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

- Consumer protection in the realm of immersive technologies
- Cryptocurrencies as commodities
- Online fraudulent practices
- Responsible AI in business and government
- Vehicles owners' access to their vehicle data
- Data governance regulation

Monitoring No. 9 (21) (Sep25)

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

The reference to this publication is mandatory if you intend to use this material in whole or in part

"September once more, as in eons of timeness ago,
and toward twilight jejuneness of cold turns to manliness.
I suspect the dim garden of clandestine schemes on tiptoe,
for it seems someone's walking there, wreathed in a scantiness".
Bella Akhmadulina

In September 2025, we can identify 6 events that define trends in the development of digital economy regulation globally.

Trend No. 1. Consumer protection in the realm of immersive technologies

In September 2025, Australia released a review[1] of the risks of immersive technologies. One such risk is the excessive realism of immersive environments, which can amplify the impact of harmful online content on children.

Trend
Consumer protection in the realm of immersive technologies

Trend No. 2. Cryptocurrencies as commodities

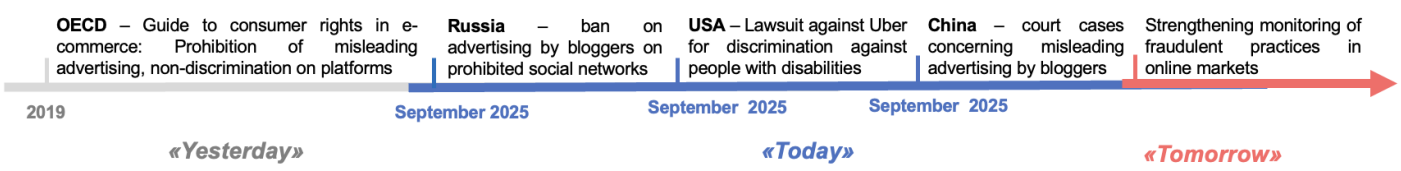
In September 2025, the U.S. Commodity Futures Trading Commission raised the issue of using tokens as collateral in derivative transactions for discussion. This will lead to an increase in the number of tokenized assets worldwide.

Trend
Cryptocurrencies as commodities

Trend No. 3. Online fraudulent practices

In September 2025, China's antitrust authority published a review of court rulings on bloggers spreading misleading online ads. In the US, a lawsuit was filed against Uber for discriminating against people with disabilities in transportation.

Trend
Online fraudulent practices



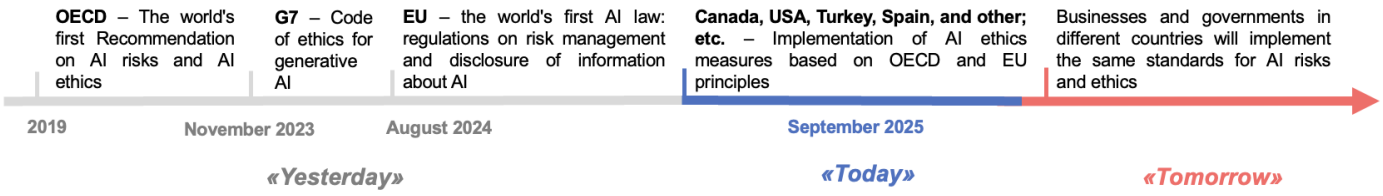
[1] https://dp-reg.gov.au/sites/default/files/documents/2025-09/DP-REG%20-%20Examination%20of%20Technology%20-%20Immersive%20Technologies_0.PDF

Trend No. 4. Responsible AI in business and government

In August 2025, the OECD identified a trend: both companies and governments are following the same international standards of ethics and AI risk management established by the OECD and the EU. In the future, these practices will evolve into similar legislation in different countries.

