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

Establishing the legal status of cryptoassets as securities, violation of consumer rights on the Internet, balancing private and public interests in content moderation, liberalization of cross-border data flows, banning social media for children

Monitoring No.11 (November 2024)

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.
Tatiana Malinina, Senior Researcher, International Best Practices Analysis Department, Gaidar Institute

"The fog was falling on the fields,
A caravan of shrieking geese
Was pulling southward: approached
A rather dull time;
November was in the air."
Alexander Pushkin

In November 2024, we can identify 5 events that define trends in the development of digital economy regulation in the world.

Trend No. 1. Establishing the legal status of cryptoassets as securities

In November 2024, a dispute that began back in the late 2010s over whether cryptoassets can be considered securities intensified in the United States. Eighteen states have filed a lawsuit against the Securities and Exchange Commission. The suit seeks to remove sales of digital assets from securities regulation. However, previous court rulings supported the Commission's position.

Trend No. 2. Violation of consumer rights on the internet

In November 2024, investigations into unlawful practices of major platforms against consumers were launched in the US, EU countries, and South Korea. This affected such companies as Sitejabber, Apple, Temu, and AliExpress in the wake of publishing false consumer reviews on the platforms, setting up geo-blocking of access to platform services, and selling unsafe products.

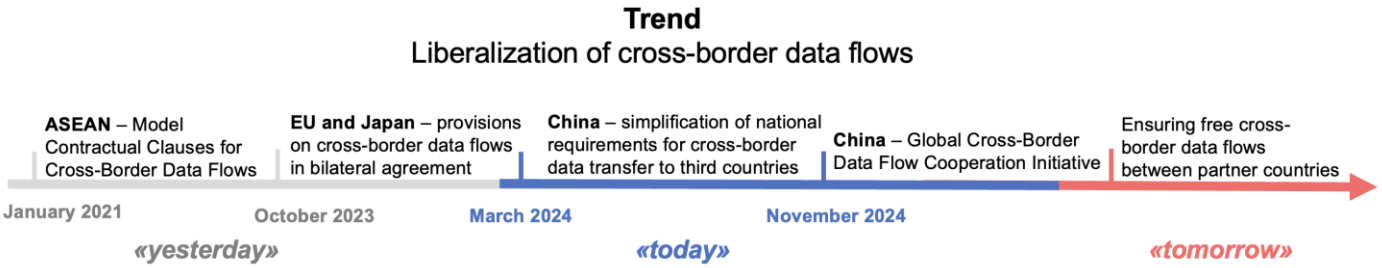
Trend No. 3. Balancing private and public interests in content moderation

In November 2024, many countries took measures to tighten the requirements for online content moderation: the EU adopted Implementing Regulation to the Digital Services Act specifying the procedure for online platforms to report on content moderation, and South Korea created mechanisms for cooperation between the authorities and Telegram to control the distribution of illegal content. Russia introduced a ban on childfree propaganda.

Meanwhile, in the US, X (Twitter) Corp. is trying to fight the trend by challenging the constitutionality of California Assembly Bill passed in 2024 requiring online platforms to remove or label materially deceptive content regarding elections.

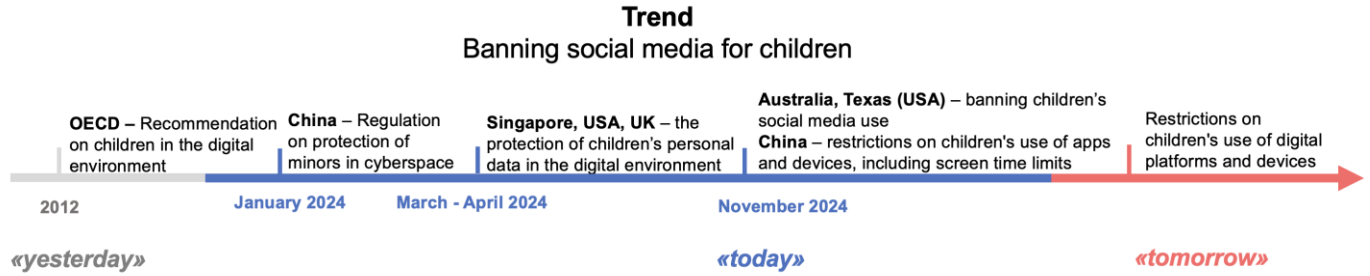
Trend No. 4. Liberalization of cross-border data flows

In November 2024, at the APEC summit,[1] China announced the Global Cross-Border Data Flow Cooperation Initiative to facilitate data transfer between countries.



