ИНСТИТУТ ЭКОНОМИЧЕСКОЙ ПОЛИТИКИ имени Е.Т. ГАЙДАРА

International Best Practices Analysis Department

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

Combating anti-competitive practices, cybersecurity, new laws for artificial intelligence

Monitoring No. 3 (March 2024)

The monitoring was produced by a team of experts of the Gaidar Institute for Economic Policy (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

APRIL 10, 2024

"There goes spring, so the thoughts are all so pleasant, sharp, fanciful, and pleasing dreams come; everything is in rose-color"

Fedor Dostoevsky

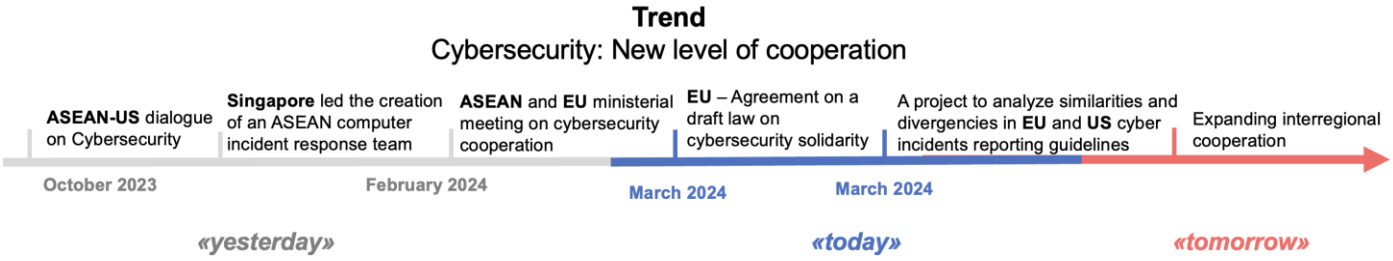
In March 2024, we can identify 3 events that identify trends in the development of regulation of the digital economy.

Trend No. 1. Combating platforms' anti-competitive practices

In March 2024, the EU launched its first antitrust infringement investigation against Google and Apple platforms for non-compliance with the Digital Markets Act, which came into force in February 2024. For example, the companies promote their own services on the platforms to the detriment of similar services of competitors.

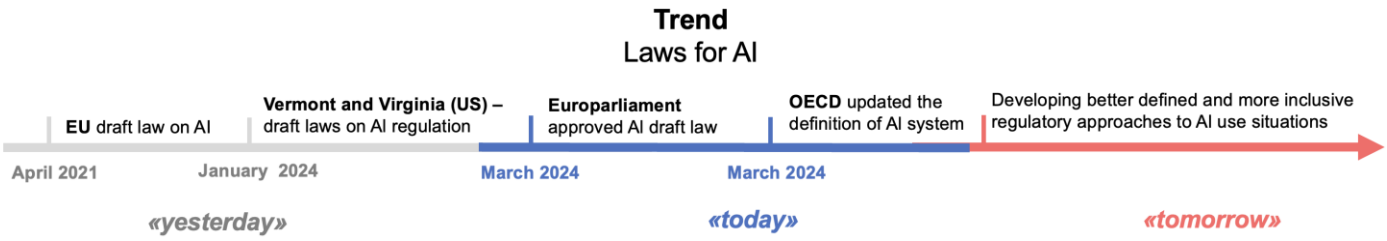
Trend No. 2. Cybersecurity: New level of cooperation

In March 2024, the EU took an important step toward adopting legislation to establish pan-European mechanisms for responding to cyber incidents. A joint EU-US project on common approaches to cyber incident reporting was also unveiled. In the digital economy, cybersecurity creates the necessary baseline conditions for the business environment, with harmonized approaches enabling more effective response to cross-border incidents. These endeavors are supported by other regions of the world: In February, ASEAN advanced the creation of a regional cybersecurity framework.



