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

EU vs large platforms, regulation of data brokers, post-quantum cryptography for cybersecurity

Monitoring No. 8 (August 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

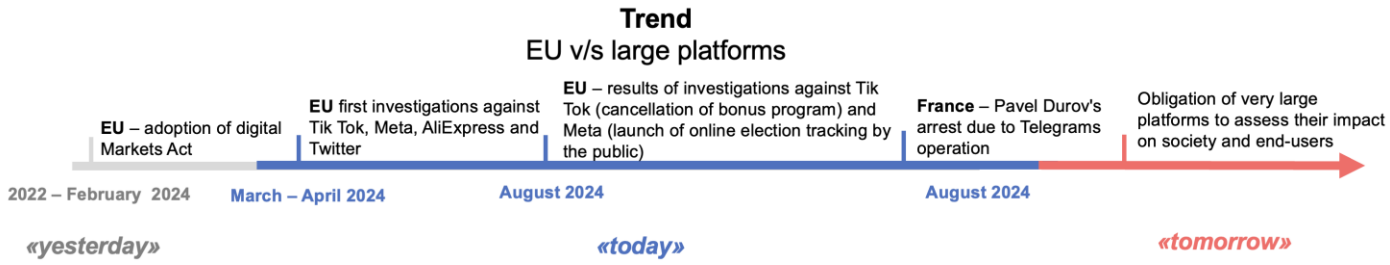
“August is fruitful in every way”.

Anton Chekhov

In August 2024, there were 3 events that define the trends in the development of digital economy regulation in the world.

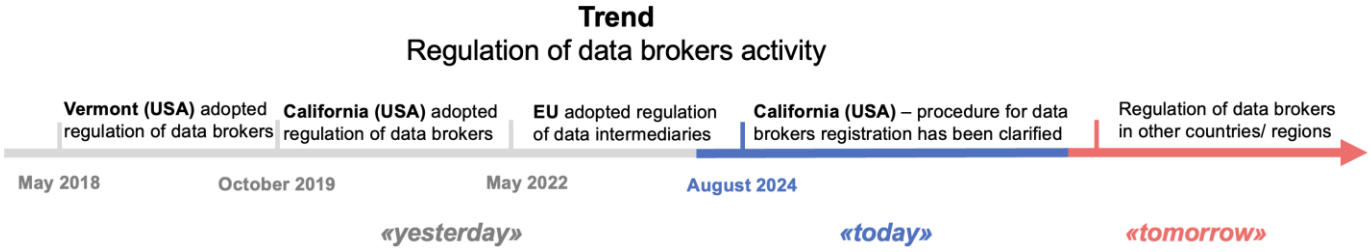
Trend No. 1. EU vs large platforms

In August 2024, the European Commission released certain results of an investigation against VERY LARGE ONLINE PLATFORMS (hereinafter VLAPs) Meta[1] and TikTok for violating the EU Digital Services Act (DSA). In addition, Pavel Durov, founder of Telegram, was arrested in France on charges of creating a social network for illegal purposes. Many of the charges correlate with the norms set for platforms in the EU law. At the same time, Telegram, operating in the EU space, does not yet fall under the regulation of VLOPs, however, the growing number of end-users will force Telegram to comply with these norms in the near future



Trend No. 2. Regulation of data brokers activities

In August 2024, California (USA) drafted clarifications to specify the criteria for recognizing a company as a data broker: for example, if a company sells data of its employees that is not obtained directly from them. In the digital economy, data brokers, by acting as intermediaries between data holders and users, contribute to the growth of their turnover, reducing costs and increasing the confidence of market stakeholders. In recent years, regulation of data brokers has been adopted in the EU and a number of US states. In Russia, there is no such regulation of brokers, which hinders the development of the data market.



Trend No. 3. Post-quantum cryptography for cybersecurity

In August 2024, 3 standards were enacted in the USA defining key establishment schemes for information encryption and digital signatures, designed to withstand future attacks by quantum computers. It is believed that current cryptography (encryption) standards can prove to be powerless. From 2029, Russia is also developing but not yet approved post-quantum cryptography standards. The EU countries are still relying on post-quantum cryptography standards developed in 2024 in the US.

[1] Meta, a company banned on the territory of the Russian Federation, is on the List of organizations and individuals for whom there is information about their involvement in extremist activity or terrorism.

August 2024 saw 2 significant events in Russia:

1. Regulation of cryptocurrencies mining

In August 2024, a federal law was enacted to create a legal framework for the regulation of mining activities, which comes into effect on November 1, 2024.[2] Mining is a process involving devices and software to solve mathematical puzzles and to make entries in an information system that uses distributed ledger technologies such as blockchain, to issue cryptocurrencies and generate income in cryptocurrency for confirming entries in the information system.

