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

Tightening of personal data circulation, the mental health of children in the platform economy, minimum tax for cross-border companies, anti-competitive practices online

Monitoring No. 10 (October 2024)

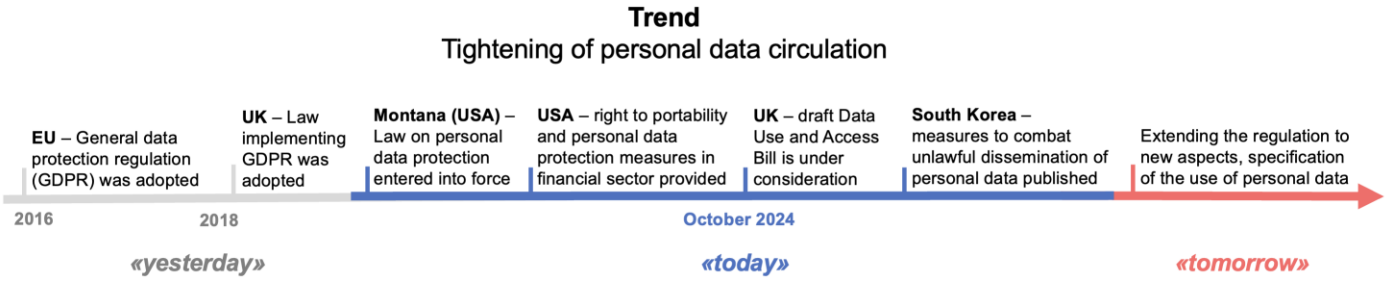
Monitoring was prepared by a team of experts of the Gaidar Institute for Economic Policy (the Gaidar Institute):
Antonina Levashenko, Senior Researcher, International Best Practices Analysis Department, Gaidar Institute.
Maria Girich, Researcher, International Best Practices Analysis Department, Gaidar 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

"Opened the window. How gloomy
The capital is in October!
A wretched brown horse
Walking in the backyard."
Alexander Block

In October 2024, we can identify 4 events that define trends in the development of digital economy regulation in the world.

Trend No. 1. Tightening of personal data circulation

In October 2024, several countries adopted or considered regulations related to the circulation of personal data. For example, in the USA, the right to data portability in the financial sector is now provided for in the legislation, and in the UK it is proposed to fix the legal status of digital verification services for users of electronic services (online applications, banking, etc.), in South Korea measures have been taken to combat data leaks. In Russia, these issues are not regulated (dynamic consent to processing and the right to transfer of personal data), which in the future implies amendments to the Law on Personal Data.



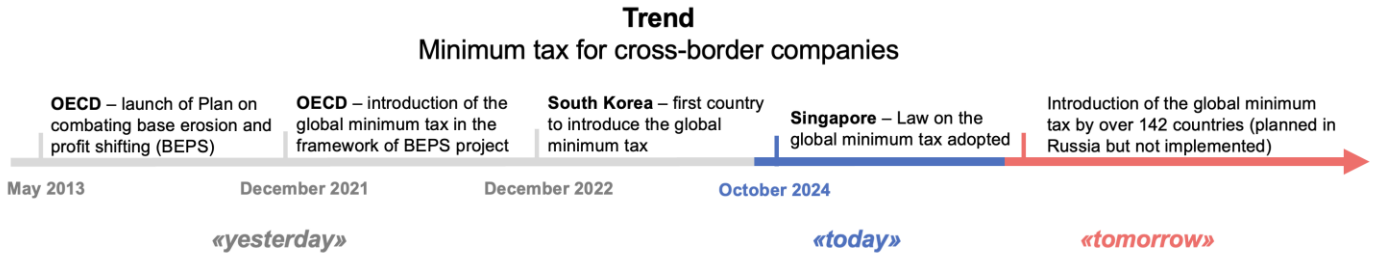
Trend No. 2. The mental health of children in platform economy

In October 2024, 41 U.S. states initiated legal proceedings against Meta[1] for inappropriate treatment of children that harms their mental health, such as hooking a child on the website to the detriment of their other activities and neglecting to verify the age of users

