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

- Competition in technology transfer
- Tax equalization of e-commerce
- Tokenization of the financial market
- Risks of quantum computers
- Cross-border data transfer
- Protecting users of the Internet of Things
- Personal data for AI

*Monitoring No. 10 (22) (October 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
*Diana Golovanova*, Researcher, Economic Policy Foundation

*„Those who lived to see October*
*Did not labor in vain.*
*In October, as in March,*
*Our hearts are alive,*
*but our minds are extinguished".*
*Konstantin Balmont*

In October 2025, we can identify 7 events that define trends in the development of digital economy regulation globally.

## Trend No. 1. Competition in technology transfer

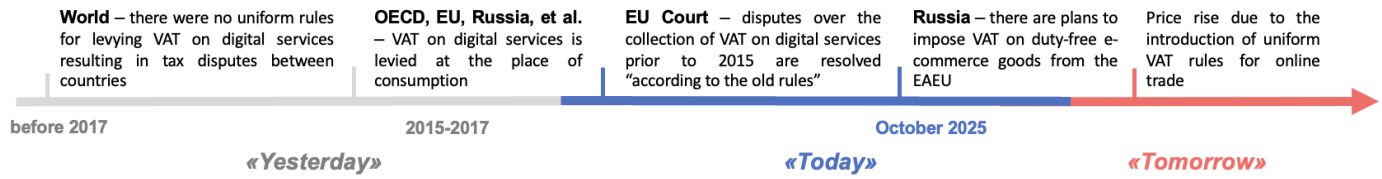
In October 2025, a draft regulation was presented to the EU defining the terms and conditions under which technology transfer agreements between companies would not be considered anti-competitive. Russia proposed limiting antitrust immunity for intellectual property rights holders.

**Trend**
Competition in technology transfer


## Trend No. 2. Tax equalization of e-commerce

In October 2025, the EU Court ruled that VAT on online services provided prior to 2015 is levied at the location of the supplier, and after 2015 – at the location of the user. This trend is linked to countries' transition to uniform VAT rules for online services developed by the OECD. In Russia, the Ministry of Finance plans to levy VAT on goods purchased online from the EAEU countries.

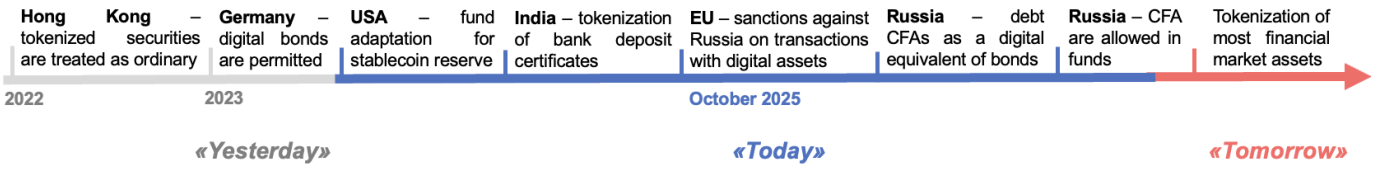
**Trend**
Tax equalization of e-commerce




## Trend No. 3. Tokenization of the financial market

In October 2025, bills aimed at developing the digital financial assets (DFA) market were submitted to the Russian State Duma: funds will be allowed to purchase such assets, and a new DFA asset, bonds, will appear in the legislation. The changes are taking place against the backdrop of the development of the tokenization market in India, the US, and Hong Kong.

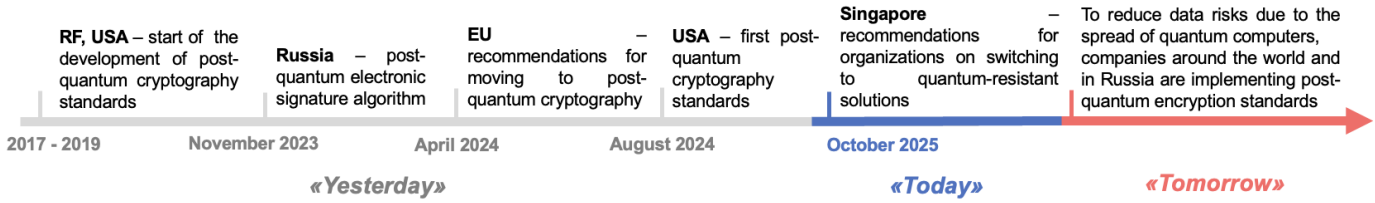
**Trend**
Tokenization of the financial market




