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

- VAT and digital services in the EU
- AI in housing
- Internet safety for children and businesses
- New cybersecurity requirements in the EU
- Government procurement of high-risk AI

Monitoring No. 3 (15) (March 2025)

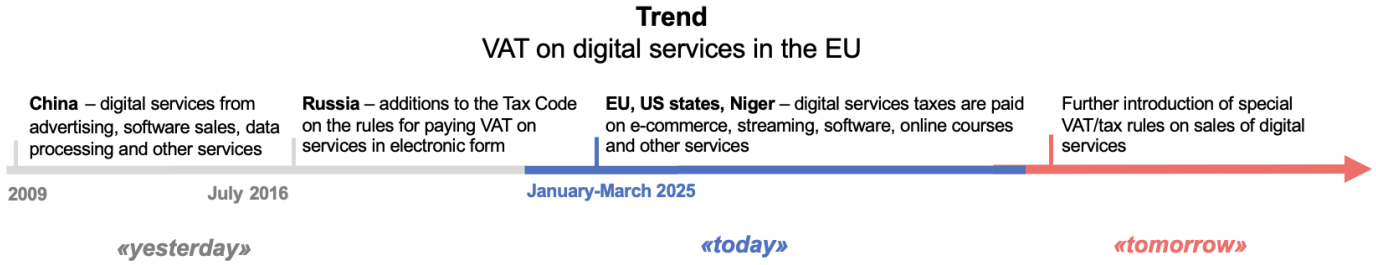
Monitoring was prepared by a team of experts of the Gaidar Institute for Economic Policy (the Gaidar Institute):
Antonina Levashenko, Senior Researcher, International Best Practices Analysis Department, Gaidar Institute.
Maria Girich, Researcher, International Best Practices Analysis Department, Gaidar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

«The spirit of spicy March was in the moonlit circle,
The sand crunched beneath the melted snow.
My city melted in the wet blizzard,
Sobbing in love at someone's feet..»
А. Блок

In March 2025, there 5 events that define the trends in the development of digital regulation in the world.

Trends No. 1. VAT and digital services in the EU

In March 2025, the EU adopted amendments to the Single VAT Regulation to require short-term rental and passenger service platforms to store information about their business users. This is to ensure that platforms (like Airbnb or Uber) pay VAT themselves for those who provide services through them.



Trend No. 2. AI in housing

In March 2025, the state of Georgia (US) proposed limiting the use of AI to determine rental prices for homes.

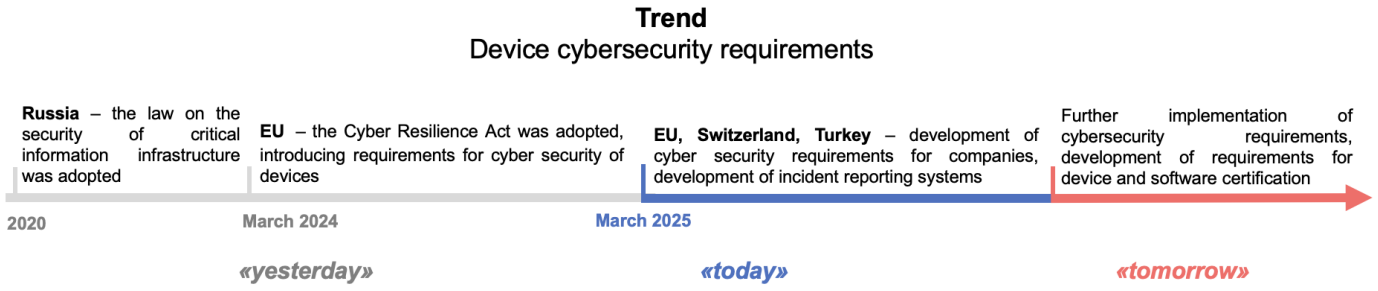
Trend No. 3. Internet safety for children and businesses