The following regulation of mining is proposed:

1) Private entrepreneurs and legal entities can be engaged in mining subject to registration in the directory of those engaged in the mining of digital currency, as well as by individuals - without the need to be entered in the register, but subject to energy consumption limits. It is possible to create a mining pool, i.e. to combine the mining capacities of several miners.

2) Registered miners will have to comply with money laundering and counter-terrorist funding legislation (e.g. customer identification), failing which the miner will be removed from the register.

3) Miners are required to report all digital currency obtained in the mining process - to indicate the address-identifier[3] to which such currency is credited.

4) The government can restrict mining in certain subjects of the Federation or in certain territories of Russia. On the one hand, this will reduce the risks of energy shortages in certain regions (e.g., the Far East), but on the other hand, it may be detrimental to miners, who will incur costs of relocating their activities to other regions.

Thus, the law creates a legal regime for mining without imposing meaningful restrictions.

Moreover, two more important updates were adopted:

1) Ban on any offer to purchase digital currencies to an unlimited number of persons. In fact, the ban on the sale of cryptocurrencies has been enhanced (previously, the ban only applied to the purchase of goods or services for cryptocurrency).

2) Admission of foreign DFAs (digital financial assets) and foreign DFA market participants to Russia:

- introduces the category of foreign digital rights, which effectively gives access to the Russian market for DFAs issued abroad. However, there is a restriction on the purchase of foreign digital rights by Russian individuals: only sole proprietorships or legal entities may purchase them. Access to the Russian market for the foreign DFAs is provided through DFA issuance operators, which must qualify the foreign asset as a DFA.
- gives possibility of Russian DFAs being credited by foreign buyers in accordance with their law rather than Russian law. This effectively allows Russian DFAs to be deposited abroad, while the holders of such DFAs can perform all activities related to the DFAs in the interests of their clients. Foreign participants may buy, hold and further sell abroad Russian-issued DFAs.

[2] https://sozd.duma.gov.ru/bill/237585-8

[3] A unique sequence of symbols intended for recording in the information system of incoming and outgoing transactions with digital money.

An opportunity has been created both to sell Russian DFAs abroad and to trade foreign DFAs in Russia.

2. Strengthening oversight of online content

In August 2024, amendments to the Federal Law “On Information”[4] were adopted to counter the spread of harmful content:

1) Social networks must monitor a new type of banned information that offends “public morality and expresses clear disrespect for society, contains images of unlawful behavior” and is disseminated “for hooligan, mercenary or other base motives." However, it is not clear by what criteria to search for such information in the flow of online content in social networks: what does “immoral and offensive content” look like? It is unclear how to assess “base motives” to classify content as unlawful?

2) Access to information may be restricted not only by federal laws, but also by acts of the President of Russia, which makes it easier to introduce new information bans. The above types of information also fall under extrajudicial blocking of a website (at the initiative of Roskomnadzor).

3) Roskomnadzor is given new powers to manage communication networks through special technical means that communications providers are obliged to install. Roskomnadzor is given the power to directly monitor information flowing through the network and take measures (e.g., block pages with illegal content). Such powers arise at the request of the Prosecutor General upon detection of mass or repeated dissemination of illegal information on the network.

The new regulation supports the trend towards stricter information regulation in two aspects. Firstly, it expands the range of information for which blocking measures are required. For information business, such innovations always raise questions on the part of executors due to unclear criteria for qualifying a new type of restricted information. Secondly, the toughening is expressed in the restriction of telecom operators' competence in relation to their own networks, since in case Roskomnadzor establishes control over the network, the decision on measures to respond to unlawful content is no longer taken by the network operator, but by the state body.

[4] https://www.consultant.ru/document/cons_doc_LAW_482411/

https://www.consultant.ru/law/review/fed/fd2024-08-09.html

Key aspects

1. EU vs large platforms

The EU experience

August 2024 summarized the results of EU investigations into TikTok and Meta for violating the requirements of the Digital Services Act[5] (hereinafter DSA), which came into force in February 2024 and established a few obligations for platforms that operate with unlawful content.

DSA identifies a special category of VERY LARGE ONLINE PLATFORMS - more than 45 million EU users per month. Currently, 19 platforms[6] fall into this category. They have special requirements, non-compliance with which has led to investigations by the European Commission against AliExpress, Meta and Instagram,[7] TikTok and Twitter.