Trend No. 5. Banning social media for children

In November 2024, regulations have been proposed in Australia, the United States (Texas) and China to restrict children's access to digital platforms, including social media.



November 2024 also saw a few significant developments in the regulation of the digital economy in Russia.

1. Regulation of the digital platform economy

The Platform Economy draft law was published in November 2024:[2]

1) Regulates “intermediary platforms” that provide interaction between “partners” and “users” (buyers) for the conclusion of civil law contracts, including the possibility of placing orders or product cards, making transactions, and making payments. By “partner” are meant sellers, order delivery points, service providers. In fact, the bill regulates marketplaces such as Ozon or Wildberries. The bill also regulates employment platforms where the partner-executor is not subject to the rules of internal labor regulations, independently determines the time and place of acceptance or execution of orders, has the right to refuse to perform work without sanctions, etc. (i.e., officially formalized employment platforms). (i.e. there are no officially formalized labor relations). This can include both cab platforms (Yandex.Taxi), couriers (Yandex.Food, Cooper), and classifieds (like Avito). Although, for example, Yandex.Taxi introduces sanctions for refusing an order - the taxi driver's rating is lowered, which raises the question of whether there are labor relations in the interaction between Yandex.Taxi and the taxi driver.

2) Platforms should be registered in a special registry (criteria will be developed).

[1] Asia-Pacific Economic Cooperation
[2] https://storage.consultant.ru/site20/202411/25/fz_251124-platform.rtf

3) The terms and conditions of concluding a contract with the platform are regulated: it must verify the accuracy of information about the partner through State Services, or USRLE/IP.[3]

4) Regulates the placement of a product card on a marketplace, including the placement of information about labels and certificates, and information that the platform is not the seller of the goods sold by the partner. This is an important measure that allows the consumer to understand who the seller is: the marketplace or the partner.

5) Regulation of discounts. If a marketplace intends to introduce a discount (both at its own expense and at the expense of the partner), it is necessary to get the partner's consent at least 14 days in advance. Partner's silence in response to the offer does not constitute consent.

6) The platform is allowed to change the contract after giving at least 15 days' notice to the partners.

7) Employment platforms are regulated, including the right of the contractor to information about the order. Platforms will have to control the time, acceptable standards of lifting and moving loads, restrictions on unacceptable work for minors, etc. The right of platforms to participate in social insurance of the self-employed is established.

The draft law also provides for the regulation of the terms of access to the personal account on a platform, the procedure for handling complaints, and the regulation of ratings, including requirements for the disclosure of information on the formation of ratings and the principles of ranking information (for example, a product card) in the platform's search engine. In addition, platforms should participate in the exchange of information with the Federal Tax Service.

The draft law regulates any type of platform. On the one hand, it mixes different types of legal relations: quasi-labor relations with performers, and between sellers and marketplaces, which can create difficulties in its application. On the other hand, the law covers regulation characteristic of all types of platforms - their rules of use, procedures, minimum requirements to protect users. Such norms can be applied to any platform without considering it specific features.

2. New criminal article in case of personal data leakage

In November, amendments were made to the Criminal Code of the Russian Federation, which criminalized the illegal use of personal data obtained in the wake of their leakage (Art. 272.1).[4] The introduction of the article is due to the need to counteract the wave of crimes involving personal data. According to the statistics of 2023, 83% of the population in Russia experienced fraud by phone or messengers (i.e., schemes using contact personal data), resulting in the theft of Rb14.2 bn.

The new article will allow prosecution of those who illegally collect and process personal data. However, the challenge of criminalizing the unlawful storage of personal data is that other actors in the common digital space with fraudsters can be drawn into crimes without their knowledge - for example, if a cloud provider supplies computing capacity for data storage, it cannot technically control the legality of the data source, although from a formal-legal point of view it may fall under the corpus delicti of “storage of data obtained unlawfully”.