Strengthening requirements for children's safety on the Internet (discussed in the Monitoring Report No. 4 for 2024) may face resistance from businesses. In March 2025, a court in the state of California (USA) issued a preliminary injunction against the application of the norms of Age-Appropriate Design CODE Act (CAADCA), recognizing it as contrary to the US Constitution

Trend No. 4. New cybersecurity requirements in the EU

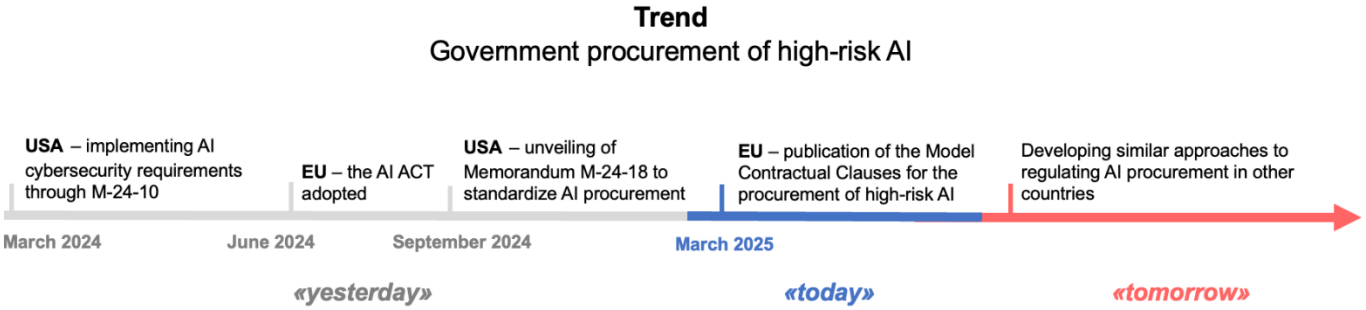
In March 2025, the EU published a description of the goods and software that will be subject to cybersecurity requirements. Without compliance, products will not be able to be sold on the European market. Imposing cybersecurity requirements directly on manufactured goods, rather than on the manufacturing company as a whole, is an approach that is currently unparalleled in other jurisdictions.

In March 2025, other jurisdictions focused on the development of traditional cybersecurity tools: Switzerland and Turkey have introduced requirements for reporting incidents to government agencies.



Trend No. 5. Government procurement of high-risk AI

In March 2025, the EU proposed the Model Contractual Clauses for public procurement contracts for high-risk AI systems.



In March 2025, Russia introduced a ban on the distribution of advertising on the platforms of undesirable and banned organizations,[1] in particular those whose activities are recognized as extremist and terrorist. In fact, this means a ban on advertising through Meta[2] resources (Instagram and Facebook), except for WhatsApp.

[1] Federal Law of 07.04.2025 No. 72-FZ "On Amending Article 12 of the Federal Law 'On Combating Extremist Activity' and the Federal Law 'On Advertising'"

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

Key aspects

1. VAT on digital services in the EU

The EU experience

In March 2025, amendments to EU Regulation No. 282/2011 were adopted.[3] The EU VAT in the Digital Age (ViDA) initiative extends the concept of deemed supplier introduced in 2021. The concept means that, in certain cases, platforms are deemed to be responsible for paying VAT on behalf of their business customers, as if those platforms were selling goods or services themselves. Previously, this concept applied to platforms for facilitating a supply of goods, primarily imported ones. From July 2028, the same rules will apply to platforms through which short-term rentals (up to 30 days) and passenger transport services are provided. Such platforms will charge and pay VAT on behalf of landlords and cab drivers. However, if a platform provides only services for placing advertisements, redirecting users to third-party resources or processing payments, it will not be considered a "deemed supplier".[4]

Platforms are also exempt from liability for incorrect VAT calculation if they acted on the basis of unreliable information from a supplier and could not have known of its unreliability. Platforms are required to collect and store additional information on suppliers and transactions, even if the deemed supplier regime does not apply, for comparison with payment data collected under the new tax control system for persons providing services through platforms.

The platform fulfills the requirements of a deemed supplier if the business user has a VAT number,[5] and if there is no VAT number, the business user is responsible for paying VAT.

