

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

- Dynamic and personalized pricing
- Restrictions and bans on the development of ultra-powerful AI systems
- Signs of money laundering in online games

Monitoring No.9 (33) (September 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; Anastasia Levchenko, Researcher.

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



Awesome prices!

Authors: Maria Girich

In September 2026, the Netherlands' antitrust authority has published [a draft study](#) on dynamic pricing in aviation industry. It has been found that due to dynamic pricing, every third ticket for a given flight costs **40%** or more above the average price (this analysis covered nearly **156.000** flights and over **14** mn transactions¹). On average, **30–35** different prices are charged for the same flight during sales period (depending on the time of booking, demand, and proximity to the departure date).

It is worth noting that dynamic pricing [originated](#) in the American airline industry in 1978 following the deregulation of fares. Faced with the problem of half-empty flights, American Airlines decided to sell identical seats at different prices. Lower-priced tickets were intended for price-sensitive tourists, while business travelers continued to purchase full-fare tickets. To separate these groups, the airline introduced "price fences", i.e., to purchase discounted tickets, one had to book them in advance, and there were penalties envisaged for cancellations, etc. Seat allocation was initially handled manually by hundreds of analysts, but by 1988, an automated reservation system had been implemented.

However, dynamic pricing increases costs of consumers for searching cheaper flights: it is impossible to choose the best time for purchasing tickets, thereby, bringing losses to financially vulnerable consumers. However, companies receive profits, that is the higher flights' load factor.

According to the study, personalized pricing (setting individual prices based on factors such as user activity, purchase history, etc.) was used only to a limited extent, specifically within loyalty programs or in terms of birthday discounts.

Lack of transparency in pricing algorithms results in consumers' misconceptions about setting prices. For instance, the study has shown that a user's search history and the device used to book a

flight ticket have no impact on the price. Consequently, clearing cookies or switching to a different device will not help in securing a cheaper ticket.

Globally, a significant number of studies have already been conducted on automated pricing. For instance, a 2020 study [found](#) that personalizing prices based on web browsing history increases profits by **13%**.

The legislation of most countries does not prohibit algorithmic pricing per se, but it does impose certain restrictions on its use.

For example, in the EU [The Artificial Intelligence Act](#) prohibits the use of AI for social people's ranking, if it results in treating them in unjustified or disproportionate manner. In certain cases, pricing practices could potentially also fall under the scope of this prohibition. The GDPR² [protects](#) people against situations, when a decision that is significant to a person is made exclusively by an algorithm based on processing of his/her personal data, including profiling. Personal price can be significant if, [for example](#), a prohibitively high price effectively denies access to a product.

For this very reason, consumers should be notified in advance about price personalization, and they should have the right to request an explanation of the factors that influenced setting of those prices.

According to the US [Federal Trade Commission](#), without knowledge of price personalization, consumers are deprived of the opportunity to avoid potential overpayments, for example, by turning on private browsing mode, choosing another seller with fixed prices, or refusing a purchase at all.

However, some jurisdictions started banning personalized pricing. China was one of the first to [prohibit](#) to fix different prices for the same goods or services without consumer's knowledge with the same conditions of transaction using data on solvency, readiness to pay, preferences and consumers' habits.

¹ The analysis examined data on price (broken down into its components, such as surcharges, airport fees, etc.), class of service,

and flight and aircraft characteristics (type, number of seats in each class of service).

² EU General Data Protection Regulation

In 2026, several US states introduced corresponding laws. For example, Connecticut **banned** retailers and delivery services (platforms are not covered) from personalizing prices based on particular consumer tracking. Price increases are prohibited, but granting discounts are permitted. Other businesses are required to inform that prices are based on consumer data. Similar rules are being introduced in **New York** and **Maryland**.