Trend

Responsible AI in business and government

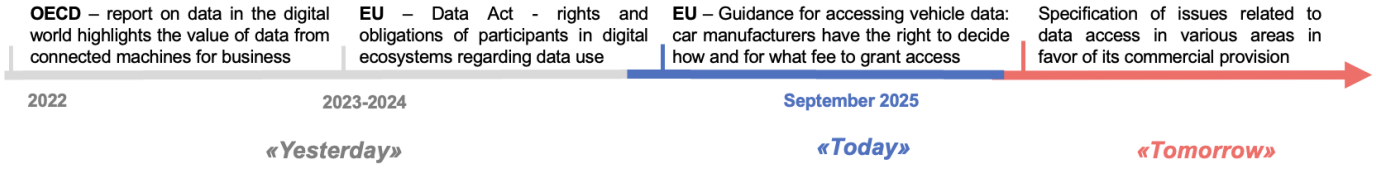


Trend No. 5. Vehicles owners' access to their vehicle data

In September 2025, the EU issued rules requiring manufacturers to provide car owners with access to vehicle data.

Trend

Vehicles owners' access to their vehicle data

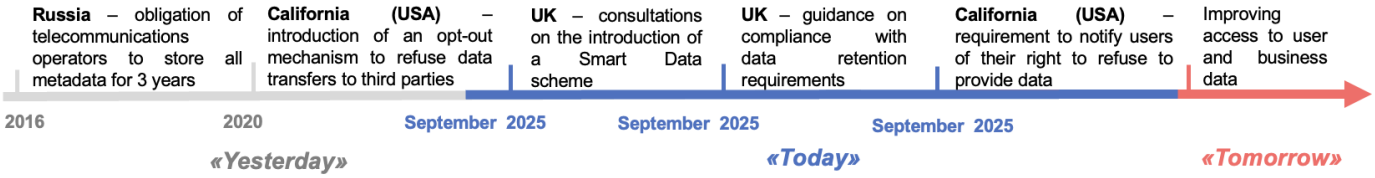


Trend No. 6. Data governance regulation

In September 2025, the UK debated the need to introduce Smart Data, a private data management scheme for users and companies, as well as rules for extending data storage. In California (USA), companies are required to notify users of their right to opt out of sharing collected data with third parties.

Trend

Data governance regulation



Also, in September 2025, the Ministry of Transport (Ministry of Transport) prepared a **draft law on liability for traffic accidents involving autonomous vehicles** (HAV[2]) and the determination of persons responsible for their operation.[3] The first attempt to develop such a draft law was made back in 2021.

The Ministry of Transport proposes that the following parties be held responsible for the operation of the HAV:

- The HAV manufacturer, if the accident occurred due to the malfunction of the HAV control system.
- The owner, in the event of non-compliance with operating rules or unauthorized modifications to the design.

[2] Highly automated vehicle.
[3] https://www.vedomosti.ru/technology/articles/2025/10/01/1143267-mintrans-opredelilsya-s-otvetstvennostyu

- The authorized service center is responsible for accidents caused by poor maintenance, repairs, or failure to update the software.
- The remote support operator[4] – for failure to perform their duties.

The draft law also establishes requirements for certification, maintenance, and admission of HAVs to roads.

The definition of liability has become one of the key issues, as current legislation does not take into account cases where a vehicle is controlled by an AI system. In such situations, liability must be determined depending on whether the accident occurred due to the driver's actions or due to a fault in the vehicle control system, and if the system is at fault, it must be determined who caused the malfunction.

[4] A person who provides remote monitoring and technical assistance during the operation of the HAVs without interfering with its direct management.

Key aspects

1. Consumer protection in the realm of immersive technologies

The experience of Australia

In September 2025, Australia released a review[5] of the risks associated with the use of immersive technologies. These technologies allow users to interact with digital content on the Internet at a level of perception (in 3D) that can feel almost like the real world. However, the level of immersion in this "artificial" world can vary.