The US experience (at state level)

In March 2025, Maryland published a bill that would impose a 3% sales tax on information services, including website development and cloud storage solutions, data processing, computer system design services for online publishing, online broadcasting, search engines, and related services.[6]

That said, New York City proposed special indirect taxes on services as early as January 2025:

1) Digital advertising. Rates from 2.5% to 10% depending on the company's gross revenue from all sources for the year.[7]

2) Excise tax on the collection of consumer data by commercial data collectors,[8] processing information from more than 1 million consumers per month.[9]

The experience of Niger

From 2025, Niger has introduced a 19% VAT on sales of goods and services made through both foreign and local e-commerce platforms, as well as on commissions received by the operators of these platforms. To fulfill their tax obligations, non-resident platforms are required to appoint a representative resident in Niger.[10]

Russia's experience

Article 174.2 of the Tax Code of the Russian Federation has been in force in Russia since 2017 regulating the taxation of services provided in electronic form, such as the provision of rights to use computer programs and databases via the internet, including updates and additional functions, and the provision of online advertising services. This norm was introduced to create uniform rules for the taxation of digital services in the EAEU.

As a general rule, foreign organizations providing electronic services to Russian individuals are obliged to calculate and pay VAT independently. Where such services are provided to Russian organizations or individual entrepreneurs, the obligation to pay VAT is imposed on Russian purchasers as tax agents.

[3] Regulation laying down measures for the implementation of Directive 2006/112/EC on a common system of value added taxation.
[4] https://data.consilium.europa.eu/doc/document/ST-14963-2024-INIT/en/pdf
[5] Individual identification number of the taxpayer registered for VAT assessment and payment purposes.
[6] https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/hb155
[7] https://www.nysenate.gov/legislation/bills/2025/S173
[8] Collection, use, processing, sale or other transfer of data that identifies, relates to, describes or can be reasonably linked to users.
[9] https://www.nysenate.gov/legislation/bills/2025/A1434
[10] https://www.impots.gouv.ne/media/loi/ORDONNANCE%20N%202024-59%20LOI%20DE%20FINANCES%202025..pdf

2. AI in housing

The US experience

In March 2025, a bill was proposed in the state of Georgia (USA)[11] that would prohibit the use of AI in the housing practices if (1) the generation of decisions to sell, rent, finance housing (e.g., mortgages), and (2) the provision of intermediary services (e.g., platform services) or related services (e.g., the delivery of AI-enabled applications to sell or rent housing) occurs without human intervention - without a responsible person reviewing the AI decisions. It is proposed to introduce liability for cases where the user is not warned that an AI or other automated decision tool was used in generating the solutions.

Similar bills have been proposed in other states. For example, as early as 2024, Colorado proposed to recognize as an unfair or deceptive trade practice the use of algorithms in setting rents amount (bill rejected).[12]

New York[13] proposed (bill rejected) to prohibit a landlord from using automated decision tools, including AI, unless a developer conducts a disparate impact analysis to assess the actual impact of any automated decision tool at least once a year. The results of the impact assessment shall be made publicly available on the website of the landlord prior to the use of such tool.

Impact assessment includes testing the extent to which the use of an automated decision tool may result in adverse impacts on a group of individuals based on gender, race, ethnicity, and so forth. The landlord should notify any applicant about the use of AI, any such applicant characteristics that the tool will take into account when making rental decisions, provide information about the type, source of data used, and the landlord's data retention policy. If an application for housing is denied, the reason for such denial.

New York is currently considering Bill A 10020[14] regarding pricing algorithms - any computational process, including AI, that processes data to recommend prices or terms in the housing practices. It is proposed to prohibit algorithmic pricing tools that use or have been trained on competitors' private data from being used in setting rents. Such data includes non-public data that may be shared by landlords, for example, if they use the same application to set housing prices, providing information on housing costs, housing quality (number of rooms, condition), previous rental housing contracts.