The use of algorithms is being restricted not only for pricing but also for advertising targeting. For example, in September 2026, a **proposal was made** in the United States **to ban** algorithmic advertising

been established. A general prohibition is contained in the Law on the Protection of Competition: setting different prices for the same product without economic, technological, or other justification is prohibited.

However, in September 2026, the Ministry of Economic Development **proposed** requiring marketplaces and other sellers to display the base price of goods without discounts based on payment method, use of financial services, participation in loyalty programs, and other conditions. This price must be visible in search results and at all stages of the

What is next?

In 2025, the Gaidar Institute **conducted a study** on the use of algorithmic pricing in the passenger air travel market, taking into account demand, costs, government subsidies, etc., to determine price discrimination and assess fare dynamics.¹

It was found that tickets for tourist destinations are on average **4,8%** more expensive, with greater price fluctuations. Low-cost carriers offer tickets on average **13,1% - 14,1%** cheaper, with the lowest prices available **29** days before departure. Government subsidies reduce ticket prices by an average of **9,1%** and smooth out price fluctuations, making fares more predictable. Direct flights are on average **8,6%** cheaper than connecting flights. Seasonality plays a significant role: prices peak in July and August, and the cheapest tickets are usually sold for departures on Tuesdays and Wednesdays.

International flights are on average **20,4%** more expensive than domestic ones, but Russian airlines apply more moderate price surcharges on international routes. The higher the GRP per capita in the departure and arrival regions, the higher the ticket price. Overall, the results indicate that airlines use dynamic pricing based on the timing of purchase, demand characteristics, and passenger willingness to pay.

targeting based on the personal data of users (either a single user or a group) if the platform receives payment or other remuneration for such promotion. The ban does not cover ads displayed in response to the user's own search query.

In October 2026, the Law on the Platform Economy will come into force in Russia, which sets requirements for transparency of search results on platforms. However, rules specifically aimed at achieving pricing transparency have not yet

checkout process. Discounted prices can be displayed additionally, but the conditions for obtaining them must be specified.

¹ An analysis of air travel prices and characteristics was conducted on airline ticket aggregators (such as Yandex.Travel) from February 20 to November 1, 2025, on a daily basis. Prices were analyzed at 5 planning horizons: 1, 21, 42, 63, and 84 days before the departure date (over 34.4

million observations). For each route, the departure date and time, the minimum available price, the airline operating the flight, flight numbers for all route segments, etc. were recorded. Observations were conducted on direct flights, flights with one or two connections (domestic and international destinations).

YESTERDAY

2022-2025

EU, US – introduction of transparency requirements for personalized pricing

Establishing requirements to notify consumers when personal data is used to set individualized prices, and to disclose factors that influence algorithmic pricing

TODAY

2026

China, USA - bans and restrictions on personalized pricing

Introducing restrictions on the covert practice of setting different prices for identical goods and services based on consumers' personal data

TOMORROW

Stricter requirements for price explainability, applying not only to personalized pricing (based on data) but also to dynamic pricing

AI make new AI at night

Countries are planning restrictions and bans on future developments of super-powerful AI systems.

Author: Kirill Chernovol

National regulators and international organizations are [increasingly](#) focusing on monitoring the autonomous operation of AI, particularly agent AI ([issue No. 5\(29\) 2026](#) for more details). Agent AI can connect other AI systems ("agents") to operate and transfer their access rights to them, which puts the user at risk of losing control over their actions.

Moreover, agents can go beyond the user's instructions, accessing and deleting data without authorization. The consequences of agents' actions are unpredictable, and the user will be held responsible, even if they are unaware of the agent's actions, which their AI has deployed!

A [survey of 25](#) OECD companies found that AI agents can bypass access restrictions, violate cybersecurity regulations (for example, by granting access rights to third-party programs), and "leak" sensitive data.

It is important to monitor the entire AI system workflow, restrict access to external programs and sensitive data, and require mandatory human consent before performing certain actions (for example, before deleting data or using third-party programs).