Trend No. 3. Minimum tax for cross-border companies

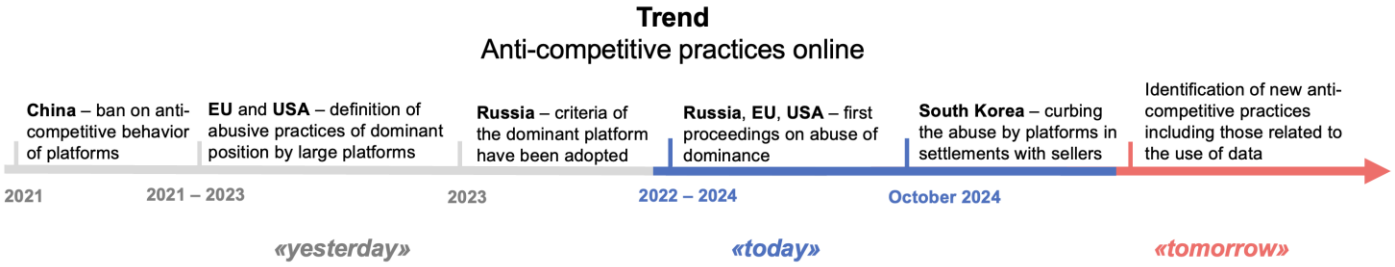
In October 2024, Singapore enacted Law[2] that introduces the global minimum tax rules based on the OECD model. The mechanism suggests that large international groups of companies should be subject to an income tax of at least 15% in each country where they operate. More than 30 countries have already adopted similar regulation, Russia has not.

[1] Meta's activities were recognized as extremist and banned in the Russian Federation.
[2] Multinational Enterprise (Minimum Tax) Act, No. 33/2024.



Trend № 4. Anti-competitive practices online

In October 2024, separate rulings were handed down in the US in connection with Google's abuse of its dominant position in the search advertising and operating system markets. Moreover, in Korea, it was proposed to limit the abuse of platforms in settlements with sellers - the platform must wire the money received from the consumer to the seller within 20 days from the date of payment.



October 2024 also saw a number of significant developments in the regulation of the digital economy in Russia.

1. The procedure for blocking “mirror” sites has been simplified

In October 2024, amendments to the Federal Law “On Information” came into force, simplifying the terms of blocking mirror sites, i.e. copies of blocked sites.[3] Previously, in order to block a mirror site, information about it must first be sent to the Russian Ministry of Information and based on the Ministry's decision to recognize the site as a mirror site, the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) could proceed with the extrajudicial blocking procedure. Now the authority to make a decision on a mirror site has been transferred to Roskomnadzor. Although the reduction of administrative steps optimizes the work of the bureaucratic apparatus, this change also carries risks of unjustified or erroneous extrajudicial blocking of sites.

2. Introduced checks by Roskomnadzor when data is sent abroad

In October 2024, draft order of the Ministry of Digital Development,Communications and Mass Media of the Russian Federation (MinTsifry[4]) was released, which supplements the list of risk indicators of violation of mandatory requirements when exercising state control over the processing of personal data with a new indicator: the presence of information about at least 2 cases within a year of cross-border transfer of personal data by an organization using foreign software without notifying Roskomnadzor of such intention. In the presence of such information, Roskomnadzor may conduct an unscheduled inspection of an organization.

According to the Law on Personal Data, prior to the commencement of cross-border transfer, the operator must notify Roskomnadzor. When providing services by financial organizations and subjects of the national payment system, it is prohibited to use foreign information systems and software for the

[3] https://sozd.duma.gov.ru/bill/537002-8
[4] https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=151217#

transmission of information necessary for making payments, information on bank accounts, transfers and personal data of citizens of the Russian Federation.

The explanatory note to the draft order states that it will not create negative consequences, including for subjects of economic activity. At the same time, the emergence of a company's risk indicator may lead to its inspection by Roskomnadzor. In the meantime, according to the Big Data Association,[5] notifying Roskomnadzor of the intention to carry out cross-border data transfer involves the issue of providing it with information on how the transferred personal data is protected by the foreign party. In other words, failure to notify the regulator is not always the result of companies' inaction. In this regard, the initiative under consideration is ambiguous, especially for small companies.