Trend No. 3. Laws for AI

In March 2024, the OECD Clarifying Memorandum on an updated definition of an AI system was released, and on March 13, 2024, the European Parliament approved the draft AI Law. This is the world's first law designed to reduce systemic risks, tackle discrimination and ensure AI transparency. There are 5 categories of AI: prohibited AI practices, high-risk AI systems, general-purpose AI, general-purpose AI models with systemic risk, and AI systems that interact with individuals or produce synthetic content. The category of high-risk AI systems also found coverage in bills passed for consideration earlier this year in U.S. states. However, the definitions of AI systems remain unclear, including the distinction between AI and smart devices or familiar models.



In March 2024, Russia also saw 2 significant developments in the regulation of the digital economy:

1. Approved the use of digital financial assets in foreign trade contracts

In March 2024, a Law was passed authorizing the use of Russian DFA and digital rights for payment under foreign trade contracts[1]:

- AML/CFT control of transactions with DFA under foreign trade contracts over Rb1 mn.
- Recognition of DFA as currency valuables including monetary claims in foreign currency, foreign securities, etc.
- Currency transactions between residents and non-residents using digital rights may be conducted only under foreign trade contracts.
- Currency transactions may be conducted through digital rights issuance operators and investment platforms.
- The Central Bank may impose bans or special conditions on certain types of foreign exchange transactions involving digital rights.
- Residents may conduct such transactions subject to settlements in rubles.

Such regulation, on the one hand, allows paying with DFA under foreign trade contracts and partially dodging sanctions, on the other hand, the DFA market is rather small (350 DFA issues, 60 billion rubles of circulating assets as of the end of 2023) and inaccessible for foreign companies, as it is possible to market or sell DFA to foreign counterparties only by applying to Russian DFA exchange operators. Allowing payment with cryptocurrencies that are freely exchanged abroad would give exporters great opportunities to reduce the sanctions impact.

It is also important for international trade to introduce payment instruments in cryptocurrencies, in respect of which transactions for the purchase of goods/services are prohibited in Russia. Cryptocurrencies, unlike DFA, can be sold on foreign exchanges, DFA - only on Russian platforms. Also, there is no regulation of crypto exchanges and crypto exchanges in Russia, which limits the access of foreign companies to the Russian market.

2. A bill has been introduced to regulate marketplaces

In March 2024, a bill on product information aggregators (like Ozone, Wildberries, Yandex.Market) was introduced[2]:

1. The regulation applies only to trade in goods. On the one hand, this allows to exclude cab platforms or classifieds (like Avito or Cian) from regulation, on the other hand, services are also part of e-commerce, where it is required to establish safeguards for sellers (e.g. against abuse by platforms).

2. The concept of electronic commerce is introduced, which is also limited to trade in goods. At the same time, the concept of “aggregator of information on goods” repeats the concept of “aggregator of information on goods (services)” provided for in the Law on Protection of Consumer Rights, which may create a conflict in the application of the norms.

3. The concept of a buyer has been expanded to include not only a consumer - a private person, but also a legal entity, which makes it possible to cover both B2C and B2B trade by regulation.

[1] https://sozd.duma.gov.ru/bill/1080911-7
[2] https://storage.consultant.ru/site20/202403/06/fz_060324-568223.pdf

4. Additional obligations of aggregators in terms of monitoring of trade in goods have been established, whereas in the practice of foreign countries the principle of limiting the responsibility of a marketplace for the third parties' actions on the platform when implementing compliance is most often applied.

5. A special status is secured for an aggregator that holds a significant position in the market - it accounts for more than 25% of transactions. Such an aggregator is subject to restrictions: not to create discriminatory conditions, not to impose additional services on the counterparty, not to prohibit counterparties from working with other aggregators or establish price parity, not to create advantages for its own goods/services. Also important is the prohibition to impose forced price reductions on sellers' goods. The aggregator must notify counterparties of changes in contractual terms that aggravate the situation at least 30 days in advance.

