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

AI in healthcare, combating anti-competitive behavior of smartphone software vendors, personal data protection in a blockchain

Monitoring No. 6 (June 2024)

Monitoring was produced by a team of experts of the Gaidar Institute for Economic Policy (the Gaidar Institute):
Antonina Levashenko, Senior Researcher, International best practices analysis department at the Gaidar Institute.
Maria Girich, Researcher, International best practices analysis department at the Gaidar Institute.
Ivan Ermokhin, Researcher, International best practices analysis department at the Gaidar Institute.
Olga Magomedova, Researcher, International best practices analysis department at the Gaidar Institute.
Tatiana Malinina, Senior Researcher, International best practices analysis department at the Gaidar Institute.

JULY 10, 2024

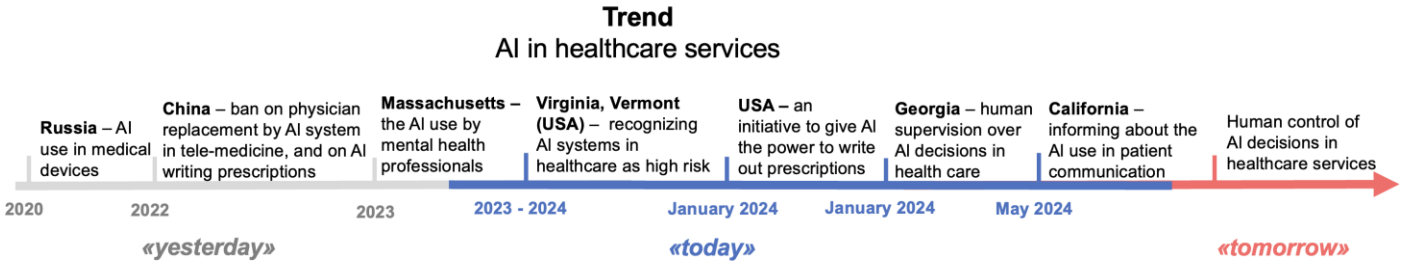
“Manuscripts do not burn”

Mikhail Bulgakov

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

Trend No. 1. AI in healthcare services

In June 2024, a bill in California (USA) clarified the obligation of healthcare providers to inform patients about the use of generative artificial intelligence (AI) to create messages about their health status. The EU law, also signed into law in June, recognized such AI systems as high-risk. The strictest regulation in this area was introduced in 2022 in China, where restrictions were set on replacing a practitioner with an AI system in telemedicine; a different approach was proposed in the US in January 2024 – qualifying AI as a practitioner.

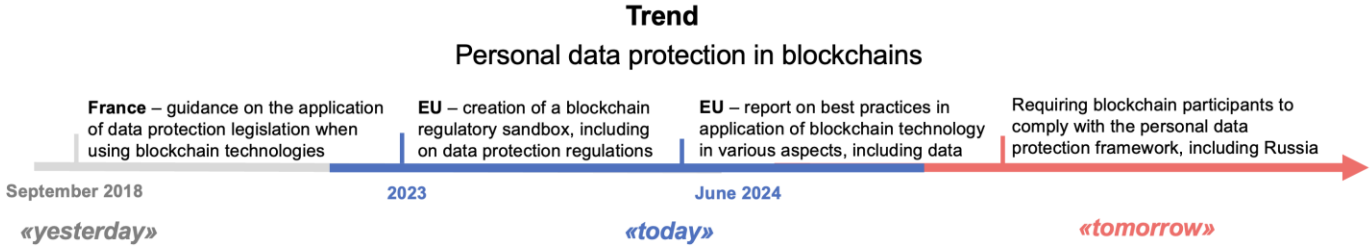


Trend No. 2. Combating anti-competitive behavior of smartphone software providers

In June 2024, Japan banned abuse of the software providers, app stores and browsers in smartphones. The law is aimed at oligopolists - Google and Apple. In many ways, the regulation replicates the EU law. Also in June 2024, the EU launched an investigation into Apple's anti-competitive practice of restricting developers' option to notify users of alternative channels for purchasing apps or services (from another app store or from the developer's own website).