The following technologies stand out: virtual reality (VR[6]) such as a virtual reality headset (VR headset); augmented reality (AR[7]) such as applications for "trying on" goods in an interior); mixed reality (MR[8]) such as the creation of virtual human avatars). The global VR/AR technology market is projected[9] to grow by 33.16% (from $20.43 bn in 2025 to $85.56 bn by 2030).

Immersive technologies pose risks:

1) Unlawful collection of large amounts of personal data (especially sensitive data). The main risk of violation is the difficulty of providing meaningful consent to the collection, as users may not be aware of what information is being collected (e.g., data on body movements, physical reactions, psychographic data, etc.)[10] which can be used to identify the user without their permission. Australia proposes integrating protective measures when creating devices and applications: a mechanism for controlling consent to collection,[11] the ability to disable individual functions (such as location sharing or eye tracking) until the user enables them, and the ability to delete data (an "delete avatar" function that erases all data).

2) Violations of Internet safety standards (especially those affecting children). Technology can provide anonymity (for example, by replacing a real person with a digital copy—an avatar) and can be used by malicious individuals to involve children in sexualized violence through emotional manipulation. Australia's 2021 Internet Safety Act categorizes content by its level of danger into "Class 1 material" (destructive content that is prohibited from being displayed) and "Class 2 material" (content that is age-restricted). Content (e.g., MR applications) may also fall under Class 1, requiring providers to restrict access to it and provide annual reports on measures to prevent its distribution.[12]

3) Violations of consumer rights through the manipulation of behavior caused by the excessive realism and emotional intensity of the content. For example, deepfakes in the form of 3D avatars of celebrities can mislead users into making purchases or investing in financial lotteries.

Russia's experience

The development VR/AR technologies in Russia was set out in the 2019 Roadmap for the Development of Cross-Cutting Digital Technology: Virtual and Augmented Reality Technologies. The national project "Digital Economy» includes the task of developing standards for processing large data sets and information security standards in VR/AR systems. At the same time, issues regarding compliance with legislation on personal data, child protection, regulation of property relations, etc. in the metaverse remain unresolved in Russia.

With the development of technology in Russia, measures to regulate the industry may also be adopted (as in South Korea and the UAE), primarily self-regulation, including issues of data protection, the emotional impact of technology on children, the distribution of illegal content in immersive environments, etc.

2. Cryptocurrencies as commodities

The US experience

In September 2025, the Commodity Futures Trading Commission (CFTC) commenced discussions on the use of tokenized

[5] https://dp-reg.gov.au/sites/default/files/documents/2025-09/DP-REG%20-%20Examination%20of%20Technology%20-%20Immersive%20Technologies_0.PDF

[6] Such technologies create the effect of complete immersion in an artificial environment, for example, special simulators for training doctors or pilots.

[7] Such technologies allow individual artificial digital objects to be superimposed on the real world.

[8] Such technologies combine virtual and augmented reality: that is, a digital object is created that is superimposed on reality, and the system allows interaction with it.

[9] https://www.mordorintelligence.com/industry-reports/virtual-augmented-and-mixed-reality-market

[10] For example, virtual helmets can collect data on eye movements, facial expressions, behavioral characteristics, etc.

[11] For example, virtual helmets can collect data on eye movements, facial expressions, behavioral characteristics, etc.

[12] 2024 Industry Standards for internet safety.

assets[13] and stablecoins[14] as collateral in derivatives markets.

Derivatives can include oil futures, Apple stock options, etc. Owning a derivative means having the right to enter into an agreement to buy or sell oil or stocks at a certain price in the future. Such transactions involve risk and therefore require collateral. The CFTC is discussing:

1) What pilot projects involving the use of tokens as collateral can be implemented.[15]

2) What rules governing collateral need to be updated so that tokens are recognized as an acceptable form of collateral.

3) What steps companies are already taking to introduce tokenized collateral for derivative transactions.