In addition, mandatory requirements have been set for the content of an agreement on the services provision by an aggregator to a seller and the owner of an order delivery point, procedures for the identification of a seller when registering on an aggregator's platform, and so on. It establishes the aggregator's obligation to verify the age of buyers for a number of categories of goods, which will make it possible to start trading through aggregators, for example, in alcoholic beverages. In addition, it establishes the aggregator's obligation to ensure proportionality of sanctions imposed on sellers and owners of order delivery points, which creates guarantees for entrepreneurs on platforms against excessive and unfair sanctions on the part of platforms.

The idea of regulating marketplaces was proposed as early as 2021 (first draft laws). However, in this case it is important to create legal guarantees both for marketplaces - in terms of reducing liability for illegal actions of sellers (for example, posting information prohibited by law or infringement of intellectual property rights of third parties), and for sellers - against unjustified fines by marketplaces or forced participation in sales.

Key aspects

1. Combating platforms' anti-competitive practices

The experience of US, EU, and China

In March 2024, the European Commission opened its first investigation into Google and Apple's non-compliance[3] under the Digital Marketplace Act. Apple is accused of restricting the ability of developers to freely sell their applications through Apple's services, Apple charges additional fees and creates technical restrictions, violating competition rules. Google favors its own services to the detriment of competitors' services.

As early as 2021, China, the EU and the US began cracking down on anti-competitive practices by platforms. At the same time, the EU[4] and the US[5] extend special rules to "large platforms", China - to any.[6]

Countries set a list of platforms' anti-competitive practices:

1. Combine personal data, e.g., for digital profiling (EU only). Data from social network services must not be combined with data from advertising services.
2. Provide advantages to your own products over those of sellers on the platform.
3. Create more favorable treatment in rating for own products/services compared to similar products/services of vendors or competitors.
4. Disadvantage some vendors over others in terms of service.
5. Use non-public data generated by sellers when using the platform services to compete with such sellers.
6. Limit the ability of merchants to sell products/services to customers through third-party platforms or through their own direct online sales channels at prices and terms that differ from those offered through platform services.
7. Apply binding agreements, i.e. requiring consumers to use some platform services to access other services.

Moreover, in the EU and the US, large platforms have a number of obligations, e.g.:

1. Ensure interoperability of platform services with third-party services.
2. Provide consumers with the ability to uninstall platform applications, change default settings, or use applications from other platforms.
3. Ensure that sellers have access to the data that it or its customers generate, as well as the option to migrate such data.

Russia's experience

Article 10.1 of the Law on Protection of Competition establishes the prohibit on monopolistic activities by a platform in a particular commodity market that occupies a dominant position, which:

1) Through network effects has a decisive impact on the market where transactions are made through the platform or makes it difficult for other economic entities to access this commodity market. However, there is no methodology for determining network effects.

2) The share of transactions through the platform exceeds by value 35% of the total volume of transactions made on this market.

3) Revenue for the last year - over Rb2 bn.

Unlike the EU and the US, Russia does not assess the number of users on platforms, but the share of commodity market transactions executed through the platform, which can create difficulties in determining platform size (especially for multi-commodity platforms) and market position.

There is no clarification for platforms on what practices may be prohibited.

2. Cybersecurity: New level of cooperation

The EU experience

[3] https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1689

[4] Regulations 2022/1925, 2022 r. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32022R1925

[5] American Innovation and Online Choice Act, versions 2021 through 2023.

[6] EU - for gatekeepers with annual sales of €7.5 bn or more, 45 mn consumers per month and 10,000 business users per year; US - for platforms with sales of $550 bn, 50 mn consumers and 100,000 business users per month. In China, the size of platforms is not taken into account.

On March 5, 2024, an agreement was reached between the European Parliament and the European Council on a draft Cybersecurity Solidarity Act[7]:

1) A pan-European infrastructure of Security Centers - the European Cyber Shield. Consists of national and cross-border cyber centers, and will use AI, among other things, to identify cyber threats and provide real-time information to individuals.