[3] Uniform State Register of Legal Entities, Unified State Register of Individual Entrepreneurs.
[4] http://publication.pravo.gov.ru/document/0001202411300012?index=2

Key aspects

1. Establishing the legal status of cryptoassets as securities

In November 2024, a dispute over the nature of digital assets, particularly cryptocurrencies, intensified in the US – are they securities? Eighteen states[5] have filed a lawsuit against the Securities and Exchange Commission (SEC). Those who filed the lawsuit believe that digital assets, especially when sold on a secondary market (e.g., a cryptoexchange), do not fall under the SEC's jurisdiction.

The SEC requires issuers of securities to register with the SEC, including disclosure and publication of a prospectus. Applying similar rules to cryptocurrencies harms states' efforts to develop the digital assets industry, which is governed by consumer protection laws and licensing requirements for money transmitting services (for example, in Florida and Kentucky).

It is important to note that the Securities Act has classified an investment contract as a security since as early as 1933.[6] A 1946 court case resulted in the development of the Howey test, which defines 3 criteria for a security:

1) Investment of money in any form (e.g., purchase of a digital asset in exchange for fiat currency).

2) Existence of a common enterprise.

3) Expectation of profit as a result of the efforts of others (the issuer of digital assets).

The third criterion, the investor's expectation of profit as a result of the efforts of others, is important. An investor can expect a profit if he sells the asset at a profit as a result of an increase in its market value due to the issuer's management efforts rather than general economic growth or inflation. For example, the issuer can make these decisions: limit the supply of the asset; decide who gets additional tokens (assets) and on what terms; monopolize the validation and confirmation of transactions with the asset; and pay its managers with the asset. The purchase of a digital asset will rather have an investment character, when the possibility to immediately use it to pay for goods and services instead of fiat currency is limited.

The SEC believes that individuals involved in Initial Coin Offering (ICO), sale or distribution of a digital asset should assess whether the digital asset has the characteristics of an investment contract. This includes not only the form and terms of the investment in digital assets, but also the circumstances and way it is offered and sold, including in the secondary market (e.g., whether it is a private offering to a limited number of investors or a public offering to all). To resolve contentious issues, the SEC encourages contacting it on its website.

The SEC has repeatedly resorted to enforcement against cryptoassets providers such as Ripple, Binance, and Coinbase.

The example of a state whose efforts are hurt by the SEC's position is Oklahoma, where HB 3594, a law regulating digital assets, went into effect in November 2024.[7] “Digital assets” include virtual currencies, cryptocurrencies, stablecoins, and non-fungible tokens (NFTs).

The law does not allow the government to prohibit or restrict the use of digital assets for the purchase of goods and services and self-custody using self-hosted wallet or hardware wallet.

Payments with digital assets cannot be subject to additional taxes and fees compared to other means of payment. The law legalizes home digital asset mining subject to local noise requirements, as well as the business of mining in industrial zones with a prohibition to set special noise pollution standards for such businesses.

Interestingly, this law in no way excepts any person, entity, transaction or activity from the jurisdiction of the Oklahoma Department of Securities, i.e. the above dispute between the states and the SEC is not about whether digital assets are securities, but rather about the distribution of powers between the center and the regions.

Russia’s experience

In Russia, the Law on Digital Financial Assets (DFA) and Digital Currency prohibits the acceptance of digital currencies

[5] Kentucky, Nebraska, Tennessee, West Virginia, Iowa, Texas, Mississippi, Montana, Arkansas, Ohio, Kansas, Missouri, Indiana, Utah, Louisiana, South Carolina, Oklahoma, Florida.

[6] https://www.govinfo.gov/content/pkg/COMPS-1884/pdf/COMPS-1884.pdf

[7] http://www.oklegislature.gov/BillInfo.aspx?Bill=hb3594&Session=2400; http://webserver1.lsb.state.ok.us/cf_pdf/2023-24%20ENR/hB/HB3594%20ENR.PDF

(cryptocurrencies) as means of payment. In Russia, there is no question of regulating digital currencies and DFAs as securities. A similar approach exists, for example, in France.

2. Violation of consumer rights on the internet

The US experience

In November 2024, a lawsuit was filed in the United States against the Sitejabber platform,[8] which, using artificial intelligence, collects reviews and creates ratings of sellers. The idea of the platform is to post real customer reviews of goods, services and sellers so that other customers can be guided by such ratings and reviews if they decide to purchase these goods and services. It was revealed that 98% of customer reviews were collected by the platform by conducting instant surveys immediately after the purchase - before the customers had an opportunity to actually experience the purchased product, and only 1% of reviews came from customers who actually experienced the product.