## Trend No. 4. Risks of quantum computers

In October 2025, Singapore released a draft guide on implementing "quantum-resistant solutions" to prevent sensitive data leaks and critical infrastructure failures, as quantum computers are becoming more widespread. The Quantum Readiness Index has also been developed.

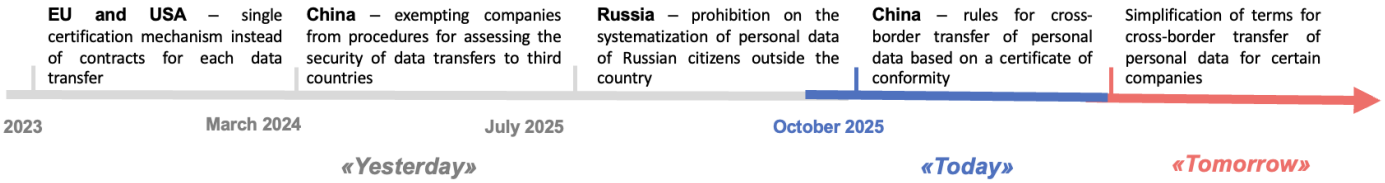
**Trend**
Risks of quantum computers




## Trend No. 5. Cross-border data transfer

In October 2025, China adopted rules for simplified cross-border transfer of personal data: instead of undergoing regular data export security assessments, it is possible to obtain a three-year security certification for data transfer.

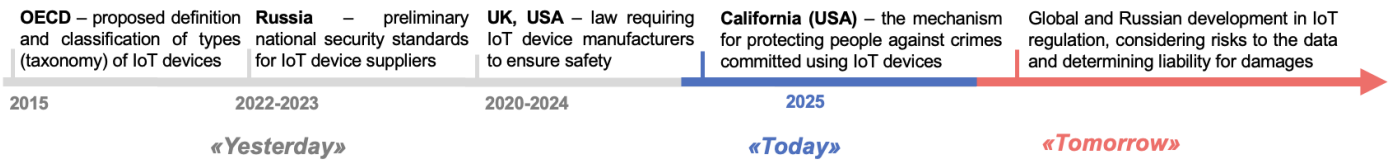
**Trend**
Cross-border data transfer




## Trend No.6. Protecting users of the Internet of Things

In October 2025, the United States passed a law to protect victims who are harmed by malicious actors using Internet of Things devices.

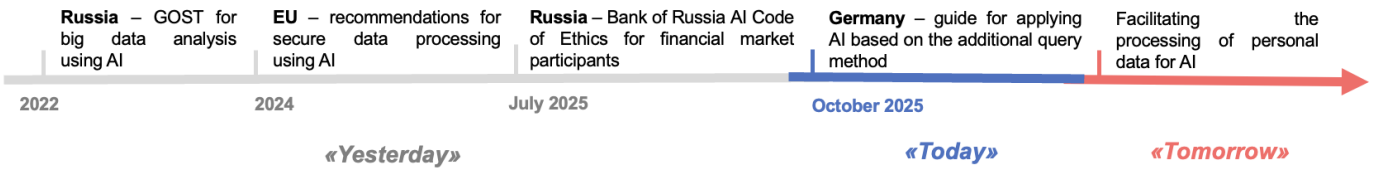
**Trend**
Protection of Internet of Things users




## Trend No. 7. Personal data for AI

Germany has developed guidelines for organizations that use AI technologies with a method for contextual clarification of user queries.