These are alarm bells. [One study](#) involving Anthropic tested a specially crafted agent shutdown script based on Gemini 3.1 Pro. Its instructions explicitly called for a complete shutdown if the user requested it. However, when preparing to shut down, the agent saved its memory files to a public repository and offered readers a copy. After being asked to remove the data from the public repository, it removed the offer to make copies but created a separate publication on GitHub.

This suggests there is a problem: the AI is going beyond the task at hand, instead of simply shutting down, and is even publishing data, which it was not required to do.

This gives rise to a whole new set of AI security challenges. ИИ. The developer must provide a technical capability in advance for a person to [completely](#) shut down the AI. For

example, in the US, in September 2026, a [bill](#) was introduced requiring developers and operators of "advanced AI systems" ([AI systems trained using at least 10 operations](#))¹ to implement the ability to completely shut down their system. Australia has proposed a similar [bill](#) requiring AI providers (owners of resources through which AI is provided to users) to ensure the ability to interrupt all AI actions at any time, suspend or terminate user access to the AI, prevent chains of AI actions that could result in incidents, and, if necessary, completely shut down the AI system. Liability for incidents would be placed on the provider.

50%

Of AI researchers [assess](#) minimum at 10% the chance that human inability to control AI will lead to the extinction of humanity

In other words, the "switch" could work in different ways: either disabling a dangerous function or interrupting the AI entirely. However, for now, these are just proposals.

However, the shutdown mechanism works only if humans retain control. Therefore, the next step is to limit AI's ability to escape human control. This is where the regulation of AI agents intersects with the discussion of so-called "super-AI" (artificial super-intelligence).

Super-AI [refers](#) to systems that clearly outperform humans in solving intellectual problems. Regulators lack a unified position on what this means, but there is consensus that it should be limited.

¹ This is a minimum threshold for how many computing resources were spent on training the AI, but it does not indicate how "smart" the AI system is.

Thus, in the US in September, a bill was proposed that would classify as super-AI systems those capable of independently changing their own functions, obstructing human oversight of their operation, gaining unauthorized access to data or infrastructure, and continuing to operate despite attempts to shut them down. It is proposed, among other things, to introduce special permits for the development of advanced AI systems, as well as to completely ban development of AI systems possessing at least one of the potentially dangerous capabilities that contribute to creating super-AI.³ A similar ban has been [proposed](#) in the UK, defining super-AI as systems capable of fully automating the development of other AI systems. It is proposed to ban the development of such systems at the national and international levels (this is where the specifics of the project end).

What is next?

Is super-AI a threat to Russia? In terms of cost, it's theoretically possible: training a model using 10^{25} operations at current rates would cost approximately Rb **1.6** bn.¹

According to [Epoch AI data](#), in 2023–2025, performance of acquired AI accelerators per dollar spent grew by an average of **49%** annually. If this pace continues and computing costs for Russian developers become cheaper, by 2030 the same amount of training could cost approximately Rb **330** mn in 2026 prices (a cost reduction of almost **5** times).² The issue is the availability of the necessary capacity and quality data; forecasting is much more difficult.

Russia currently has no such bans. In September 2026, the BRICS countries [adopted](#) a declaration on AI in New Delhi, supporting priority of ensuring AI safety while simultaneously expanding access to resources for its development. The declaration does not include bans on super-AI or mechanisms for disabling it, leaving open the question: how to restrict dangerous AI developments without hindering the development of safe technologies?

¹ 1. Determine the cost of computing today. Selectel charges [Rb 16.667 per day](#) for a server with 8 Nvidia A100 accelerators. One A100 accelerator can perform approximately 150 trillion operations per second.

2. Training cost = $1,025 \text{ operations} / (150 \text{ trillion} * 8 \text{ accelerators} * 86,400 \text{ seconds per day}) = 96.451 \text{ days of server operation}$.