Much of this regulation and the attempt to limit the use of AI is due to the risks of anti-competitive behavior and price collusion that drive up housing prices. For example, due to the use of AI-enabled apps that help landlords set housing prices, prices in the US rental real estate market increased by 20% from 2020 to 2024.

Russia's experience

In Russia, AI is used by housing search platforms (e.g. on Cian), but there is no specific regulation.

3. Internet safety for children and businesses

The US experience

In March 2025, a California state court issued a preliminary injunction against enforcement of California's Age-Appropriate Design Code (effective since January 2025),[15] finding the Code unconstitutional. The Code establishes requirements to protect minor users.[16] Subjects are large digital platforms with revenues in excess of $25 million or companies selling data from more than 100,000 users.

The Netchoice Association (comprising Google, Meta,[17] Amazon, Netflix) has sued in a California court claiming the Code of Amendments to the US Constitution and other laws are violated because the Code:

1) Violates the 1st Amendment to the US Constitution on freedom of speech because it restricts the flow of information. Freedom of speech in the US constitutional law is interpreted broadly, including the right to express opinions

[11] https://www.legis.ga.gov/legislation/71101

[12] https://custom.statenet.com/public/resources.cgi?mode=show_text&id=ID:bill:CO2024000H1057&verid=CO2024000H1057_20240110_0_I&

[13] https://custom.statenet.com/public/resources.cgi?mode=show_text&id=ID:bill:NY2023000A7906&verid=NY2023000A7906_20230719_0_I&

[14] https://custom.statenet.com/public/resources.cgi?mode=show_text&id=ID:bill:NY2023000A10020&verid=NY2023000A10020_20240501_0_I&

[15] https://netchoice.org/wp-content/uploads/2024/11/2024-11-12-NetChoice-v-Bonta-2024-Complaint-FILED.pdf

[16] For example, age estimation requirement, default privacy settings, monitoring signal

[17] Recognized as an extremist organization and banned in Russia

through information resources - any requirements related to mandatory content moderation may limit freedom of speech.

The Code assigns platforms the role of censors, requiring them to assess what content is “harmful” or likely to cause “material damage to a child's health”. Platforms use their own discretion in deciding what information to restrict, as there are no clear criteria for “harmful information”.

2) Violates the 4th Amendment to the US Constitution, the right to privacy, by requiring verification of a user's age. Such a requirement necessitates the collection of as much personal data as possible, which is contrary to the principle of “minimizing data collection”.

3) Violates the 14th Amendment to the US Constitution due process clause because it contains many vague concepts: what is “material detriment to a child's health”, “harmful content”? The Code requires data to be processed strictly for one purpose, but allows data to be used for a new purpose, if there is “a compelling reason that an alternative setting is in the best interests of children.” The criteria of “best interests” and “weight of evidence” are not disclosed.

4) Conflicts with other laws. For example, a child is defined as a person under the age of 18, which contradicts the 1998 Children's Internet Privacy Act, which covers users under the age of 13 as “children”.

The California court found NetChoice's arguments valid for issuing a temporary injunction against the application of the disputed rules, which will remain in effect until the court makes a final decision on the merits.

Russia’s experience

In Russia, the safety of children on the Internet is regulated by the provisions of the Federal Law No. 436 “On the Protection of Children from Information” of 2010. The law encompasses only the display of dangerous information to children, such as propaganda of pedophilia or information motivating sex change, etc. The law does not stipulate requirements to provide parental control tools for child information security. The Law on Information imposes an obligation on social networks to monitor content on the platform to prevent the dissemination of information prohibited in Russia, including information dangerous for children (Clause 5, Article 10.6, Federal Law No. 149). Social networks are obliged to form public reports on the results of content monitoring.

4. New cybersecurity requirements in the EU

The EU experience

In March 2025, the European Commission published a draft implementing regulation that formulated technical descriptions of the categories of products that are classified as important and critical[18] and will be subject to the Union's cybersecurity requirements. The adoption of the draft is expected to increase the requirements and cost for companies to enter the European market.