It was clearly not disclosed to customers that the surveys were artificial reviews of sellers and generated their rankings on the Sitejabber platform. Through such surveys, Sitejabber artificially inflated the number of reviews and average ratings, misleading customers about the reliability of customer reviews.

Unlike Russia, the United States has the Consumer Review Fairness Act of 2016 (15 USC § 45b).[9] The law prohibits restricting consumer's right to leave a review, including a negative one. And in October 2024, the Federal Trade Commission adopted the Rule Against Fake or False Consumer Reviews,[10] including prohibitions on writing, selling, or buying fake or false consumer reviews that were created by a non-existent consumer, buying positive or negative reviews by a company, the prohibition of removal of negative reviews, and so on.

The EU experience

In November 2024, the European Commission and the Consumer Protection Cooperation Network initiated an investigation against Apple and Temu (a Chinese marketplace).

Apple is accused of illegally geo-blocking users of App Store, Music, Books, etc.:[11]

1) The services have a different interface for different EU countries. The customer only gets access to the interface made for the country where they have registered their Apple account. It is difficult to change the interface when moving to another country.

2) For paid purchases, consumers are allowed to use means of payment (e.g., bank card) that are issued in the country where the Apple account is registered.

3) Due to different versions of the App Store in different countries, customers not allowed to download the apps offered in other countries, even if users are traveling or temporarily located in another country.

These actions violate the EU Geo-Blocking Regulation 2018/302, which establishes a prohibition on unjustified discrimination between EU customers on the basis of their nationality, residence, or place of establishment when they want to buy goods and services from a trader located in a different Member State. Apple has a month to clarify or remedy these violations.

Investigation against Temu involves the use of “dark practices”:[12]

1) Creating the false impression that goods are offered at a discount, but in fact are not discounted.

2) Pressuring consumers to make purchases by falsely notifying them that the quantity or timeframe for purchasing a product is limited.

3) Forced gamification - forcing customers to play a game of “spin the fortune wheel” game to gain access to the marketplace, hiding important information about the terms of use of rewards in the game.

4) Displaying incomplete and incorrect information about customers’ legal rights to return goods and receive refunds.

5) Unclear information on how the authenticity of customer reviews on its website is ensured.

---

[8] https://www.ftc.gov/news-events/news/press-releases/2024/11/ftc-order-against-ai-enabled-review-platform-sitejabber-will-ensure-consumers-get-truthful-accurate

[9] https://www.law.cornell.edu/uscode/text/15/45b

[10] https://www.ftc.gov/business-guidance/blog/2024/08/well-pay-you-give-our-new-rule-good-review

[11] https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5727

[12] https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5707

6) Temu's contact details are hidden - customers cannot contact Temu if there are questions or complaints.

Temu also has a month to clarify or remedy violations.

South Korea Experience

In November 2024, the Commerce Commission launched 2 investigations against AliExpress and Temu. The first investigation concerned practices that violate competition and consumer laws:[13]

- Platforms disclaimed any legal liability for damages of any kind arising from the transactions.
- Unlimited collection of user data: companies required consumers to provide access to the account and all data with the right to transfer it to affiliated companies. Users were encouraged to give up intellectual property rights protection for their user-generated content.
- Limiting consumers' ability to go to Korean courts - suggested disputes be heard in international courts.
- Platform has discretion in determining whether a user has violated the platform agreement - risk of unreasonable blocking.
- Injunction against lawsuits: users agree not to bring any action or lawsuit against platforms in connection with disclosures (e.g., in the event of information leaks).

The second investigation is related to the sale on Temu and AliExpress of unsafe consumer goods, including household appliances, electronics with high levels of lead, and cadmium. Another 359 items (56.9% of all items investigated) posed a risk of electric shock. As a result, the Trade Commission banned 1,915 dangerous goods from trading on AliExpress and Temu.

Russia

In Russia today there is no regulation of the practice of artificially inflating or falsifying customer reviews. There has been an attempt to introduce rules on the use of subscription traps.