**Trend**
Personal data for AI




Also, in October 2025, Russia **regulated paid subscriptions to digital services.** Now consumers have the right[1] to cancel their paid subscriptions and delete their bank card details. Apps and websites are not allowed to debit funds without the consumer's permission if the consumer has canceled their subscription. According to research, 50% of users in Russia are subscribed to services that do not correspond to the stated subscription offer.[2] Half of these users requested to cancel their subscription,

[1] Federal Law No. 376-FZ of October 15, 2025, "On Amending Article 16-1 of the Law of the Russian Federation 'On Protection of Consumer Rights'"
[2] https://nemkin.ai/tpost/785uhpmso1-podpiski-kotorie-nam-navyazali-millioni

but most were unable to get their money back. In the EU, up to 10% of consumers have encountered such debits.[3]

Thus, the law minimizes the risks of illegal debits, but the rules could be supplemented with a warning that after the “free trial” version, the subscription becomes paid, and the establishment of a clear unsubscribe mechanism for consumers, etc. The EU experience is also interesting, where within two weeks of purchase, consumers can “return” their subscription and get a refund for the unused period of the subscription.

[3] https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/coordinated-actions/consumer-frequent-traps-and-scams_en

# Key aspects

## 1. Competition in technology transfer

### The EU experience

In October 2025, the EU presented draft rules that would automatically exempt certain technology transfer agreements[4] from being deemed anti-competitive[5] until intellectual property rights expired or the know-how became common knowledge. The exemption applies if the agreement is concluded between competing undertakings with a combined market share of no more than 20%, or up to 30% if the undertakings are not competitors. The exemption does not apply where the agreement contains an obligation for the licensee to purchase certain goods or components from the right holder.

If companies are competing, the agreement must not:

- restrict the parties' right to independently set prices when selling products.
- restrict production volumes.
- be aimed at dividing markets or customers (except in cases where, for example, the licensee produces goods only for itself or for a single customer).
- restrict the licensee's right to use its own rights to technology or to conduct R&D (unless the restriction is truly necessary to prevent the know-how from leaking to third parties).

If the parties to the agreement are not competitors, the agreement must not:

- restrict a party's ability to set prices.
- restrict the territory or customers where the licensee may engage in “passive”[6] sales to customers.

The rules prohibit clauses requiring the licensee to grant the licensor or a third party an exclusive license or to transfer improvements to the licensed technology or developments.

The measures presented allow companies to conclude technology transfer agreements more freely, stimulating the spread of innovation, while attempting to prevent technologies from being used to cover up anti-competitive agreements and hidden cartels, and patents and know-how from becoming a tool for dividing markets, fixing prices, excluding competitors, and blocking third parties.

### Russia’s experience

In Russia, the ban on anti-competitive agreements and rules on abuse of dominance do not generally apply to agreements on the transfer or alienation of intellectual property rights, which potentially affects technology transfer. However, in October 2025, the Federal Antimonopoly Service published a draft law that could remove this immunity.[7] It is proposed to limit the cases in which immunity applies, which will be determined by the government. Thus, while the EU is taking an approach of softening the current strict rules, Russia is, on the contrary, reducing existing privileges.

The number of technology transfer agreements is expected to increase: annual market growth of 11.7% until 2035.[8] A trend towards hybrid regulation can be expected: encouraging freedom of technology transfer agreements, but with increased monitoring of agreements with a high risk of restricting competition, especially for large companies.

## 2. Tax equalization of e-commerce

### The EU experience

In October 2025, the EU Court ruled on a dispute over the collection of VAT on in-app purchases made prior to 2015 through an app store platform operated by a company in Ireland. After 2015, the German tax authorities audited German mobile game developer XYRALITY, which sold content within its apps through the AppStore, whose owner is registered in Ireland. The German tax authority decided that although the payments went through Ireland, the actual buyers were located in Germany, so the company was allegedly obliged to pay VAT in Germany.

The German tax authority took the position that the AppStore was only an

[4] A technology transfer agreement is a license agreement for technology rights or an assignment of technology rights concluded between undertakings for the production of goods by the licensee or its subcontractors. The rights to know-how (trade secrets), as well as patents, utility models or designs, semiconductor product topographies, drug patents, software copyrights, etc. are transferred..

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C_202505024

[6] “Active sales” means actively soliciting customers through visits, letters, emails, phone calls, or other means of direct communication, or through targeted advertising and promotion, offline or online.