The criteria for the acceptability of such collateral have been established. Following consultations, measures have been defined for the official recognition of stablecoins and tokens as acceptable collateral for settlements and derivatives trading.[16]

The implementation of this initiative in the market could potentially significantly change the crypto economy: at the end of 2024, various assets worth $0.9 trillion were used as collateral for financial transactions,[17] and their tokenization could increase the crypto economy market by a third ($3.7 trillion as of October 10, 2025).[18] A positive resolution of this issue could also diversify the collateral market through the tokenization of tangible assets and the “splitting” of ownership rights to them.

Also in September 2025, the CFTC and the Securities and Exchange Commission announced the development of a procedure for admitting crypto assets to exchange trading on the spot market (a market where transactions are conducted almost immediately, for example, the seller transfers the cryptocurrency and receives fiat currency at the time of the transaction).[19]

The regulators confirmed that the current rules already allow for the trading of cryptocurrencies (such as Bitcoin and Ethereum) as commodities, subject to investor protection and trading transparency requirements. In addition, regulators have identified practical issues that market participants need to work on: how margin requirements are set and maintained, how clearing and settlement are organized, and how data exchange between platforms is established (to monitor underlying markets[20] and prevent manipulation).

The implementation of the initiative will affect crypto exchanges around the world, as the CFTC's jurisdiction will now cover not only cryptocurrencies themselves, but also the exchanges on which they are traded. The CFTC has already taken the initiative to regulate the right of foreign crypto exchanges to provide services to US residents (this right has been in effect for traditional commodity exchanges since the late 1990s). Foreign crypto exchanges will be able to serve US customers if their jurisdiction meets comparable regulatory standards.[21]

Russia’s experience

There are currently no decisions in Russia similar to the initiatives in the U.S., but in May 2025, the Bank of Russia[22] allowed financial institutions to offer qualified investors instruments with returns dependent on cryptocurrency prices (derivatives, securities, CFAs) with a conservative risk assessment (full capital coverage and limits of 1% of capital, as discussed in Monitoring No. 8 (20)). At the same time, the Central Bank emphasizes that it does not support direct investments in cryptocurrencies, considering them to be high-risk.

In the future, the Russian financial market will also consider the possibility of using tokenized assets (e.g., CFAs[23]) as collateral,

[13] A digital form of collateral representing rights to real assets and used for settlements and guarantees in transactions.
[14] Tokens whose value is pegged to a stable asset (e.g., the dollar or gold).
[15] For example, Coinbase is planning a pilot project where USDC will act as collateral in futures settlements.
[16] Derivative financial instruments (futures, options)
[17] https://www.fia.org/sites/default/files/2025-06/FIA%20-%20Tokenisation%20-%20Accelerating%20the%20velocity%20of%20collateral.pdf
[18] https://coinmarketcap.com
[19] https://www.sec.gov/newsroom/speeches-statements/sec-cftc-project-crypto-090225
[20] Monitoring and analyzing transactions, prices, and trading volumes in markets where underlying assets are traded to identify manipulations, anomalies, and risks that may affect related derivatives.
[21] https://finance.yahoo.com/news/cftc-may-approve-foreign-crypto-150409711.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAD-3E2EI2fsEeUHT4x2jLNveV4yCA-s6V187idtDduJkPXImrm3AcuOxxv5E1Z8CXgkI07HP3MqW8rylj7vVdAg4M75faeL13EhPJBb_EI4t4M_9rwacm4A_d4t7xjBK8dHNuDquYcqJkUyHhga4ONtR6izdRnIDorpy4js1a4bP
[22] https://cbr.ru/press/event/?id=24647
[23] Digital financial asset

given their potential to speed up and simplify settlements.

3. Fraudulent online practices

The experience of China

In September 2025, China's antitrust agency (SAMR) published enforcement practice of investigating false advertising in e-commerce. For example, Desheng Hospital in Shanghai hired 169 bloggers to advertise medical services in short videos (shorts), who talked about the quality of services they allegedly used themselves. In another case, a company promoted virtual reality projects through bloggers who posted videos of themselves using VR applications. However, it turned out that in none of the cases did the bloggers actually use the companies' services. Those involved in the investigations were fined between 100,000 and 200,000 yuan (between $14,000 and $28,000) for fraud and the use of deepfakes.