Telegram Messenger also operates in the EU. An investigation against Telegram founder, Pavel Durov, was launched in August 2024.The allegations of violation of French law largely correlate with the rules laid down by the DSA.

Let's look at the investigation against Meta and TikTok, and whether Telegram could be recognized as a VLOPs, and what consequences would that lead to?

Firstly, the VLOPs' status entails several responsibilities:

- Assess at least once a year "systemic risks" (Art. 34) in relation to its services, including content moderation systems, design of recommendation systems, advertising services, etc. Systemic risks include distribution of unlawful content, violation of human dignity, violation of the rights to personal data protection, freedom of speech and information, non-discrimination, child and consumer protection, etc.
- Reduce systems risks (Art. 35), including adaptation of design and interfaces, service functions, content moderation (e.g., speed of response to complaints on unlawful content, prompt removal of such content), algorithmic systems, including recommendation systems, introduction of child protection tools (age verification and parental control), labeling of deepfakes, etc.
- Introduce a crisis response mechanism (Art. 36) to security threats.
- Conduct an independent audit at least once a year (Art. 37) and have an independent compliance mechanism for DSA compliance (Art. 41).
- Have an advertising repository - a repository of information on the ads being placed.
- Provide an option in their recommendation systems that is not based on user profiling.

In August 2024, the Commission's investigation against TikTok in connection with TikTok Lite's "TikTok Lite Challenge and Rewards Program," which allows users to earn points by completing certain "tasks and rewards" such as watching videos, liking content, inviting friends to join TikTok, etc., concluded. Points can be exchanged for Amazon vouchers, PayPal gift cards, TikTok own digital currency, and more. According to the European Commission, the Program was launched without prior assessment of systemic risks, such as the risk of "addictive effect to the platform" of users, and no measures were taken to mitigate such risks, especially in relation to children and their mental health, encouraging addictive behavior. As a result, the TikTok Lite Program was first suspended (in April 2024), and given TikTok's failure to conduct a risk assessment - since August, the Commission decided to ban the Program in the EU.

Also in August, the probe into Meta gained momentum.[8] The probe itself began back in April 2024 since Meta:

- Infringes the requirements to the mechanism for flagging illegal content - the mechanism is not easily accessible and user-friendly, and there is no internal system

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

[6] Alibaba AliExpress, Amazon Store, Apple AppStore, Booking.com, Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, YouTube, Zalando, Bing, Google Search.

[7] Meta, an organization banned on the territory of the Russian Federation, is on the List of organizations and individuals in respect of which there is information about their involvement in extremist activity or terrorism.

[8] https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-meta-under-digital-services-act-2

for handling complaints about content moderation decisions.

- Does not provide tools for civil discourse and real-time election monitoring in the run-up to elections. Meta plans to shut down CrowdTangle, a public information gathering tool for real-time elections monitoring. According to the Commission, shutting down CrowdTangle jeopardizes civil discourse and electoral processes in the EU. Consumers will not be able to monitor misinformation, election interference and ensure overall transparency in real-time by providing facts to journalists and other stakeholders.

In the run-up to the May 2024 elections, Meta included new features in CrowdTangle - 27 publicly available dashboards (1 for each EU state). The features have now been discontinued and the Commission has requested information on the operation of such features for further proceedings in August 2024.

August 2024 saw the arrest of Pavel Durov,[9] the founder of Telegram, accused of complicity in the creation of an online platform for illegal transactions, refusal to provide information on the storage of pornographic images of minors at the request of competent bodies, sale of equipment and programs to gain access to the automated data processing system in order to disrupt its functioning, fraud, provision of cryptological services and import of cryptological tools without their declaring.

However, the accusations are predominantly based on breaching the French law. For example, the Law on confidence in the digital economy[10] stipulates the declaring of cryptologic tools, equipment, and programs to public authorities.

Some charges correlate with the norms enshrined in the DSA, such as the obligation to provide competent bodies with information (Art. 10), the obligation to protect minors (Art. 28), and so on.

It is worth noting, Telegram is not currently recognized as a “very large platform” under the DSA, as it has less than 45 million EU users per month. In addition, Telegram has appointed a legal representative in Belgium in compliance with the DSA. Therefore, for the time being, Telegram cannot yet be subject to investigations like those against Meta and TikTok for breaching the DSA. Nevertheless, soon Telegram's audience may reach more than 45 million people - after that the European Commission itself should define Telegram as a “very large online platform”. In this case, Telegram will have to ensure full compliance with the DSA within 4 months, otherwise it will lead to an investigation by the Commission itself.