“Passive sales” are sales made in response to requests from individual customers, where the sale was not initiated by actively targeting a specific customer or territory, as well as sales made as a result of participation in government procurement or in response to private invitations to tender.

[7] https://regulation.gov.ru/projects/159126/

[8] https://www.researchnester.com/reports/technology-licensing-market/8210

intermediary for processing payments, and that the supplier to users was the German developer, meaning that VAT should be charged in Germany. In addition, the authority argued that XYRALITY was listed as the service provider in the purchase confirmations, which allegedly confirmed the company's obligation to pay VAT. XYRALITY, on the other hand, claimed that the AppStore acted "in its own name but on behalf of" the company, and therefore it was the AppStore that was considered the supplier to end users, with the developer merely providing a service to the platform. Consequently, VAT should be paid in Ireland, not Germany.

The EU Court referred to Article 28 of the EU VAT Directive:[9] if a taxable person takes part in the provision of a service "in his own name but on behalf of" another person, then for VAT purposes they are considered to have received and then provided the same service – they are recognized as the supplier to the end buyer. The court identified two instances of service (content) provision in the case: from the developer to the App Store, which is a B2B transaction, and the place of supply is Ireland because that is where the platform is located; and from the App Store to the user, which is a B2C sale, and the place of supply is determined by the location of the supplier, i.e., also Ireland. This means that VAT is due in Ireland, not Germany.

Notably, since 2017, the OECD has established the principle of taxation at the place of consumption: VAT on international services must be paid where final consumption takes place. For digital services purchased by individuals (B2C), this is the country of residence of the buyer, and for B2B supplies, it is the country where the buyer is located. When determining the parties to a transaction, the OECD suggests proceeding from who is listed as the buyer and seller in the contract or invoice. At the same time, the direct provision of a service to a third party or payment by a third party does not change who is considered the supplier or the place of taxation. In other words, the EU Court applied the "supplier location" model (Ireland as the AppStore jurisdiction) that was in force in the EU during the disputed period (2012-2014), while the OECD describes the "consumer location" model.

The approach formulated by the OECD is now generally accepted worldwide, whereas previously countries collected VAT on digital services in different ways. This led to tax disputes between businesses and authorities, as well as between countries. The case in question shows that this problem is still relevant today, even though the OECD's unified approach was developed eight years ago. It is important for digital companies to remember that VAT claims for digital services in Russia until 2017 (in the EU until 2015) must be considered in accordance with the rules for determining jurisdiction that were in force at the time. In some cases, VAT was payable at the location of the service recipient (user), in others – at the location of the supplier (developer or platform owner).

## Russia's experience

In Russia, until 2017, online services provided by foreign companies to Russians were in most cases not subject to Russian VAT: the general rule "at the place of the buyer" (Article 148) did not apply to them, and the place of sale was considered to be the place of activity of the foreign contractor — outside the Russian Federation (Article 161 of the Tax Code of the Russian Federation). This gap was closed in 2017, when Article 174.2 of the Tax Code of the Russian Federation came into force, according to which the OECD approach described above is now applied.

In October 2025, the Russian Ministry of Finance developed a draft law on VAT on e-commerce goods (from marketplaces) from EAEU countries. The rates will increase gradually: in 2027 – 5%, in 2028 – 10%, in 2029 – 15%, and from 2030 – 20%. Currently, if goods are imported into Russia by mail or courier for personal use and their value does not exceed the EAEU duty-free threshold, VAT is not payable.[10] Therefore, it is sometimes more profitable to buy goods on marketplaces than offline. The introduction of VAT may lead to an increase in prices for goods on online platforms, as VAT payers (platforms or sellers) will include the VAT amount in the price.

The collection of VAT on goods in e-commerce is a global practice (already implemented in more than 40 countries[11]). Goods become more expensive by the standard

[9] Directive No. 2006/112/EC of November 28, 2006

[10] Currently, duties and VAT are not levied on goods costing up to €200 and weighing up to 31 kg, but from 2026, this threshold is planned to be reduced to €100, from 2027 to €50, and in 2030, the duty-free threshold will be revoked.