It is worth noting that China and other countries are tightening regulations on blogger advertising, requiring, for example, the provision of reliable information about the blogger's experience using the product and the requirement to indicate that the products discussed by bloggers are advertisements. The most stringent regulations have recently been introduced by the UAE, where bloggers must obtain a license to distribute advertising.

The US experience

In September 2025, a lawsuit was filed against Uber in the United States for discriminating against passengers with disabilities.[24] The U.S. Department of Justice accused Uber of refusing to serve passengers with service dogs and folding wheelchairs. Uber has a “credit” system, a form of compensation whereby, for example, if a trip is canceled, a driver behaves inappropriately, or money is debited in error, Uber credits the user's account with a certain amount in the form of credits. But there is a limit on credits. Due to the large number of refusals by drivers, passengers with disabilities reached the limit, and Uber stopped providing them with compensation or reimbursing them for canceled orders.

In addition, an illegal fee was charged for cleaning up after service dogs, drivers often insulted passengers, and did not provide opportunities for convenient travel, for example, they did not allow a person with limited mobility to sit in the front (for example, one passenger was unable to sit in the back because of her prosthetic leg). At the same time, Uber did not provide specialized training for drivers who transport passengers with disabilities.

Despite the fact that passengers often faced discrimination from drivers, Uber also bears direct responsibility, as it is a licensed transportation service provider (on par with taxi companies) and is required to comply with legislation protecting persons with disabilities from discrimination—ensuring that service animals are allowed on board, not charging additional fees related to a passenger's disability, etc.

Russia’s experience

Russia is also seeing a trend toward tighter advertising regulations, including for bloggers. For example, from September 1, 2025, advertising on banned social networks such as Instagram[25] will be prohibited. This could lead to the advertising market going “underground,” reducing the transparency and revenue of the online advertising market and decreasing tax revenues from advertising.

When it comes to the social responsibility of platforms, Russia does not regulate the issue of ensuring the rights of people with disabilities when using platforms (there are only requirements for carriers, i.e., taxi companies, and drivers). However, taxi platforms such as Yandex Taxi have introduced special features for users with physical disabilities and have policies for transporting such people. Most likely, the regulation of the social responsibility of platforms will develop through self-regulation of platforms and driver training.

4. Responsible AI in business and government

The OECD experience

In September 2025, the OECD published a review of the first reports from companies as part of the Hiroshima Process on AI, a G7 initiative to establish universal rules for the development and use of AI systems. The review examined companies' practices in seven areas:[26]

[24] https://www.justice.gov/usao-ndca/media/1414021/dl?inline

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

[26] https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/09/how-are-ai-developers-managing-risks_fbaeb3ad/658c2ad6-en.pdf

1) Identification and assessment of organizational risks.[27] Companies like Microsoft, Google, OpenAI, IBM, and others conduct AI "red teaming" exercises, where teams use simulated attacks to "trick" the model to identify risks of system malfunction.

2) Risk management through procedures and technical measures. First, AI is tested within the company, then for a limited circle of trusted users, and only then is it made widely available. Technical measures are implemented: cleaning and selecting training data, "fine-tuning" the model for specific tasks, and checking the results of queries before they are seen by humans.

3) Disclosure of information about the transparency of AI systems. For consumer-facing AI products, companies publish model "passports" and transparency reports: what the system can do, where its weaknesses lie, and how it was tested. Providers of B2B solutions include disclosure obligations in their contracts.

4) Incident management. There are prescribed scenarios for incidents: who monitors, who records, who responds—companies have teams of specialists. Hotlines are set up for reporting AI problems (at KYP.ai and Rakuten), and special procedures are in place for reviewing the operation of high-risk AI systems.