3. Balancing private and public interests in content moderation

In November 2024, the EU and South Korea strengthened online content moderation requirements. X Corp. challenged the constitutionality and legal validity of California (USA) bill requiring online platforms to remove or label materially deceptive election-related content.

The EU experience

The European Commission has adopted an implementing regulation to the Digital Services Act on new transparency reporting rules for providers of intermediary services and online platforms. It will enter into force on July 1, 2025.[14]

The Act requires[15] intermediary service providers and online platforms to publish in machine-readable format, at least once a year,[16] reports on any content moderation by them, including information categorized by type of illegal content on: moderation measures taken on their own initiative; the number of content complaints received through the provider's internal systems and their resolution; and the use of automated moderation tools, including specification of their purposes and accuracy indicators.

The regulation stipulates that:

(a) reports should be filed in CSV or XLSX format in the form in Annex I to the regulation. Includes 15 content categories to categorize information,[17] which increases the comparability of reports from different companies.

б) The reporting periods for very large online platforms are January 1 through June 30 and July 1 through December 31.

в) Reports should remain available for 5 years.

[13] https://www.ftc.go.kr/www/selectReportUserView.do?key=10&rpttype=1&report_data_no=10892

[14] https://digital-strategy.ec.europa.eu/en/news/commission-harmonises-transparency-reporting-rules-under-digital-services-act; https://digital-strategy.ec.europa.eu/en/library/implementing-regulation-laying-down-templates-concerning-transparency-reporting-obligations

[15] https://eur-lex.europa.eu/eli/reg/2022/2065/oj

[16] Providers of very large online platforms – once in 6 months.

[17] Animal welfare; consumer information infringements; cyber violence; cyber violence against women; data protection and privacy violations; illegal or harmful speech; intellectual property infringements; negative effects on civic discourse or elections; protection of minors; risk to public security; scams and/or fraud; self-harm; unsafe, non-compliant or prohibited products; violence; other violations of provider's terms and conditions.

South Korea experience

Following Mr. Durov's arrest in August 2024 in France (see Monitoring No. 8), Telegram began cooperating with law enforcement agencies in other countries, including South Korea.[18]

In November, Korea Communications Commission sent a request to Telegram to combat the distribution of illegal content, including sexually explicit deepfakes, on its platform and to appoint a responsible youth protection manager to encourage Telegram to strengthen its internal regulation. Telegram has complied with the request and, in cooperation with the Commission through the appointed manager, plans to block information harmful to young people.

The US experience

On November 14, 2024, X Corp. filed a lawsuit against California authorities regarding the Defending Democracy from Deepfake Deception Act of 2024 (AB 2655).[19] The Act requires large online platforms such as X Corp. to remove or label content about candidates, election organizers, and elected officials that the state deems "materially deceptive " and to create a mechanism for residents to report such content to the platform.

X Corp. is seeking an injunctive relief against the enforcement of this bill because, according to the company, the bill results in the state, rather than the platform, even with a content moderation system, deciding what content will appear on the platform, which is contrary to the free speech protections of the First Amendment to the U.S. Constitution and Article I, Section 2 of the California Constitution. Thus, the company challenges the constitutionality and legal validity of AB 2655.

It is important that the definition of materially deceptive content in the bill[20] is not limited to deepfakes and chatbot outputs. The bill contradicts the Supreme Court's position in Moody v. NetChoice LLC 2024: when a platform presents a curated and edited compilation of a speech, it is itself protected speech.

X Corp. emphasizes that companies cannot be assured of compliance with AB 2655 because its definition of content is based on many undefined or evaluative concepts. For example, such terms include "satire" and "parody" because content, including deepfakes, created in this capacity is not subject to removal and labeling requirements.

Also, according to X Corp., the bill conflicts with national telecommunications regulation, which prohibits online platforms from being treated as publishers/speakers with respect to information from other content providers.[21] The company cites, among other things, the court's position in Calise v. Meta Platforms Inc. 2024, that this statutory provision protects Meta from requirements to review and evaluate third-party advertisements.

Russia's experience

In Russia, it is becoming expensive not to remove illegal online content. At the beginning of November, several technology giants were handed significant fines for violating Part 2, Article 13.41 of the Administrative Offences Code of the Russian Federation.