2) An emergency cybersecurity mechanism to respond to cyber incidents. Will operate in 3 areas:

а) Coordination of testing in critical sectors, including health care and energy.

б) EU cybersecurity reserve of trusted providers ready to intervene in case of cyber incidents.

в) Financial support for mutual assistance.

3) European cybersecurity incident management mechanism.

On March 20, 2024, the European Commission and the U.S. announced initiative to analyze cyber incident reporting to better align transatlantic approaches in 6 areas[8,9]. The goal is to respond to cross-border cyber incidents and reduce reporting costs for multinational companies.

The ASEAN experience

In February 2024, Singapore's Cybersecurity Agency announced a collaboration with ASEAN member states to establish a Regional Computer Emergency Response Team.[10]

The experience of Russia and BRICS

In Russia, the Law on Critical Infrastructure Security provides for a system for detecting, preventing and eliminating the consequences of computer attacks on information resources, and a National Computer Incident Coordination Center has been established. The Center exchanges information on computer incidents between "subjects of critical information infrastructure and authorized bodies of foreign states, international, international non-governmental organizations and foreign organizations engaged in activities in the field of response to computer incidents. However, there is no information about such interaction with the EAEU and BRICS countries.

3. Laws for AI

OECD

In March 2024, the OECD released a Clarifying Memorandum on an updated definition of an AI system.[11]

The previous definition of an AI system[12] is modified (p. 4): "An AI system is a machine system that, for explicit or implicit purposes, deduces from the input data it receives how to generate outputs such as predictions, content, recommendations or decisions that can affect the physical or virtual environment. AI systems vary in their levels of autonomy[13] and adaptability[14] once operationalized".

The definition is expanding as AI practices evolve. For example, the OECD considered content-generating AI systems to be such a significant type that they were given a separate mention in the definition, although their work can be seen as a sequence of decisions to output certain words/pixels/sounds if desired. In principle, the definition of AI systems usually covers machine recognition of objects and speech, language information processing, intelligent decision support systems, and intelligent robotic systems (pp. 6, 9).

The OECD believes that goal setting for AI can always be traced back to the person who initiates the development of an AI system, even if the goals are set implicitly. However, some AI

[7] https://ec.europa.eu/commission/presscorner/detail/en/IP_24_1332.

[8] https://digital-strategy.ec.europa.eu/en/news/dhs-and-dg-connect-announce-initiative-comparing-cyber-incident-reporting-better-align.

[9] 1) Definitions and reporting thresholds, 2) timelines, triggers and types of cyber incident reporting, 3) reports content, 4) reporting mechanisms, 5) aggregation of incident data and 6) public disclosure of cyber incident information.

[10] https://www.csa.gov.sg/News-Events/Press-Releases/2024/singapore-moves-ahead-to-establish-the-asean-regional-cert-to-strengthen-regional-cybersecurity.

[11] Explanatory memorandum on the updated OECD definition of an AI system. OECD artificial intelligence papers no. 8. March 2024;. https://www.oecd-ilibrary.org/docserver/623da898-en.pdf?expires=1710851224&id=id&accname=guest&checksum=E0A20405C7B511BB50F0E6BB10A86556.

AI system is a machine system that is capable, for a given set of human-defined goals, of making predictions, recommendations or decisions that affect the real or virtual environment. AI systems are designed to operate at different levels of autonomy.

[13] The autonomy of an AI system, meanwhile, refers to the degree to which it can learn or act without human input after processes have been automated by humans (p. 6).

[14] Adaptability refers to AI systems that are able to change their behavior after interacting with inputs and data after enactment (p. 6).

systems may develop implicit sub-goals and set goals for other systems.

The experience of EU and US

On March 13, 2024, the European Parliament approved the draft AI law.[15]

The bill[16] identifies the following types of AI:

1. Prohibited AI practices (8 categories), e.g. to build or extend facial recognition systems using images from the Internet or surveillance cameras.