5) Creation of mechanisms for authenticating and tracking AI content. Companies are implementing labeling of AI-generated content (such as watermarks) and other ways to inform users that they are interacting with AI.

6) investing in AI security. Most companies are investing in cybersecurity, increasing trust in information (for example, Google is developing tools to detect fakes), and identifying discriminatory behavior in AI (for example, Fujitsu and OpenAI are testing AI models for discrimination).

7) the contribution of AI systems to achieving socially important goals. Large companies are conducting research on sustainability, fairness, transparency of models, and confirmation of content origin (Microsoft has an AI & Society network and an AI Frontiers lab). Many projects are focused on healthcare, education, accessibility, and climate, and support the UN SDGs.

The OECD has also published a review of the use of AI in public administration.[28] Like companies, public authorities are guided by the OECD Recommendation on AI, the Hiroshima Process rules, etc. For example, Canada has a mandatory algorithm impact assessment for all automated decisions in public administration. Typically, (in 45 out of 200 cases reviewed), AI is implemented into public services. For example, in Greece, AI "reads" and analyzes documents for real estate registration, which has accelerated the assessment of such transactions from several months to 10 minutes. In second place in terms of popularity is AI in open government and interaction between the state and civil society. For example, the European Parliament Archives have implemented AI to assist in searching and analyzing documents from the archives. AI is also often used in judicial process. For example, in Brazil, the Supreme Court has implemented AI for the initial review of applications to determine whether they meet the requirements and whether the content of the applications can be reviewed (e.g., whether a sufficient set of documents has been submitted). As a result, the time required to review applications has been reduced from more than 40 minutes to a few seconds.

Russia's experience

In Russia, ethical principles for the development and implementation of AI systems are based on "soft" regulation for specific industries. In Monitoring No. 7 (19), we already discussed the Bank of Russia's Code of Ethics for AI in the Financial Market. In addition, the AI Alliance (which includes Yandex, VK, Sber, and others) has developed voluntary codes: a general AI Code of Ethics, a Code of Ethics in Medicine, a Declaration on Generative AI, and others. These documents partially replicate the 2019 OECD Guidelines on AI.

In 2025, the Russian government also initiated an experiment on the use of generative AI in public administration: the Ministry of Digital Development, Communications and Mass Media will develop methodological

[27] Companies focus either on the provisions of the 2019 OECD AI Recommendation or on the risk categories under the EU AI Act, and less frequently on the standards of the US National Institute of Standards and Technology.

[28] https://www.oecd.org/en/publications/governing-with-artificial-intelligence_795de142-en.html

recommendations and rules for its implementation (including criteria for services and restrictions on application scenarios), with participation envisaged for federal and regional authorities.[29] It appears that in the next 1-2 years, Russia will move from soft regulation to basic mandatory requirements for AI in public administration and in certain sectors (e.g., transport, finance, medicine). Based on the experiment with generative AI, the Ministry of Digital Development, Communications and Mass Media may develop standard methodologies: testing AI systems before they are released to the market, incident management procedures, and complaint review mechanisms. Industry recommendations may also be introduced (checklists for managing AI system risks, similar to financial services, for example, in the transport sector).

5. Vehicles owners' access to their vehicle data

The EU experience

In September 2025, the European Commission published guidance on the EU Data Act 2023[30] regarding access to data collected by car manufacturers during vehicle operation and the provision of related digital services. This refers to vehicles that collect information about their use (e.g., data on speed, temperature, mileage, fuel or charge level, and malfunctions) and are capable of transmitting it to third parties, as well as digital services without which the vehicle cannot operate (e.g., remote ignition, door unlocking, self-diagnostics). A service is considered "related" when there is a two-way exchange of data between the vehicle and the provider that affects the operation of the vehicle (e.g., route optimization systems). However, driverless vehicles are not covered by this guidance.