Russia’s experience

Russia currently lacks regulation like the EU one, however, there is regulation in terms of monitoring and removal of information recognized as illegal from platforms. However, in Russia, the main method of combating the issue is blocking, and in some cases, for example, when information is disseminated in violation of the law (calls for mass riots, extremist activity, false reports of acts of terrorism), Roskomnadzor has the right to block the information resource without warning. In other cases, Roskomnadzor sends a preliminary request to remove the content, and if the content is not removed, only then does Roskomnadzor have the right to block it.

Moreover, there are special obligations for social networks to take measures to prevent the dissemination of information containing calls to commit criminal acts, terrorist activities, extremism, materials promoting cruelty, violence, etc. Social network must provide a communication channel to receive reports of prohibited information, establish user rules to limit the dissemination of such information, and ensure annual public reporting of monitoring results. For this purpose, social network must provide a communication channel to receive reports on prohibited information, establish user rules to limit the dissemination of such information, and ensure annual public reporting on the results of monitoring.

2. Regulation of data brokers activity

Special regulation for data brokers has emerged since the mid-2010s. In the digital economy, data brokers (intermediaries between

[9] https://www.tribunal-de-paris.justice.fr/sites/default/files/2024-08/2024-08-26%20-%20CP%20TELEGRAM%20.pdf

[10] https://www.legifrance.gouv.fr/codes/section_lc/JORFTEXT000000801164/LEGISCTA000006117690/2020-01-01

sellers and buyers of data) help to reduce transaction costs (e.g., finding the right data set and its seller), enhance trust between market stakeholders (e.g., by making their activities transparent), and thus develop the data market. At the same time, the emergence of an intermediary between data owners and users poses additional risks to security of data in transit, such as data leakage risks. Regulation can enhance the benefits of such persons (e.g., through an open register of data brokers) and reduce the risks of their activities (e.g., through liability measures, including fines for information security breaches).

The U.S. experience (Vermont, California)

In August 2024, California prepared clarifications on the registration of data brokers, including clarifying the criteria for recognizing a company as a data broker: in particular, such criteria include the absence of a "direct relationship" (investor-company, employee-employer, etc.) between the company and data subjects.

Among US states, Vermont (2018)[11] and California (2019)[12] have adopted regulation of data brokers. In these states, data brokers are professional participants whose function is to lawfully collect personal data from various sources (e.g., websites, businesses), transform it to meet market needs, and sell/transmit it under license. In Vermont, for a company to be recognized as a data broker, the data must be in electronic form and prepared for distribution to third parties. However, both states do not recognize as data brokers companies that sell data of their customers, employees, investors, etc., such as an app that sells data of its users.[13]

In both states, data brokers are required to register annually. Registration is done in the period following the activity, i.e., it essentially contains a reporting element. The information provided varies slightly: for example, Vermont requires the number of data security breaches (storage, transmission, etc.), while California requires the number of requests from consumers to exercise their rights (data deletion, etc.) and the reply time.

Vermont also has a requirement for data brokers to have comprehensive information security that includes, but is not limited to, risk assessments, regular review of security measures, and data access controls.

The EU experience

Ita In the EU, the Data Governance Act establishing requirements for data brokering services was adopted in 2022.[14] Brokers provide intermediary services between data holders and users (Article 10(a)).

Unlike the US states mentioned above, the registration of data brokers in the EU is carried out once and before the beginning of their activity, at the same time, as in the US, it has a notification character and the information about the broker, including the description of its services, is published in the unified register.

Otherwise, the EU's approach is tougher than that of the US:

1) Provision of services through a separate legal entity: even if a company is already active in the data sector, intermediary services must be strictly separated from other activities, both legally and commercially.[15]

2) Generally, data should be exchanged in the format where it is received from the data holder. Related services, such as anonymization, only at the explicit request/approval of the data holder. In other words, the EU restricts functions that are part of the core functions of data brokers in the reviewed US states.

3) Mandatory anti-fraud and abuse procedures - in Vermont, verification of the integrity of data consumers is related to best practices but is not mandatory.

