, it is prohibited to automatically mark the purchase of

[1] https://storage.consultant.ru/site20/202412/11/fz_111224-600974.pdf
[2] https://www.consultant.ru/document/cons_doc_LAW_491932/
[3] https://frankmedia.ru/187874?utm_referrer=https%3a%2f%2fwww.google.com%2f
[4] https://storage.consultant.ru/site20/202412/05/pr_fz_328.pdf

additional goods or services. In fact, the draft law is aimed at combating “dark” commercial patterns, for example, when marketplaces automatically add additional goods to a consumer's shopping cart without the consumer's knowledge.

Key aspects

1. Strengthening of AI regulation

December 2024 saw developments indicating increased regulation of AI in different countries: both those with specific laws for AI (Spain) and those operating under general regulations (USA).

The US experience

On December 3, 2024, the Federal Trade Commission published a draft consent order with U.S. company IntelliVision Technologies.[5] The company is prohibited from disseminating misrepresenting information about the accuracy and efficacy of its AI software (used in home security systems and smart home touch panels) for facial recognition, as well as its performance across individuals with different genders, ethnicities, and skin tones.

The FTC alleges that the company did not have evidence to support its claims that its software is highly accurate and unbiased, and that its anti-spoofing technology ensures the system can't be tricked by a photo or video image. For example, according to the National Institute of Standards and Technology's 2019-2023 testing results, the error rate of the company's technology's algorithms varies depending on demographic characteristics, including a person's region of birth.[6] The company also trained the AI on a meaningfully smaller number of images than it claimed. Meanwhile, AI developers and service providers are subject to general principles regarding unfair advertising. If the agreement is finally adopted, its violation threatens the company with a fine of more than $51,000.

This is the second major AI facial recognition case brought by the FTC in a year. In December 2023, Rite Aid will be prohibited from using facial recognition technology for surveillance purposes for five years to settle the charges that the retailer failed to implement comprehensive safeguards that resulted in the surveillance technology mistakenly identifying people, especially women and dark-skinned people, as shoplifters.[7]

Experience of Spain

On December 4, 2024, Organic Law 5/2024 on the right to protection[8] in the use of AI and other technologies in the provision of legal services entered into force in Spain. Monitoring No. 7 has already raised the issue of the use of AI in courts.

Spain establishes the right of a person to be informed in a clear, simple, understandable and publicly accessible form about how digital platforms use artificial intelligence to make recommendations and decisions in legal services. For example, how AI is used to select lawyers and law firms.

Experience of Brazil

On December 10, 2024, the Brazilian Senate passed a law regulating the use of AI.[9] The definition of AI system in this document is in line with the OECD definition updated in March (see Monitoring No. 3).

The Law borrows from the approach implemented in the EU AI Act[10] adopted in June (also analyzed in Monitoring No. 3): regulation is based on the level of risk of AI systems: the higher the risk, the higher the requirements for the development and use of the system. The Brazilian law identifies the same risk-based categories of AI as in the EU:

1) Prohibited AI systems with excessive risk.

2) Authorized high-risk AI systems.

3) General-purpose AI systems, among which generative AI and AI with systemic, i.e. potentially large-scale risk are identified.

At the same time, the composition of prohibited systems differs: Brazil includes in this category the distribution of materials on the exploitation of minors, which is more of a criminal offense, but does not include the expansion of facial recognition systems based on images from the Internet and the detection of emotions in education and work (which is categorized as high-risk). The composition of high-risk AI systems in Brazil is expected to be

[5] https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-intellivision-technologies-deceptive-claims-about-its-facial-recognition
[6] https://www.ftc.gov/system/files/ftc_gov/pdf/Complaint-IntellivisionTechCorp.pdf
[7] https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without
[8] https://www.boe.es/buscar/doc.php?id=BOE-A-2024-23630
[9] https://www25.senado.leg.br/web/atividade/materias/-/materia/157233; https://legis.senado.leg.br/sdleg-getter/documento?dm=9881643&ts=1735605226813&disposition=inline
[10] AI Act; https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

clarified at the bylaw level, the law contains examples: security, medicine, courts, etc., but the law does not include the expansion of facial recognition systems based on images from the Internet and emotion detection in education and work (which is categorized as high-risk).

The law establishes the right of everybody to be informed about their interaction with an AI system, including automated systems. For high-risk AI systems, the rights to clarification, to challenge the system's decisions and to have them reviewed by a human being are additionally provided for.

The requirements for developers of high-risk AI systems in Brazil are also higher than general-purpose AI: for example, its accuracy assessment and safety tests are required. At the same time, the requirements are more lenient and framework-based compared to the EU. For example, risk assessment, mitigation measures and evaluation of their effectiveness are required for high-risk AI, but the assessment procedure (criteria, frequency) is not defined.