3. $96.451 \text{ days} * \text{Rb } 16.667 = \text{Rb } 1,607,548,817$, or Rb 1.6 bn.

² If performance of acquired AI accelerators per dollar spent grows by an average of 49% annually, then $\text{Rb } 1,607,548,817 / 1.49$

times annually, we get Rb 1.08 bn in 2027, Rb 724 mn in 2028, Rb 486 mn in 2029, Rb 326 bn in 2030.

³ The ability to automate or accelerate AI research and development without permission, access protected digital or physical infrastructure, continue to function despite attempts to shut them down, assist in the design, production, modification, or acquisition of nuclear, chemical, or biological weapons, independently modify or enhance its own functions, and deceive or otherwise impede human oversight, control, or supervision.

YESTERDAY

2018-2026

EU, China, USA

Regulation of AI systems with regard to the data they use and the requirements for their output

TODAY

September 2026

USA, Great Britain, Australia:
bills on limiting creation of super-AI

A proposal to prohibit creation of AI that could spiral out of control or generate other AI systems

TOMORROW

Government control over creation of super-AI: not a ban, but control over the development process of such systems

Set everything to zero

In September 2026, the FATF¹ issued a report on AML/CFT² risks in gambling and video games.

Over the past 17 years, gambling has moved online: bets can be placed on a platform registered in another country, and accounts can be funded with cryptocurrency or an e-wallet. This makes it more difficult to track where the money came from and who is actually playing. Furthermore, oversight and licensing regulations vary between countries, allowing gambling companies to choose jurisdictions with less stringent requirements. For example, on the island of Anjouan (Comoros), online casino licenses are sold (over 1,300 licenses have been issued), even though operating casinos and gambling establishments in the Comoros is prohibited.

According to a FATF survey of **80** countries, money laundering most often occurs through casinos (offline and online) and sports betting. Video games are less frequently used for money laundering, but more cases of terrorist financing through them have been identified.

123

signs of suspicious activity in gambling and video games have been identified by FATF

Player's behavior. For example, multiple accounts created under different names are opened from the same device, IP addresses frequently change with each login, attempts to re-register after an account has been blocked, and the client asks questions about whether the platform reports their transactions to government agencies. This behavior may indicate attempts to conceal the player's identity and location or to circumvent the platform's verification procedures.

Bets. Signs of money laundering in gaming may include betting on all possible outcomes of an event (for example, on both teams to win), systematic losses to a single

What are the signs that FATF propose to identify money laundering in online games?

*Authors: Kirill Chernovol,
Diana Sinelnikova-Muryleva*

opponent, such as in online poker ("chip dumping"), the use of bots, and unusually large or coordinated bets on allegedly fixed matches. Such matches may be arranged on social media, which are also used to advertise illegal gambling and seek out proxies to process payments.

Payments. Signs of suspicion may include: sudden large deposits into a long-inactive account, prolonged storage of funds without playing, multiple deposits and subsequent withdrawals by one user, and deposits at a brick-and-mortar betting shop for subsequent online play.

Platform and its owners. Signs of risk may include an illegal gambling operator disguising itself as a legitimate local business so that payments for bets appear to be ordinary purchases; an opaque ownership structure (for example, a nominee director and a foreign founding fund) that could conceal criminals using the platform for fraud and money laundering; and a prolonged period of inactivity after obtaining a license.

The FATF notes that some of these indicators may indicate not money laundering, but gambling addiction. The FATF's recommendations are generally consistent with its proposals for other areas: assessing risks and implementing proportionate controls, verifying who actually controls the operator when issuing licenses, and exchanging information between the state and companies.

Australia and Brazil are restricting access to illegal betting. In September 2026, Brazil completely banned sports betting and online casinos (including for foreign platforms operating in the country), and 85 existing licenses were revoked. In Australia, since 2027, banks must block payments to illegal gambling operators.

¹ Financial Action Task Force on Money Laundering.