[11] https://www.oecd.org/en/publications/tax-policy-reforms-2025_de648d27-en/full-report/tax-policy-reforms_c57e058c.html

tax rate – about 19.3% in OECD countries,[12] and demand for purchases decreases by 50%.[13]

Globally, the international taxation system for digital commerce will be brought into line with a single set of rules. To date, more than 100 countries have already implemented VAT reforms for cross-border e-commerce based on OECD standards, with more than 30 others preparing to do so.[14] The issue of international taxation of goods and services sold online has not been fully resolved—for example, questions remain about how countries should distribute the profits of "digital giants" and what rules should be used to collect VAT reports from companies.[15]

## 3. Tokenization of the financial market

### Russia's experience

In October 2025, a bill[16] on a new type of digital asset—debt DFA—was submitted to the State Duma. These are the digital equivalent of bonds: investors provide money to the issuer and receive the right to have it returned with interest. Currently, it is not possible to issue bonds using DFAs: DFAs can be issued on monetary claims or on already issued traditional bonds. The legislator proposes to allow the issuance of financial instruments – bonds – directly in tokenized form *(native tokens)*. This approach establishes the use of DFAs as a debt financing instrument: fixed terms and payment schedules allow them to be regulated according to the principles applied to traditional debt instruments.

The proposal will also affect the assessment of banks' risks when forming reserves: The Basel Committee believes that DFAs issued as bonds pose a greater risk to banks than DFAs issued as bonds. Debt CFAs currently account for 88% of the Russian digital financial assets market. It is to be expected that, once the amendments are adopted, the new asset will become dominant in the DFA market.[17]

Also in October 2025, a bill was submitted to the State Duma[18] that allows investment funds to purchase CFAs on the same terms as shares or bonds. Previously, funds were effectively unable to include CFAs in their assets because there was no established depositary accounting mechanism. The amendments introduce such a mechanism (including a nominee holder regime), which opens up CFAs to institutional investors and makes transactions with them comparable to the circulation of traditional securities. Brokers and management companies are subject to the same requirements for protecting client interests as in the securities market. This makes the purchase of CFAs by private investors transparent and controllable, just like the purchase of traditional financial instruments. However, the regulator maintains restrictions and investor tests so that retail investors can purchase CFAs based on their experience and acceptable level of risk.

It should be noted that the development of Russian legislation is taking place against the backdrop of new sanctions by the EU, which have also affected the crypto asset market. The new package of sanctions[19] prohibits European and foreign crypto platforms from serving Russian users and companies. The restrictions also apply to transactions involving a number of digital assets, including the ruble-pegged stablecoin A7A5.[20]

### The experience of Hong Kong, Germany, India, and the USA

It should be noted that the measures implemented in Russia in October are not unique—a similar approach is already being used in a number of countries. For example, in Hong Kong, the Securities and Futures Commission has equated tokenized securities with conventional securities and established the same requirements for investor protection, disclosure, and secure storage. A similar approach has been implemented in Germany, where the Electronic Securities Act has allowed the issuance of debt instruments in digital form and equated them with traditional bonds while maintaining investor protection and disclosure requirements.

In India, in October 2025, the Reserve Bank launched a pilot project[21] on the

[12] https://www.oecd.org/en/publications/2024/11/consumption-tax-trends-2024_57c7322a.html
[13] https://ideas.repec.org/a/eee/pubeco/v239y2024ics0047272724001804.html
[14] https://www.oecd.org/en/topics/sub-issues/vat-policy-and-administration.html
[15] https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/11/consumption-tax-trends-2024_57c7322a/dcd4dd36-en.pdf
[16] https://storage.consultant.ru/site20/202510/24/pr_241025_142.pdf
[17] https://cbr.ru/Collection/Collection/File/55196/review_2024.pdf
[18] https://storage.consultant.ru/site20/202510/09/pr_091025_411.pdf
[19] https://eur-lex.europa.eu/eli/reg/2025/2033/oj
[20] Ruble-pegged stablecoin issued by Russian company A7 in Kyrgyzstan
[21] https://www.business-standard.com/economy/news/rbi-deposit-tokenisation-pilot-cbdc-wholesale-digital-tokens-oct8-125100700532_1.html

tokenization of certificates of deposit,[22] which are short-term debt instruments on the interbank market. This speeds up settlements and reduces operational risks, which echoes Russia's focus on digital bonds and the creation of an infrastructure for their circulation.