Russia's experience

In Russia, currently legislative regulation of AI use is carried out only through experimental legal regimes.[11]

2. Anti-competitive practices online

Experience of China

In December 2024, China's State Administration of Market Regulation (SAMR) opened an investigation against U.S. GPU maker Nvidia for violating the acquisition terms of Mellanox Technologies[12] for more than $6.9 bn, which SAMR authorized in 2020.[13] Information on the exact reasons for the charge has not been released, but back when this deal was approved in 2020. SAMR identified that the merger could impact the global and Chinese market for GPUs, private network interconnect equipment and high-speed Ethernet adapters. SAMR has therefore approved the transaction subject to the following conditions:

1) Unreasonable trade restrictions should not be imposed on the sale of GPUs and high-speed networking equipment on the Chinese market, and the market should be supplied on the basis of fairness and non-discrimination.

2) Compatibility of NVIDIA GPUs, as well as Milos high-speed networking devices must be ensured with products from competing manufacturers, including Chinese manufacturers.

3) The open originating software code for peer-to-peer and aggregated communications for the Milos High Speed Network Interconnect Appliance must be maintained so that other vendors can support interoperability of the appliances.

Experience of South Korea

South Korea's Fair Trade Commission (KFTC)[14] has fined Kakao Mobility and its subsidiary the taxi-hailing services KakaoT for $10.2 mn.

On the cab market, Kakao offers general taxi-hailing services (as an aggregator, similar to Yandes.Taxi) and specialized taxi-hailing services under the franchise of its subsidiary Kakao T Blue (for example, Uber and TADA operated under the franchise). It was revealed that from 2019, the company, in order to exclude competing taxi operators working under the Kakao franchise, began blocking taxi bookings for drivers who work for rival companies. The company reasoned that taxi calls were being duplicated on multiple platforms, on Kakao and those of competing operators, creating confusion for passengers. Kakao therefore required the 4 competing franchised taxi operators to pay their drivers a commission for using Kakao, or the company needs to sign a partnership agreement with Kakao. This allowed Kakao Mobility to collect information including trade secrets of its competing franchisees, data on users, cab drivers, and trips.

The KFTC considered that on the one hand, Kakao Mobility entered into such contracts and collected confidential information for its own business strategy, for example, Kakao could manipulate the platform's algorithms to prioritize franchised taxis over non-franchised taxis. This allowed Kakao Mobility to hold a dominant position.

On the other hand, a competing franchised taxi operator is forced to enter into a

[11] Federal Law No. 258-FZ entered into force in January 2025.

[12] Mellanox Technologies, Ltd. - Israeli technology company, engaged in the research, development, manufacture and sale of network interconnect products. It plays an important role in the field of data centers, cloud computing and high-performance computing.

[13] https://www.samr.gov.cn/xw/zj/art/2024/art_ed4d3090401741a0894e475d35db652b.html

[14] https://www.ftc.go.kr/solution/skin/doc.html?fn=57268d4f18a446a6b4ea5843906b414815572d0e5005faeb9533f07a681436c6&rs=/fileupload/data/result//news/report/2024/

partnership agreement or else it will not be able to receive taxi call information from Kakao Mobility, which has a market share of over 50%. KFTC estimates that Kakao Mobility's practices have led to an increase in its market share from 51% in 2020 to 79% in 2022.

Experience of Italy

In December 2024, the Italian National Authority for Market and Competition[15] published the results of an investigation into the use of dynamic pricing algorithms in passenger air transport on domestic routes to and from Sicily and Sardinia.

Airlines use dynamic pricing algorithms - when prices for the same service (or product) change based on demand and other information. The frequency of price adjustments can vary for each individual transaction, including depending on the data available to the airline. Dynamic pricing can lead to price discrimination,[16] where a monopolistic company offers different prices for the same goods or services to different consumers or groups of consumers in order to make more profit. The companies processed information on the number of bookings, load factor, flight occupancy rate, previous booking trends on the same flight, route, departure dates, number of days before departure, etc.

Information on market structure and trends was also analyzed, such as the market shares held by competitors and their prices. To obtain such information, all companies used the same Infare platform that releases publicly available information on competitors' flight prices. However, such data was rarely used to determine prices for each flight but was necessary for the companies' analysts for comparative analysis and assessment of their own position on the market.

The Competition and Market Authority concluded that the information collected, including from competitors, is not used for price discrimination. Changes in airfares are mainly influenced by trends in actual and expected demand estimated based on historical booking data for the same flight or using forecasting models, for example, if actual demand is higher than expected demand or the occupancy rate of a flight is also higher than the expected rate, the system determines a shift to higher fare classes.