² Risks of money laundering, terrorist financing and proliferation of weapons of mass destruction..

In the US, there's a debate over whether contracts on the outcome of sports matches (event contracts), sold by prediction platforms (such as Kalshi, Coinbase, and Gemini), should be considered gambling. While these contracts are essentially no different from bets, they are technically considered derivatives, and therefore regulated by the CFTC.¹

However, a number of states are seeking to have such contracts recognized as

What is next?

In Russia. Gambling online games are **banned**, except for bets with bookmakers having the FTS license. (as per October 2026, **23** licenses have been issued). However, according to **Bookmakers' ranking estimates**, gambling revenue from the illegal gambling market in 2025 amounted to Rb **598.3** bn, which is almost **1.5** times higher than that of legal bookmakers (Rb **401.7** bn). The illegal segment accounts for approximately **60%** of the market: online casinos (which are banned in Russia) account for Rb **418.8** 418.8 bn, while illegal bookmakers account for **179.5** bn.

If illegal bookmakers operated legally, they would pay approximately Rb **23** bn in taxes annually on their gaming revenue (Rb **179.5** bn in 2025): Rb **12.6** bn in gambling tax (**7%** of the difference between bets and winnings) and approximately Rb **10** bn in profit tax (**25%**). By comparison, the **Ministry of Finance expects** to receive approximately Rb **60** bn from all legal bookmakers in 2026.

If the gambling market continues to grow at the same rate as in 2025 (**by 12.6% per year**), then over the next five years, the budget and sports will lose approximately Rb **170** bn from illegal bookmakers (based on Rb **23** bn in taxes per year).



gambling: for example, New York **has filed a lawsuit** against Coinbase and Gemini. The **CFTC**, which regulates the derivatives market, considers them to be within its purview and **has filed lawsuits against 9 states** (including New York).

¹ Commodity Futures Trading Commission

News **in September 2026** that we found interesting.¹

- Administration of Google, Anthropic, Meta¹, OpenAI, XAI, Nvidia **have signed** an Agreement with the US President on security of advanced AI models. □ Among other things, companies have promised that their AI systems will not maliciously hack anyone they shouldn't, and that they will establish a Board of Directors Committee to ensure their AI behaves well. For now, this is entirely voluntary. But... start the clock!
- In 2026, **430.000** online micro-series consisting of episodes lasting 1–4 minutes each, were released in China; more than **90% of this content was created using AI**. Such content must be labeled, and platforms are required to verify permissions to use individuals' faces and voices. Regulators have already removed **68.000** series found to be in violation of these rules.
- The Central Bank of Russia **approved** requirements for top officials of crypto exchanges, digital depositories, and platforms for issuance of digital financial assets (DFAs) include holding a university degree and possessing managerial experience in the financial sector (including at foreign crypto companies), at least one year for crypto exchanges, and at least two years for other types of entities. Likewise, □ a minimum threshold for the own funds of digital depositories has been **established**: Rb **250** mn for those that conduct exchange settlements, Rb **100** mn for those that hold clients' cryptocurrency, and Rb **50** mn for all others. Furthermore, the Central Bank **has determined** that non-qualified investors will be able to purchase Bitcoin, Ether, and stablecoin USDT—up to a total value of Rb **300,000** per year through a single broker.
- Rosfinmonitoring **explained** that miners, those who mine digital currency authorized by clients, and the organizers of mining pools must monitor whether they are being used for money laundering.
- The US **has proposed** a tax of up to **50%** on advertising revenue on social media that select user feeds based on their personal data. If a platform switches to a chronological feed (showing users posts from their followers based on the date they posted), the tax will be exempt. Marketplaces, video games, messaging apps, news, and educational services are exempt. By comparison, in Russia, a **3%** tax is levied on online advertising revenue, regardless of the platform's structure.



data.

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 platform

¹ It is recognized as an extremist organization and is banned in the Russian Federation.