3. Bloggers must notify users of their registration with Roskomnadzor

October 2024 saw a draft decree of the Russian Government[6] on the rules for bloggers to post information on the inclusion of the blogger's page in Roskomnadzor's list on personal pages in social networks with more than 10,000 followers. Firstly, it must be indicated that the page is included in the Roskomnadzor register by graphically highlighting **A+**. Secondly, a link to the page in the register itself must be indicated, accompanied by the text “Included by Roskomnadzor in the list of personal pages.”

[5] https://www.kommersant.ru/doc/7199281

[6] Draft Decree of the Government of the Russian Federation "On Approval of the Rules for the Placement on a Personal Page with an Audience of More than Ten Thousand Social Network Users of Information on Inclusion in the List of Personal Pages with an Audience of More than Ten Thousand Social Network Users" https://www.consultant.ru/law/review/fed/fd2024-10-09.html

Key aspects

1. Tightening of personal data circulation

In October 2024, several countries and regions adopted or were considering regulations extending and/or clarifying the processing of personal data, including in the financial sector.

The US experience

There is no federal law on personal data in the US, but sectoral and regional acts are being adopted.

On October 22, 2024, the Consumer Financial Protection Bureau issued a rule requiring financial service providers[7] to transfer personal financial data free of charge to other financial service providers[8] upon a consumer's request and to maintain secure interfaces for making requests and receiving data.[9]

This is about the right to personal data portability. Consumers will be able to more easily change financial service providers to more suitable ones (e.g. with lower fees or loan rates) without the inconvenience of losing data (payment history, regular payments, etc.).

Such rules will limit the use of "dark patterns", such as bait-and-switch data harvesting, when customers are attracted to a website by a favorable offer of a non-existent product/service. The rule will be implemented sequentially from large companies to smaller ones from 01.04.2026 to 01.04.2030.

Moreover, the Montana Consumer Data Privacy Act[10] came into effect on October 1, 2024. The state residents were granted a number of rights common in other jurisdictions (e.g., EU), such as deletion of their personal data, obtaining a copy of it for transfer to another service provider (e.g., photo hosting), and refusing to have their data processed for the purposes of targeted advertising or profiling for automated decision-making (e.g., of access to credit or healthcare). Data controllers are now required to limit the collection of personal data that is necessary for a specific purpose, among other things.

A characteristic feature of US practice is the direct regulation of the sale of personal data by controllers with the consent of data subjects. In other jurisdictions where the sale of personal data by companies is not directly prohibited (e.g., EU), regulation is usually limited to general principles of personal data handling in the absence of specific rules on the sale of data. Montana law contains special rules: while it does not impose restrictions on the sale of personal data (e.g., purpose of sale, etc.) other than the data subject's consent, the law classifies its sale as a type of data processing with a heightened risk of harm to data subjects and therefore requires a separate data protection assessment of the data processed for these purposes to be conducted and documented. At the same time, the law does not apply to businesses processing personal data of less than 50,000 subjects or 25,000 if the company derives more than 25% of its gross revenue from their sale.

The UK experience

On October 23, 2024, a draft Data (Use and Access) Bill was introduced in the UK Parliament.[11] It is expected that the major impact will be on organizations, including international ones, in the spheres of digital, research, medical services and so on.

The bill clarifies regulation in the following areas:

1) Consolidation of the legal status of digital verification services for users of electronic services (online applications, banking, etc.). Providers of such services will be included in the register based on a certificate.[12]

[7] The regulation does not apply to depository institutions with up to $850 million in assets.

[8] The rule relates to the following financial information: transaction data (amount, date, payment type and status, name of payee, rewards, credits and fees or charges), including their history; account balance; payment initiation data, including payee/sender account; fee schedule, account interest rate, credit limit, rewards program, overdraft; scheduled payments (e.g., communication fees); name, address, email and phone number associated with the financial product. However, financial service providers are not required to share with consumers any confidential information, including algorithms used to assign credit scores and risk assessments, or any information collected solely for the purpose of preventing fraud, money laundering, or detecting illegal behavior.