2. Authorized high-risk AI systems, such as remote biometric identification systems.

3. General-purpose AI, among which stand out AI models with systemic risk.

4. Certain AI systems (4 categories) that interact with individuals or produce synthetic content, such as generating deepfakes.

The requirements for permitted types of AI vary according to their risk: the higher the risk, the greater and more complex the requirements, from labeling to risk management systems.

In the US, bills aimed at the AI general regulation were introduced in the Vermont and Virginia legislatures in January 2024.[17]

The legislative initiatives of these US states are markedly similar - right down to the overlapping language - but there are some basic divergences as well:

1. The Virginia bill has a narrower list of persons subject to regulation than Vermont's: it only addresses developers and operators of high-risk AI systems, whereas Vermont's bill also contemplates regulations for developers of generative AI systems.

2. The Vermont's bill is more detailed in its definitions and broad in its requirements for developers and operators of high-risk AI systems, specifically spelling out factors for algorithmic discrimination, while Virginia's only references a statutory prohibit.

3. The scope of liability in the Virginia bill is shifted from developers to operators of high-risk AI systems compared to Vermont: for example, avoidance of any risk of algorithmic discrimination in Virginia is mandated only for the latter, whereas in Vermont both.

In terms of comparing the approaches to AI regulation in the EU and the reviewed US states, the following can be pointed out:

1. Approach to AI regulation in the EU relative to U.S. states:

а) Much more comprehensive: the regulation applies not only to high-risk and generative AI (in terms of, for example, deepfakes), but also imposes requirements on other types of AI.

б) Stricter: certain AI practices (e.g., recognizing emotions in the workplace) are prohibited, regardless of the standards and requirements for AI systems.

In principle, emotion recognition in the workplace could meet the definition of an important decision (employment) and therefore fall within the spectrum of high-risk AI systems in the US state bills considered, if it affects, for example, layoffs in the case of downsizing, but even then the AI system operator is limited only by the obligation to notify employees of the operation and purpose of such a system.

2. In terms of the criteria for high-risk AI systems, the same trend is generally evident: in the EU, they are broader, and consequently the regime is stricter. The broader definition is achieved by including elements of product safety and critical infrastructure security among the high-risk areas, whereas in the US states considered, it concerns only certain human interests.

3. None of the considered definitions of AI systems is clear enough from the point of view of identifying the qualifying AI features. As a consequence, the narrowing of the subject of regulation to high-risk/risk-bearing (e.g., to a person's personal space) AI systems may be due to the currently unresolved problem of clearly separating AI from familiar devices (e.g., temperature sensors on devices) and human-made models (e.g., econometric models).

Russia's experience

In Russian legislation, AI is defined, in particular, in Federal Law No. 123-FZ dated

[15] https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law.

[16] https://www.europarl.europa.eu/RegData/seance_pleniere/textes_adoptes/definitif/2024/03-13/0138/P9_TA(2024)0138_EN.pdf.

[17] https://legislature.vermont.gov/Documents/2024/Docs/BILLS/H-0710/H-0710%20As%20Introduced.pdf; https://lis.virginia.gov/cgi-bin/legp604.exe?241+ful+HB747H1.

24.04.2020: it is a set of technological solutions that allows imitating human cognitive functions (including self-learning and search for solutions without a predetermined algorithm) and obtaining, when performing specific tasks, results comparable, at least, to the results of human intellectual activity. Furthermore, AI technologies include computer vision, natural language processing, speech recognition and synthesis, intellectual decision support and promising methods of artificial intelligence.

It should be noted that the Russian definition of AI technologies largely overlaps with the directions of application of AI systems listed by the OECD; having said that, the very definition of AI based on imitation of cognitive abilities and comparison with the results of human intellectual activity looks controversial, as they are not measurable unambiguously and differ between people.