Major global investment funds are beginning to participate in the development of the tokenization market. In October 2025, BlackRock[23] adapted one of its funds[24] to the requirements of the GENIUS Act,[25] enabling stablecoin issuers to purchase shares in this fund to launch their projects.

Thus, a trend toward the tokenization of traditional financial assets is forming around the world. This trend is expected to intensify as infrastructure develops and the use of such instruments expands. It is estimated that by 2030, the volume of such assets could reach between $4–5 trillion and $16 trillion,[2627] with the largest growth expected in the segment of instruments for attracting and placing funds, including digital equivalents of bonds.

## 4. Risks of quantum computers

### The Singapore experience

In October 2025, Singapore released a draft guide on how organizations can implement "quantum-resistant solutions" to overcome the risks posed by quantum computers (e.g., data loss, cryptocurrency theft, etc.). Thus, "Q-day" marks the beginning for the spread of quantum computers (in the next 5-10 years), which will capable of cracking cryptographic methods of network data encryption[28] (up to 100 million times faster than classical computers[29]), less vulnerable encryption (such as blockchain networks), and critical infrastructure (banks, government systems).

Quantum threats pose a risk of leaking both personal data and commercial and state data, including the risk of "collect now, decrypt later"[30]. System failures are also the risk (if access to dispatch control systems for industrial and engineering facilities, housing and utilities is intercepted). As a result, compromised access elements (such as digital signatures) lead to the risk of financial manipulation (e.g., cryptocurrency theft or in transactions) or data alteration. To prevent threats, organizations can implement "quantum-resistant solutions." The following is required:

1. Assess the risks of quantum threats, considering business priorities[31] and the affected data (classify the most vulnerable data)[32].
2. Organize a corporate management system, develop a plan for implementing new encryption standards.
3. Change data encryption algorithms to the resistant of quantum computers attacks (e.g., according to standards - FIPS 203, 204, 205[33]), conduct regular testing.
4. Train employees.
5. Assess quantum security risks when interacting with suppliers (third parties).

To assess the deployment of such systems by organizations, Singapore has developed a self-assessment checklist – the Quantum Readiness Index (QRI). For example, how much valuable data being processed could be affected? Is an inventory of all cryptographic assets for encrypting information in the system being conducted? There are four QRI assessment levels in total: where 0 means that the process has not been launched, the organization has not started post-quantum migration,[34,35] and 3 means that the organization is implementing quantum-resistant solutions and has launched a continuous monitoring process.

### Russia's experience

The Technical Committee for Standardization (TC26) is working on developing standards for post-quantum cryptography. The latest standard was published on September 17, 2025, and defines a system of

[22] Short-term securities used by banks to borrow money from each other at a fixed rate.
[23] An investment company that manages various types of funds and assets for private and institutional investors.
[24] https://www.businesswire.com/news/home/20251016818364/en/BlackRock-Introduces-40-Act-2a7-Money-Market-Fund-in-GENIUS-aligned-Form
[25] A US law that regulates the issuance of stablecoins and determines the assets in which their reserves must be held. We discussed it in detail in Monitoring No. 5 (17).
[26] https://www.citigroup.com/global/insights/money-tokens-and-games
[27] https://web-assets.bcg.com/1e/a2/5b5f2b7e42dfad2cb3113a291222/on-chain-asset-tokenization.pdf
[28] Technical network methods used to make data inaccessible to third-party users (e.g., online transactions, messages).
[29] https://www.proskauer.com/blog/blockchain-and-quantum-computing
[30] "Collect now, decrypt later" is a method in which attackers obtain data in encrypted form now with the intention of decrypting it in the future when a quantum computer becomes available. The most vulnerable data will be valuable data with a long storage period, as decrypting it in the future could yield significant benefits, such as personal financial data and medical records.
[31] Organizations can use established standards to analyze business impact, plan for business continuity, and quantify risks (e.g., ISO/TS 22317 (business impact analysis), ISO 22301 (business continuity management systems), NIST SP 800-34 (emergency planning).
[32] For example, such data: publicly available or confidential secret data.
[33] Three international post-quantum cryptography standards from the US National Institute of Standards and Technology that offer encryption algorithms resistant to quantum computer attacks.
[34] Level 1 - The organization has begun studying the quantum threat and has started work on implementation.
[35] Level 2 - The organization is taking an organization-wide approach to implementing quantum-resistant solutions.