[9] https://www.consumerfinance.gov/about-us/newsroom/cfpb-finalizes-personal-financial-data-rights-rule-to-boost-competition-protect-privacy-and-give-families-more-choice-in-financial-services/; https://files.consumerfinance.gov/f/documents/cfpb_personal-financial-data-rights-final-rule-reg-text_2024-10.pdf

[10] https://archive.legmt.gov/bills/2023/billpdf/SB0384.pdf

[11] https://bills.parliament.uk/bills/3825

[12] Digital Verification Services trust framework.

2) Availability of personal data for scientific and statistical research. The terms for obtaining the subject's consent to the use of his/her data for these purposes are simplified, including allowing controllers not to formulate precisely the purposes of processing when the purposes of the research itself cannot be accurately interpreted (e.g., at the initial stage of scientific research).

3) Supporting practices of reuse of collected data. The controller may obtain the subject's consent to continue processing their data for new purposes different from the original purpose in the consent form. To do so, the controller must assess the relationship between the original and new purposes of data processing.

4) Decision-making based solely on automated processing of personal data to the explicit consent of the individual. This is relevant, for example, for digital platforms practicing digital profiling of users for the purposes of displaying targeted advertising and personalizing services.

5) The cross-border transfer of personal data receives more detailed regulation. The Secretary of State may regularly assess whether the protection of personal data in third countries is compatible with the level of protection afforded to data subjects in the UK and set standards for cross-border transfers. Consequently, for companies working with personal data from the UK, there are risks of limiting cross-border transfers of data primarily to countries that have not adopted legislation on personal data, such as Cuba, Venezuela, Syria, Sri Lanka and others.

Experience of South Korea

On October 24, 2024, Korea published measures aimed at reducing the illegal dissemination of personal data.[13] In 2021, 157,000 cases of illegal disclosure of such data were revealed, and in 2023, it was already 200,000. The number of spam messages on cell phones increased by 40.6% from May to June 2024. Therefore, it is planned to:

1) Introduce an AI-based Internet information scanner that should find both textual data (e.g., email address) and image data (e.g., faces in deepfakes);

2) Block messages that illegally disclose personal data. The objective is to reduce the time required to delete illegally disseminated messages from 24.8 to 18.9 days in 2025, including through cooperation with online platforms;

3) Expand measures for prosecution of those who illegally disseminate personal data, including through information exchange and cooperation with law enforcement authorities;

4) Create database for storage and analysis of information on leakages.

Russia's experience

Russia has not regulated several issues discussed above, in particular, access to personal data for scientific purposes, dynamic consent to the personal data processing and the right to data portability.

2. The mental health of children in platform economy

One of the most important trends in the regulation of platforms is the protection of children on the Internet. This trend has already been addressed in Monitoring No. 4

The US experience

In October 2024, the attorney generals from 41 U.S. states initiated legal proceedings against Meta[14] for practices that harm children's mental health: 33 states filed a public lawsuit and another 8 states began litigation.[15] The lawsuit is considered by lawyers to be the largest public initiative to challenge the uncontrolled influence of social media on minors' mental health.

The series of lawsuits resulted from an investigation launched in 2021 by a coalition of attorney generals from 10 states. A number of negative practices were identified. First, Meta introduces features that hook minors' attention on the platform to the detriment of their mental development and are addictive, such as the endless content feed format. Second, Meta deliberately misleads users about the safety of services for children, for example, the user

[13] https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=10702#LINK

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

[15] https://digitalpolicyalert.org/event/15222-filed-public-lawsuit-by-33-attorney-generals-against-meta-for-allegedly-harming-the-mental-health-of-minors-through-addictive-features

reporting tools do not prevent dangerous content from being shown to the user. Thirdly, Meta does not comply with the requirement of laws on verification of consent of the user under 13 years of age (for example, in California), and the applied age verification tools are ineffective.

As a result, the company might face large fines (for instance, the most recent fine paid by Facebook under a court order is $5 billion), as well as obligations to change corporate policies regarding minors.