In addition, in November, amendments to the Federal Law "On Information" were adopted, prohibiting the dissemination of information on the Internet that promotes childfree propaganda (clause I of Article 10-6). Dissemination of such information can lead to extrajudicial blocking of an information resource (clause L of Article 15-1). The problem is that it is not clear whether books about informed parenthood (about the need for preconditions, emotional and material maturity, for childbearing) or public criticism of state demographic programs fall under this category.

4. Liberalization of cross-border data flows

The World Bank estimates that the digital economy accounts for 15% of global GDP, outpacing the traditional economy in annual growth by a factor of 2.5 over the past 10 years.[22] Today, countries are striving to balance

[18] https://www.france24.com/en/live-news/20240930-telegram-cooperates-with-s-korea-deepfake-porn-crackdown-regulators

[19] https://www.courthousenews.com/wp-content/uploads/2024/11/xcorp-2655-lawsuit.pdf

[20] § 20512(i); https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB2655.

[21] 47 U.S. Code § 230(c)(1), https://www.law.cornell.edu/uscode/text/47/230

[22] https://www.edgemiddleeast.com/business/dco-2030-digital-economy-to-contribute-30-of-global-gdp-and-create-30-million-jobs-by-2030

the requirements for data circulation in order to eliminate unnecessary barriers. For example, in November 2024, China launched an international initiative facilitating cross-border data flows.

Experience of China

The draft Global Cross-Border Data Flow Cooperation Initiative envisions the following objectives:

1) Prohibition to discriminate against countries when regulating cross-border data transfers.

2) Prohibition to use by a state any security measures to protect data restrictions or requirements as a pretext for restricting data flow into the territory of that state.

3) Cooperation on personal data protection.

4) Mutual recognition of standards in the field of data protection.

5) Definition of closed lists of data types for special regulation.

6) Definition of conditions for a healthy competitive environment in the field of data circulation. For example, the development of regulatory measures for digital platforms that prevent monopolization of the digital services market based on the accumulation of large data sets.

7) Support of developing countries in the digitalization of their economies, for example through technical assistance.

8) Identification of data mishandling practices.

China expects the International Initiative to ensure free circulation of data not only from China, but also from third countries to China. Thus, China ranks first in terms of e-commerce market volume, outpacing the United States by 2.2-fold.[23] China is also actively developing data-driven technologies: China's share in global funding of AI startups hits 48%.[24]

Russia's experience

In Russia, cross-border transfer of personal data is limited by the requirement to notify Roskomnadzor in advance of data transfer to third countries. Roskomnadzor can decide to restrict data transfers, but the criteria under which such a decision can be made are not disclosed. In terms of the China Initiative principles, such risky regulatory measures could be seen as a means of arbitrarily restricting data transfers to China.

5. Banning social media for children

Australia experience

Australia has passed a law restricting the use of social media by children under 16. Platforms must incorporate age verification into their systems when creating accounts, however, the law does not require such verification.

Texas experience (USA)

In the state of Texas, a bill[25] proposes to set the age threshold for accessing social media at 18 years of age. However, in Texas, the requirement to implement an age verification method must be commercially reasonable.

Texas has proposed a rule that a request to delete an existing account can be made by a parent or guardian of a child, in which case the platform would need to verify that there is a relationship between the people.

Experience of China

China has issued guidelines[26] for mobile device, app and app-hosting platform providers on creating a juvenile mode (under 18). Developers should ensure that it is easy to enter and exit the juvenile mode on devices or platforms and provide communication between devices on the transition from the modes.

The children's regimen must include:

1) Daily limit of device, app usage (e.g., no more than 1 hour per day for children under 16).

2) Content moderation requirements - restriction of content dangerous for children's psyche or encouraging deviant behavior.

3) Technical settings that should be considered during operation (e.g., blocking unfamiliar users, settings to reduce the visibility of information about children).

Russia's experience

In Russia, the law "On the Protection of Children from Harmful Information" does not provide any restrictions on the use of social networks. The law also does not contain even

[23] https://www.statista.com/chart/32159/revenues-in-the-e-commerce-segment-by-country/

[24] https://www.statista.com/chart/14218/china-dominates-global-funding-of-ai-startups/

[25] https://legiscan.com/TX/text/HB186/id/3026218

[26] https://www.cac.gov.cn/2024-11/15/c_1733364304749288.htm

more important measures against cyberbullying, tracking children through geolocation (disabling geolocation for children's social network accounts), etc.