The formation of cybersecurity requirements in the EU began as early as the adoption of the 2020 Cybersecurity Strategy. It was proposed to develop requirements for cyber risk management in companies and individual infrastructure facilities, as well as requirements for cybersecurity of end products (goods and software) used by companies and consumers. The increased focus on end products is due to the paradigm shift in data storage, processing and transmission: from storage and processing in centralized data warehouses to the development of edge computing, i.e. when data is processed directly on the device.

In October 2024, the EU adopted the Regulation on horizontal cybersecurity requirements,[19] which requires all manufacturers and importers of goods with “digital elements” to implement product cybersecurity standards.[20] Such goods include software or hardware products that have remote data processing functionality. In other words, any product that involves connection to the Internet (or other network) for data processing is subject to the regulation. The regulation covers both consumer products (e.g. smart home products) and industrial ones.

The Regulation identifies 3 categories of products that are subject to increased cybersecurity requirements:

1) Important products (class 1) - routers, password manager programs, VPNs, etc. Such products are subject to the requirements of compliance with the European cybersecurity

[18] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14449-Technical-description-of-important-and-critical-products-with-digital-elements_en

[19] https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

[20] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847

standard, but without certification of such compliance, or, if there is no such standard, with the general requirements to be established by the EC.

2) Important products (Class 2) - firewalls;[21] hypervisors,[22] etc. These products are also subject to compliance requirements, but compliance must be certified by a third-party organization (e.g., a business association).

3) Critical products - smart cards (bank cards; identity cards; cards used as electronic wallets or key storage devices), smart meter gateways used for electricity measurement,[23] etc. These products are already subject to European Common Criteria (EUCC) certification requirements, which imply certification only by organizations that have received special accreditation from government agencies.

For the remaining product categories, the manufacturer will independently assess cybersecurity risks. The EC estimates that up to 90% of all products will fall into this category. The requirements of the regulation will come into effect from December 2027.

The draft implementing regulations published in March 2025 clarify what applies to certain products. This allows companies to better understand the requirements being imposed. For example, password managers include both software and hardware devices designed to store passwords.

The experience of Switzerland

In March 2025, Switzerland adopted a regulation that requires operators of critical infrastructure (energy and drinking water suppliers, transportation companies, cantonal and municipal administrations) to report cyber attacks to the National Cyber Security Center (NCSC) within 24 hours of discovery.[24]

Cyberattacks that threaten the operation of critical infrastructure, leak or alter information, or are accompanied by extortion, threats or coercion are subject to mandatory reporting. Operators who fail to comply with the requirement may be fined.

After submitting the initial report within 24 hours of discovering the incident, organizations will have 14 days to complete their report about the incident.

It is noteworthy that a similar system has already been established in the EU, as we mentioned in Monitoring No. 3 for 2024. In addition, the EU regulation on digital elements described above also envisages the introduction of a system of notification by manufacturers of such products of identified vulnerabilities - the requirement will apply from September 2026.

The experience of Turkey, Vietnam

In March 2025, Turkey's Cybersecurity Law came into force, stipulating obligations and measures for individual companies and government agencies to implement cybersecurity measures, including incident reporting, the ability to purchase certified cybersecurity products, and more.[25]

The Vietnamese government has finalized a public consultation on requiring individual companies to implement a cyber risk management system, conduct regular security audits, and develop incident response plans to mitigate cyber threats.[26]

Russia's experience

In Russia, since 2017, the Law "On the Security of Critical Information Infrastructure" has been in force, which, as well as similar norms adopted in the EU, Switzerland and other countries, provides for a mechanism for reporting computer incidents and also requires to ensure the security of significant critical information infrastructure objects.