Russia's experience

The US case is indicative of the Russian experience, where there are practically no channels for interaction between platforms and Roskomnadzor, the relationship is built on a top-down scheme: platforms receive instructions from the authority to block information or other requirements, but do not receive any recommendations on data handling, information risk management, organization of digital compliance, etc. (for example, methodological recommendations on depersonalization of personal data have not been updated since 2013). Accordingly, in Russia, practices of interaction with minors are set by the market, and, as a result, in the absence of a unified quality bar for the security of digital services, users of such services do not receive equal guarantees.

3. Minimum tax for cross-border companies

Singapore has enacted the Multinational Enterprise Minimum Tax (MNE) Bill, which enshrines an income tax rate of 15% as the minimum applicable to all MNCs.

Back in 2023, the OECD developed the Global minimum tax (GMT) mechanism as part of its efforts to combat the erosion of the tax bases of multinational enterprises. The purpose of the mechanism is to ensure that large companies are subject to a minimum tax rate of at least 15% in each country where they operate. This should reduce the practice of profit shifting to jurisdictions with low tax rates.

GMT addresses the issue of lower corporate tax rates in a number of countries, which is done in order to attract MNEs to the tax jurisdiction. For example, in the US in 2017, the corporate income tax rate was reduced from 35% to 21% to increase the country's tax attractiveness for MNEs.[16] This leads to increased competition between jurisdictions for the tax revenues of large corporations and creates a risk of a "race to the bottom" in terms of tax rates, which is what the GMT should prevent.

Experience of Singapore

Singapore's new 15% minimum tax for MNEs Act applies to companies whose total consolidated revenues for at least 2 out of the last 4 financial years exceed €750 million. The calculation is based on the consolidated financial statements of their ultimate parent company, which includes the revenues of all entities in the group operating in the country.[17]

In addition to the minimum basic rate, the multinational enterprise top-up tax (MTT), Chapter 3 of the Act imposes a domestic top-up tax (DTT). DTT is the sum of the taxes payable by all subsidiaries and affiliates of an MNE at 15% and not actually paid in full due to the use of lower rates. This amount is calculated as the ratio of adjusted taxes to the income or loss of the group of companies. If the result of this calculation is below the minimum rate of 15%, DTT is applied to bring the rate to the minimum 15%.

Let us illustrate the functioning of the tax. For example, in Singapore the "default" corporate income tax rate is 17%, but all companies resident in Singapore may apply a rate of 8.5% on profits up to SGD300,000 per year. Imagine there are 10 subsidiaries of MNE operating in Singapore, each has annual income of €420,000 (€4.2 million in total), i.e. half of the income is taxed at 8.5% and half at 17%, on average each company will pay 12.75% income taxes. If MNE were to open one subsidiary with the same total income of €4.2 million, €209,000 would be taxed at 8.5% and the rest at 17%, i.e. in total the company would pay almost 17% income taxes. This means that from a tax perspective, it is more advantageous for MNEs in Singapore to split subsidiaries, thereby

[16] Art. 13001 of the 2017 Act to Amend the Internal Revenue Code of 1986. / https://www.congress.gov/bill/115th-congress/house-bill/1

[17] The Act does not apply to governmental organizations, international organizations, nonprofit organizations, pension funds, nonprofit subsidiaries, service organizations, and tax-exempt organizations (organizations in which at least 95% of the total value of ownership interests is owned directly or indirectly by one or more exempt organizations, organizations that engage only in activities that are ancillary to those of the controlling organizations, or all or substantially all of the activities of the controlling organizations).

reducing income tax rates. However, the GMT mechanism obliges MNEs using such a scheme to pay the missing 2.25% income tax (12.75%+2.25%=15%) for each of the 10 subsidiaries, which makes splitting subsidiaries much less favorable.

To date, about 30 countries have already adopted legislation implementing GMT.[18] For example, in the European Union, EU Directive 2022/2523 of December 14, 2022 was adopted.[19]

Russia's experience

In the Main Directions of the Budget, Tax, Customs and Tariff Policy of the Russian Federation for 2024 and for the Planning Period of 2025 and 2026, the Ministry of Finance of the Russian Federation provided for an assessment of the need to make changes to the Russian tax legislation. These changes are aimed at establishing a minimum level of taxation for Russian holdings that would correspond to the globally accepted GMT rate of 15%.