The manufacturer is not obliged to provide the user with constant and continuous access to data at any given moment; it has the right to provide data when it decides that it is "relevant and technically possible." These rules develop the EU's data governance policy, under which the European Commission seeks to empower consumers and companies to control the data generated by devices connected to digital networks.

Manufacturers also have the right to share data with other companies for "reasonable compensation."

Russia's experience

There is no specific law in Russia that gives users and their chosen services the right to request data collected by vehicles. Issues related to the transfer of data from private vehicles to manufacturers are regulated by general personal data regulations. Roskomnadzor's position on the admissibility of collecting user behavioral data, including driving data, is that data that could identify a vehicle user cannot be collected without their consent. In the near future, regulators may issue clarifications on the collection and use of telematic data from vehicles and the owner's right to access it, such as non-discriminatory access to data by independent services that perform maintenance on connected vehicles, with the owner's consent.

6. Data governance regulation

The UK experience

In September 2025, the UK discussed the idea of introducing the Smart Data Scheme, a mechanism for accessing user and business data. Smart data refer to any user and business data that is obtained from companies holding user data by special authorized third parties (ATP) on behalf of the user. Fintech startups, online platforms, analytical services, tariff aggregators, etc. can act as ATPs.

User data are accumulated by companies, but users cannot dispose of their own data, as this is technically difficult: first, they must request their data, then receive it in a machine-readable format, and then transfer it to another company (for example, one from which the user wants to receive a service). Under the Smart Data Scheme, users can instruct ATPs to obtain accumulated data from companies (for example, on banking transactions, tariffs, energy consumption, or subscriptions). Next, when ATP gains access to user data from other companies, it can analyze raw user data to create personalized digital products for the user. For example, ATP can be a financial services provider and use banking transaction data to provide this user with financial advice.

[29] https://www.garant.ru/products/ipo/prime/doc/56928658

[30] https://digital-strategy.ec.europa.eu/en/library/guidance-vehicle-data-accompanying-data-act

Another area of the Smart Data scheme concerns business data. Executive authorities may request businesses to disclose non-personal data accumulated in business processes: information about goods, services, digital content, terms of delivery, availability, price, quality, and user experience. If data are publicly disclosed by one company, other market participants will be able to use them to compare, analyze, and improve their goods and services.

Technically, the Smart Data scheme involves the creation of uniform standards for data formats and interfaces (APIs) through which information can be transferred smoothly, quickly, and securely among data circulation participants.

The UK has also issued guidance on the rules for storing data after the purpose of its processing has been achieved. The only permissible purpose for storage is to preserve the data of a minor user in the investigation of their death. The storage of such data is only permitted on the instructions of the Information Commissioner's Office (ICO).[3132] By comparison, in Russia, there is a requirement for telecommunications operators to store user metadata for three years, but this requirement applies to each operator at all times (rather than for a specific purpose), that creates costs for companies to store data which may not be useful to government agencies.

The US experience

In September 2025, California adopted regulations regarding the opt-out mechanism, i.e., instrument for refusing to provide data.[33] Now, browser providers are required to inform users of their right to opt out of sharing their data with digital service providers that they access through browsers and to explain them how to do so.

Russia's experience

In Russia, personal data subjects are still limited in their ability to control their data, as the law does not provide for the right to transfer data between operators. Against the backdrop of foreign initiatives such as the Smart Data Scheme, this situation widens the gap between the capabilities of Russian and foreign users. The lack of tools such as an opt-out mechanism gives raise to a gray market of personal data and weakens the protection of user rights in the digital economy.

The prospects for the digitalization of the economy depend to a large extent on the quality of user data involvement in economic processes, i.e., on how consciously and actively users manage their own data. Therefore, in order to support national digital business, regulators may introduce amendments to personal data legislation, for example, to enshrine the human right to provide personal data for socially significant purposes, i.e., on altruistic grounds.

[31] Data Preservation Notices

[32]https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/consultation-on-data-preservation-notices/consultation-on-data-preservation-notices.pdf?v=402980

[33]https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260AB566