The Authority for Competition and Market concluded that the collected information, including from competitors, is not used for price discrimination. Changes in airfares are mainly influenced by trends in actual and expected demand estimated on the basis of recent booking data for the same flight or using forecasting models, e.g., if actual demand is higher than expected demand, or the occupancy rate of a flight is also higher than the expected rate, the system determines a shift to higher fare classes.

It is also revealed that airlines use in the mechanism of price dynamization a classical system of fare formation due to a predetermined fare grid, within which the price of each flight varies over time, opening and closing orders for each predetermined price class randomly, although based on the data collected by the companies, the distribution of the number of seats in each fare class can occur.

Nevertheless, no evidence of discrimination was found regardless of the type of device used to purchase tickets or the operating system used to search for tickets. Although one company was found to change its pricing policy when the same user logs in repeatedly, or when logging in to an airline's website via a flight aggregator (like Google Flights). As browsing history or information about other user activities is accumulated, the user may be offered a personalized price (rather than a randomly generated price within the fare grid), but more often than not it was a price “frozen” for the user, which does not change up or down, for example, each time the user browses the prices again, which also does not cause price discrimination.

Russia’s experience

In November 2024, FAS and the Ministry of Transport released a joint statement[17] attempting to regulate airfares. Airlines were recommended to describe approaches to the pricing of passenger transportation in economy class, including the methodology for determining minimum, maximum and intermediate fares with

[15] https://digitalpolicyalert.org/change/12154-competition-and-market-authority-investigation-into-the-use-of-pricing-algorithms-in-passenger-air-transport-on-domestic-routes-between-sicily-and-sardinia

[16] The following types of discrimination are identified:
1) First-degree discrimination - each item is offered at a different price depending on the profile of the individual consumer.
2) Second-degree discrimination - discounts, preferential rates, etc.
3) Third degree discrimination - offer different prices for different groups of customers depending on their willingness to pay.

[17] https://t.me/fasrussia/3984

justification of the method of their pricing. It is also proposed to increase the range of fare groups with a detailed description of each of them, to work out approaches to the implementation of sales and price reduction measures. Such measures should increase the transparency of passenger air transportation pricing.

3. Protection of consumers online

The number of consumers purchasing goods and services online including digital ones increased from 2.14 billion to 2.71 billion over 2021-2024. Around 20.1% of retail sales are made online.[18] In the EU in 2023, 70% of 16-74 year-olds purchased goods and services online.[19] Questions arise about the safety of goods and services purchased online.

The EU experience

As of December 2024, the EU Regulation 2023/988 on common product safety requirements[20] for digital and remotely marketed products and platforms selling such products has been in force. Any products are covered, except those subject to special regulation such as medicines.

Cybersecurity has been added to the list of features by which product safety is assessed. Thus, a digital product (such as a computer program or mobile application) cannot be considered safe and sold on platforms if it is not protected from malicious interference in its operation by third parties or may harm the health of users (e.g., drug advertisements in computer games).

Products producers and importers are obligated to inform platforms about:

1) Any product safety issues (e.g., the product can emit harmful substances when heated).

2) The results of investigations into incidents and consumer complaints regarding the safety of imported products (e.g. when a non-EU purchaser of utensils complained about their release of harmful substances during cooking). The Regulation requires online sales offers for a product to contain information on its safety in a consumer-friendly manner.

Platforms, on the other hand, are obligated:

1) To ensure direct communication on product safety issues with supervisory authorities and consumers and process reports from them within 2-3 working days.

2) To regularly monitor products placed on the site using information from the Safety Gate Portal platform[21] created by the European Commission, to take voluntary measures to block/remove content related to the offer of unsafe products and to inform the supervisory authorities about them in accordance with the orders of the supervisory authorities.

3) To restrict access to vendors who repeatedly offer unsafe products.

4) To notify consumers who have purchased a product on the site that has been withdrawn from the marketplace due to unsafety.

Russia's experience

In Russia, the Law on Consumer Rights Protection (Article 7) establishes the consumer's right to safety of goods and services, but the requirements to ensure it are specified only for food products. There is no special regulation for goods purchased online, including digital products.[22] At the same time, the owner of an aggregator that has provided the consumer with inaccurate/incomplete information about the product/service is not liable to the consumer if it does not change the information provided by the seller (clause 2.1 of Article 12).

Also, Russia does not participate in international systems of information exchange on unsafe goods, such as the OECD Global Recalls system.[23]

[18] https://www.statista.com

[19] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-commerce_statistics_for_individuals

[20] Regulation 2023/988 on general product safety; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32023R0988

[21] A rapid notification system for dangerous non-food products. An information-sharing system where government agencies share information about products identified as unsafe so that other jurisdictions can remove such products from the marketplace.

[22] Order of Rospotrebnadzor of 18.01.2016 No. 16.

[23] Global Recalls contains consumer product recall information from 47 jurisdictions, as well as recall information from the EU (Safety Gate) and ASEAN (Product Alert) regional portals.