5. Government procurement of high-risk AI

The EU experience

In March 2025, the EU published model contractual clauses for public procurement of high-risk AI systems (MCC-AI-High-Risk),[27]

[21] Software that filters incoming information and keeps out malicious content and viruses.
[22] Software that is used to run multiple operating systems on a single device and is responsible for providing computing resources to each operating system during use.
[23] A communication device capable of transmitting and receiving data for information, monitoring and control purposes.
[24] https://www.admin.ch/gov/en/start/documentation/media-releases/media-releases-federal-council.msg-id-104400.html
[25] https://www.resmigazete.gov.tr/eskiler/2025/03/20250319-1.htm
[26] https://xaydungchinhsach.chinhphu.vn/toan-van-du-thao-nghi-dinh-quy-dinh-chi-tiet-mot-so-dieu-va-bien-phap-thi-hanh-luat-du-lieu-du-thao-2-119250123120619898.htm
[27] https://public-buyers-community.ec.europa.eu/communities/procurement-ai/resources/updated-eu-ai-model-contractual-clauses

which public contractors can include in contracts with suppliers of AI systems. The Regulation of EU AI Act[28] defines high-risk AI as systems related to critical infrastructure, biometrics, human rights, education, employment and justice.

MCC-AI-High-Risk establishes typical vendor contractual obligations, including establishing a risk management system, ensuring data quality, transparency of AI system operations, human oversight of AI-generated solutions, etc., as required by the AI Act, (discussed in Monitoring No. 3 for 2024).

From a procurement perspective, the primary concern is securing the rights to the data being used. MCC-AI-High-Risk distinguishes between customer and supplier data. The customer's data (whether transferred by a public body or specifically collected for it) remains the property of the customer, while the supplier may not use it outside the scope of the contract and must return or destroy it on demand. Supplier data (such as models and training datasets) remain under the supplier's control, but the customer is granted a non-exclusive license to use them as part of system operation. To ensure compliance with all contract requirements, the customer may request supporting documentation and audits from the supplier at all stages (design, implementation and operation).

MCC-AI-High-Risk obliges to include in the original contract price all costs associated with meeting AI Act requirements, including audit costs, preparation of supporting documentation, implementation of transparency mechanisms, etc.

The US experience

In the United States, in September 2024, Office of Management and Budget of the President (OMB) issued Memorandum M-24-18[29] to standardize the procurement of AI systems by federal agencies. The document emphasizes procurement of particularly high-risk AI:

- Rights-affecting systems that impact on human rights (e.g. automatic selection in employment). Contractual terms should include mandatory transparency measures, remedial mechanisms and mandatory human review of disputed decisions.
- Systems that affect safety - impacting the health and lives of citizens, infrastructure, etc. (e.g., transportation management systems, energy management systems, etc.). (e.g., transportation and energy management systems). The procurement should be accompanied by full access to information on the development of the system, allowing to assess its reliability and prevent negative consequences.

It is recommended that the following conditions includedin contracts to regulate AI:

- Use of test data sets generated by the government customer for independent verification of the supplied AI. Such sets should not be available to the contractor in advance and should mimic as closely as possible the real data with which the AI system will work.
- The contractor's obligation to provide access for the state customer to conduct tests under conditions close to the actual conditions of system use (similar requirement in the EU).
- The right of the state customer to publish the methods and results of system testing (without violating the supplier's intellectual property rights).

The Memorandum establishes requirements for:

- Generative AI - by mandating content labeling (e.g. watermarking), providing detailed documentation on training and testing methods, etc.
- Biometric AI that performs personal identification - requires independent tests for recognition accuracy, compliance with input data quality standards, setting search accuracy thresholds and mandatory maintenance of secure logs of queries and identifications.

The Memorandum reinforces contractors' obligation to notify agencies of serious AI incidents to promptly respond and prevent negative consequences.

Russia’s experience

Currently Russia lacks specialized regulation for state procurement of AI systems. However, GOST R 71752-2024 “Artificial Intelligence. Terms of Reference” which establishes requirements for technical specifications for the procurement and implementation of AI systems, including public and commercial procurement.

[28] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

[29] https://www.whitehouse.gov/wp-content/uploads/2024/10/M-24-18-AI-Acquisition-Memorandum.pdf

The Russian Ministry of Finance developed Methodological Recommendations on Digital Transformation, which recommend integrating AI into the business processes of government organizations, forming strategies for the use of AI and assessing the effectiveness of implemented solutions.