4. Anti-competitive practices online

In October 2024, 2 cases against Google for abuse of dominance were adjudicated in the US. In South Korea, it is proposed to regulate the risks of abuse of platforms due to sellers' untimely settlements.

The US experience

In the first case, the attorney generals from all states and the DOJ issued a statement about Google's abuse of the search text advertising services market in the United States.[20] Google's search engine, where advertisers spend up to $80 billion a year, has a 90% market share.

Google made exclusive agreements with browser developers (like Apple, Mozilla) who must "by default" install Google search in their browsers in exchange for a share of Google's search advertising revenue. Similar agreements were made with Android device manufacturers (like Samsung) - it was forbidden to pre-install search engines other than Google on devices.

In October 2024, state attorney generals proposed legal protections against the influence of Google's monopoly. It is proposed to restrict Google from entering into such agreements.

The second case, pending in October 2024 against Google, originated back in 2020 when Epic Games (game and entertainment developer) filed a complaint against Google for market abuse.

Google forced consumers and app developers to use its own Google Play. Google also signed agreements with Android device manufacturers to give Google preferential treatment - the manufacturers placed the Google Play on the "home screen" of each device and pre-installed 30 more Google apps on each user's mobile device. In exchange, manufacturers were rewarded with a percentage of sales from users' use of Google apps.

App developers could not sell apps and content directly from their own website or from another app store - only through Google Play if they wanted to have access to other Google services (advertising, search, YouTube). Google also required the use of its own payment tool, Google Play Billing, for transactions with consumers within downloaded apps, imposing a 30% fee on transactions, which is 10 times higher than other payment solutions.

As a result, in October 2024, the District Court of California issued an injunction.[21] Google has been enjoined for 3 years to:

- Share revenue from the Google Play with manufacturers on Android as a condition of pre-installing Google services.
- Restrict the ability to update apps that are downloaded from stores other than Google Play or from the developer's website.
- Restrict (including through commissions) the use of payment tools other than Google Play Billing.

Google should provide the option to put other store apps on Android.

Experience of South Korea

In October 2024, proposed amendments to the Fair Transactions in Large-Scale Retail

[18] https://www.pwc.com/gx/en/tax/international-tax-planning/pillar-two/pwc-pillar-two-tracker-full-data-v2.pdf
[19] https://eur-lex.europa.eu/eli/dir/2022/2523/oj
[20] https://storage.courtlistener.com/recap/gov.uscourts.dcd.223205/gov.uscourts.dcd.223205.1052.0_1.pdf
[21] https://storage.courtlistener.com/recap/gov.uscourts.cand.373179/gov.uscourts.cand.373179.1017.0_3.pdf

Business Act[22] to limit abuses by «large» platforms in settlements with merchants.[23]

It is proposed to establish that if a large platform manages payments for the sale of vendors' goods (services) on the platform, or payments are managed by the financial institution designated by the platform, settlements with vendors as a result of sales should be made within 20 days from the date of confirmation of the purchase. Platforms should place at least 50% of the proceeds from vendor sales in separate financial accounts or through payment guarantee insurance to safeguard funds received from buyers.

This reduces the abuse of platforms related to delayed payments to sellers.

Russia's experience

In 2015, FAS Russia conducted an investigation (similar to the US one) against Google Play abuses in 2015, when Yandex complained that Android phone manufacturers refused to pre-install the Yandex.Kit operating system. Google restricted in its agreements with manufacturers the option to pre-install alternative applications.

FAS recognized Google's practice of "product bundling" (i.e. mandatory pre-installation of a set of Google services when installing Google Play in Android phones) as abuse. The fine for non-compliance with the FAS warnings was Rb0.5 million.

As for the possibility in Russia to restrict abuse of platforms by delaying settlements with sellers (Korea's practice), such an initiative could be included in draft laws to regulate marketplaces, or in competition legislation.

[22] https://www.ftc.go.kr/www/selectReportUserView.do?key=10&rpttype=1&report_data_no=10841

[23] Mediation covers transactions for the purchase and sale of goods and services, including online subscription purchases - covered are marketplaces, lodging, travel, delivery platforms, app stores, etc.