Russia's experience

In Russia, there is no special regulation for data brokers. This may discourage data

[11] https://legislature.vermont.gov/bill/status/2018/H.764
[12] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB1202. Сейчас действует редакция 2023 г.: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB362, clarifications to which were issued in 2024: https://cppa.ca.gov/regulations/pdf/data_broker_reg_prop_text.pdf
[13] https://ago.vermont.gov/sites/ago/files/wp-content/uploads/2018/12/2018-12-11-VT-Data-Broker-Regulation-Guidance.pdf, https://cppa.ca.gov/regulations/pdf/data_broker_reg_prop_text.pdf,
[14] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0868
[15] Micheli M., Farrell E. et al. Mapping the landscape of data intermediaries. Emerging models for more inclusive data governance. JRC Science for Policy Report. European Commission, 2023, c. 23.

sharing in the economy, increasing the costs of finding counterparties and concluding contracts, and not contributing to the development of trust in the data market. For example, it makes it difficult to hold professional data market shareholders liable: when data processing is delegated to a data consumer, the data consumer is responsible for the fulfillment of the operator's obligations. In this regard, it is advisable to define the rights, duties and responsibilities of professional data market stakeholders in the laws on personal data and on information.

3. Post-quantum cryptography for cybersecurity

In Monitoring No. 2 we have already examined the trend towards standardization in the field of quantum technologies in some countries (USA, UK) with a focus on the security aspects of such technologies.

Cryptography is essential in the digital economy, protecting electronically stored and transmitted information such as emails, medical records and billing data. Cryptography is based on mathematical problems that are too difficult or impossible for conventional computers to solve. But with the advent of quantum computers, characterized by the power and speed of computation, many such problems become solvable, which jeopardizes both the confidentiality of personal information and the security of critical infrastructure, such as power supply. In this regard, the development and implementation of standards of post-quantum cryptography, i.e., based on tasks that are beyond the power of either conventional or quantum computers, is relevant - such a task, for example, is a learning-with-error (LWE) problem.

The US experience

In August 2024, the first 3 post-quantum cryptography standards were adopted in the US: 1 on key-encapsulation[16] for information transmitted over networks and 2 (primary and backup, based on a different mathematical approach) for digital signatures.[17]

The National Institute of Standards and Technology (NIST)[18] began developing post-quantum cryptography standards in 2017 and selected options in 3 phases, including security assessments and performance benchmarking.

The technical solutions contained in the standards are resistant to attacks by quantum computers. For example, in the standard on key-encapsulation,[19] the solution for establishing a secret key that can then be used for encryption and authentication is based on the computational complexity of a learning-with-error (LWE) problem.

Despite the fact that this is essentially a matter of preparing for future threats, in the U.S. as early as 2023, prior to the adoption of these standards, all organizations were encouraged to begin planning for the transition to post-quantum cryptography standards.[20]

The EU experience

In contrast to the US, the EU is currently discussing more general parameters. In April 2024, the European Commission's recommendations for the transition to post-quantum cryptography were adopted to define goals, milestones, and timelines for the formation of a joint roadmap. [21]

In the mean time, at the level of member states (e.g., Germany, France, the Netherlands and Sweden[22]), data protection authorities are urging companies to take steps toward quantum-resistant encryption now. According to the agencies of these countries, the focus should be on post-quantum cryptography available on existing hardware, including using the standards developed by the US NIST.

[16] A scheme that can be used to establish a shared secret key between two parties communicating over a public channel.
[17] https://www.federalregister.gov/documents/2024/08/14/2024-17956/announcing-issuance-of-federal-information-processing-standards-fips-fips-203-module-lattice-based; https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
[18] Refers to the Department of Commerce.
[19] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf
[20] https://www.cisa.gov/news-events/news/cisa-nsa-and-nist-publish-new-resource-migrating-post-quantum-cryptography
[21] https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography
[22] https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/240126_QKD-Positionspapier.html; https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.pdf?__blob=publicationFile&v=4

Russia's experience

Since 2019, the development of national standards for post-quantum cryptographic information protection in Russia has been carried out by working group 2.5 "Post-quantum cryptographic mechanisms" of the Technical Committee for Standardization "Cryptography and Security Mechanisms" (TC26).[23] TC26 works under the direction of Rosstandart and the Federal Security Service of Russia.[24]

In 2023, within TC26 a post-quantum electronic signature algorithm "Shipovnik" based on the problem of decoding a random linear code[25] was developed, and in March 2024 - a post-quantum key-encapsulation scheme "Codium" for the protection of information transmitted in networks, including communications, based on the same class of mathematical problems.[26] A draft standard using this scheme is being prepared.

[23] https://tc26.ru/about/structure/
[24] https://tc26.ru/about/
[25] https://kryptonite.ru/news/postkvantovyi-algoritm-shipovnik-realisatsiya/
[26] https://habr.com/ru/companies/kryptonite/articles/802121/; https://tc26.ru/news/novosti-kriptografii/v-rossii-razrabotan-kriptograficheskiy-mekhanizm-sposobnyy-vyderzhivat-ataki-kvantovykh-kompyuterov.html?sphrase_id=77397