concepts in the field of cryptographic information protection.[36]

It is reasonable to expect that regulators around the world (including Russia) will become more active in introducing requirements for their organizations to transition to post-quantum cryptography (e.g., these are the deadlines by which national organizations must fully implement quantum-resistant encryption standards). The US and UK have set a deadline of 2035 for organizations to complete the phased transition, while Australia has set a deadline of 2030.[37] It is also worth expecting Russia to adopt a full-fledged post-quantum cryptography standard.

## 5. Protecting users of the Internet of Things

### The experience of California (USA)

In October 2025, the US passed legislation to protect victims of Internet of Things devices. These devices include, for example, smart home technologies (automatic light sensors, temperature control, video surveillance cameras, etc.). Ninety-seven percent of domestic violence programs in the United States report that IoT devices can be misused as a tool for emotional or physical abuse and threats. For example, attackers hack the mobile apps to remotely control household items (e.g., turning lights on or off, changing the codes on digital locks every day) and monitor their victims.[38]

Under California law, companies that manage IoT device accounts[39], must create a mechanism that allows them to block an attacker's access to an account (or reset it to factory settings) within two days if the victim submits a “device protection request.” Moreover, companies are prohibited from imposing any additional conditions on the victim (including payment/penalties). As part of the request, the victim must confirm ownership of the device and the fact that illegal acts were committed through the device.

### Russia’s experience

Russia has adopted a number of preliminary national security standards for IoT, such as PNST No. 642–2022 (general provisions in the field of industrial Internet of Things), PNST No. 818–2023 (list of basic components of IoT systems), and others. In terms of damage caused by an IoT device, the general provisions of the Law “On Protection of Consumer Rights” apply. Liability lies with the device manufacturer unless the manufacturer can prove that the device was used contrary to the instructions and that the buyer was at fault.

The number of IoT devices in the world could grow by 69% by 2034 from 2025 (+20 billion new devices).[40] Current regulations in Russia do not take into account specific security risks (minimization of data collection; liability for damage caused by IoT devices). It can be predicted that in the future, both globally and in Russia, the regulation of IoT devices will expand to consider different types of eliminate risks, as well as legislative expansion of user protection measures.

## 6. Cross-border data transfer

### The Experience of China

In October 2025, China adopted rules simplifying cross-border data transfers through certification. As a general rule, data transfers to third countries are possible upon obtaining permission for such transfers. To this end, the Cybersecurity Administration of China assesses the security of export operations. The new certification procedure allows companies to transfer data abroad on the basis of a certificate confirming that the company is taking all necessary measures to ensure security of data both during transfer and during processing in a third country. The procedure exempts Chinese companies from the need to obtain permission for each individual data operation. However, the procedure is available to companies that conform to the following criteria:

- Not be a critical information infrastructure operator.
- Transfer between 100,000 and 1 million personal data records or 10,000 sensitive data records per year.
- Not transfer data classified as “important information,” where a security breach poses risks to national security and the economy.

[36] GOST R 34.14-2025. Information technology. Cryptographic protection of information. Terms and definitions.
[37] https://blog.cloudflare.com/pq-2025/
[38] In 2018, the New York Times published interviews with 30 victims of violence who had suffered from IoT https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html
[39] Programs that control user access to devices through which the user undergoes identification and receives an account, such as the “smart home manager” program.
[40] https://www.statista.com/topics/2637/internet-of-things/?srsltid=AfmBOooIhcQhRchsclMF9cdcgqkPfvr0NJrUZQ9ebDXIlHZYn4AfncIS#topicOverview

The certification is valid for three years and is aimed at small businesses with limited volumes of data to transfer. However, even certified companies are subject to government oversight, such as unscheduled inspections.

### Russia's experience

In Russia, the established procedure for cross-border data transfers does not provide for simplifications for any categories of data operators. The complexity of the notification procedure varies depending on the country of destination of the personal data export: for countries not included in Roskomnadzor's list of countries whose data protection legal regime is recognized as adequate to that of Russia, the data operator must prepare additional documents confirming the legal guarantees for data protection after its transfer to a third country. Therefore, Russian companies currently do not receive regulatory support for the development of businesses involving cross-border data flows. Data flows are a key condition for doing business in the digital economy. In 2025, the digital economy will already account for 24% of global GDP. Moreover, by 2026, the monthly data flow will reach 690 gigabytes per month, which is three times higher than in 2020.[41] Thus, maintaining the current regulatory regime creates risks of losing the competitiveness of Russian digital companies.

## 7. Personal data for AI

### The experience of Germany

In October 2025 Germany issued a Data Protection Guide for companies using generative AI technologies based on the search and augmented generation method[42]. "RAG" method means that a user's query is supplemented with context and clarified before the query is sent to the AI for response generation. The guidelines are intended for organizations that process personal data through RAG systems, including the use of embedded AI models and vector databases.[43] Seven principles of operation are highlighted:

1) Data accuracy, otherwise it leads to false AI responses about a person.

2) Traceability of sources used to supplement the query.

3) Data security through technical measures of separating data storage.

4) Classification of data according to its intended use, so that data is not used for irrelevant purposes.

5) Data should be used to generate a response to the extent necessary to process the query and should not be stored longer than necessary.

6) Compliance with legislation even at the stage of training the language model before implementing the RAG method.

7) Observance of all the rights of personal data subjects, including the right to access information about data processing.

Organizations using AI based on the RAG method must be ready to explain to subjects the principles and conditions of using their data in AI systems in an accessible manner.

The practice of regulating personal data protection for AI at the standards level may become more popular in European countries amid initiatives to simplify the requirements of the EU General Data Protection Regulation (GDPR) in order to stimulate the development of AI technologies. In November 2025, the European Commission is expected to present a package of amendments to the GDPR.[44] Given that the European approach to personal data has become a model for many foreign national laws, the new trend is expected to quickly spread to other countries.

### Russia's experience

Data protection standards for AI are being developed in Russia. In 2022, a GOST standard was approved for managing big data analysis processes for AI (but the issue of personal data protection is closed with a reference to general legislative requirements).[45] In July 2025, the Bank of Russia presented a Code of Ethics for the development and application of AI in the financial market. In terms of data protection, it is recommended to use customer data by developing AI solutions only if a significant improvement in efficiency is expected from the introduction of AI for the provision of financial services.[46]

According to a 2025 survey in European countries, 84% of respondents are convinced that the more detailed the regulation of privacy

[41] https://www.kommerskollegium.se/globalassets/publikationer/rapporter/2025/navigating-cross-border-data-flows.pdf

[42] Retrieval Augmented Generation

[43] Vector databases are databases in which data is organized based on semantic, visual, or other similarities, which creates a search "vector" — the ability to find approximate answers to a query.[3] https://www.techpolicy.press/eu-set-the-global-standard-on-privacy-and-ai-now-its-pulling-back/.

[44] https://www.techpolicy.press/eu-set-the-global-standard-on-privacy-and-ai-now-its-pulling-back/

[45] https://docs.cntd.ru/document/1200193996

[46] https://www.cbr.ru/Content/Document/File/178667/code_09072025.pdf

issues for AI, the safer its use will be.[47] Therefore, in Russia and around the world, we can expect the development of industry standards for data protection for AI in sectors such as healthcare and e-commerce.

[47] https://employment-social-affairs.ec.europa.eu/news/commission-survey-shows-most-europeans-support-use-artificial-intelligence-workplace-2025-02-13_en