Trend No. 3. Personal data protection in a blockchain

In June 2024, the EU released a report on best practices for blockchain technology and the personal data protection, including identifying the stakeholders who are responsible for data security and the types of data subject to the protection framework. That said, back in 2018, France made its first attempt to define what blockchain data can be deemed personal data and what obligations arise for participants.



Key aspects

1. AI in healthcare services

The US experience

In June, California (USA) considered a bill on utilization of AI in patient communication.[1] Earlier in the US (2023-2024), initiates to regulate the utilization of AI in healthcare services were considered. The following approaches can be highlighted:

1) AI qualify as a **practitioner:**

- Eligible to prescribe drugs. Qualify AI as a practitioner if (1) authorized by the State involved and (2) approved, cleared, or authorized by FDA[2] (Federal US Bill США[3]).

2) **Limiting the use of AI**:

- Prohibit the use of AI in making certain decisions regarding healthcare (together with insurance coverage and public assistance) solely based on the results generated by the AI (Georgia State Bill[4]). Any such decision must be meaningfully considered by the individual. It is planned to set up rules for this purpose.
- Prohibit healthcare facilities from substituting independent evaluations by licensed patient care professionals for AI recommendations or decisions (State of Illinois).[5] For example, if a nurse has identified procedures for a surgery patient's recovery, the facility may not order her to change them based on the AI's recommendations.

Some States do not specifically regulate AI systems in healthcare services, but they are recognized as **"high risk"** (Vermont,[6] Virginia,[7] Colorado[8]). These 3 States require developers and users of high-risk AI systems to take measures to avoid algorithmic discrimination in human access to healthcare services, and users to notify about the utilization of AI in the provision of services. There is an obligation for the developers to educate users about the ability and methods of monitoring.

In California, June 2024 clarifies the obligation of healthcare facilities that the use of generative AI to create written or verbal communications about patients' health conditions[9]:

- Inform that the message is generated by AI and that such message has been verified by the human service provider.
- Brief the patient how to contact the person providing the service.

In addition, Massachusetts is considering a Bill to use AI in mental health starting in 2023:[10]

- Licensed professional in the field must be approved by the licensing authority for the use of AI.
- AI needs to be constantly monitored by a specialist.
- The patient provides written informed consent to receive treatment from the specialist who will utilize AI. Obtaining written consent from the patient is a prerequisite for any medical intervention. However, when using AI, consent is required after being informed about how the AI.

The EU experience

The EU signed the AI Act into law in June 2024 recognizing usage of AI[11] as high risk:

1) To ensure the safety of a medical device used, for example, for in vitro.[12]

2) When authorities assess a person's eligibility to access public health services (e.g., through health insurance).

[1] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB3030

[2] Food and Drug Administration

[3] https://www.congress.gov/bill/118th-congress/house-bill/206/text

[4] https://www.legis.ga.gov/legislation/65973

[5] https://www.ilga.gov/legislation/fulltext.asp?DocName=&SessionId=112&GA=103&DocTypeId=SB&DocNum=2795&GAID=17&LegID=&SpecSess=&Session=.

[6] https://legislature.vermont.gov/Documents/2024/Docs/BILLS/H-0710/H-0710%20As%20Introduced.pdf.

[7] https://lis.virginia.gov/cgi-bin/legp604.exe?241+ful+HB747H1.

[8] https://leg.colorado.gov/sites/default/files/2024a_205_signed.pdf

[9] Patient health information does not include administrative matters including scheduling appointments and billing.

[10] https://malegislature.gov/Bills/193/H1974.

[11] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:PE_24_2024_REV_1.

[12] Performing experiments where they are done "in vitro".

3) To assess and classify emergency calls, such as prioritizing referrals to emergency first aid services and obtaining medical assistance.

High-risk AI has special requirements including requirements to analyze risks, provide human control over AI, etc.

The EU approach is like that of the US states of Vermont, Virginia, and Colorado, but there are differences. The EU requires human control when using high-risk AI (in the above states there is no such requirement), however, there is no obligation to inform people about the AI use. This is due to a desire to remove any liability from healthcare consumers. Unlike Colorado, the EU does not have an established ability to require human review of an adverse AI decision. From technology development perspective, Colorado's approach has advantages: revised decisions provide feedback and can be used to improve AI performance.

The experience of China

In 2022, National Health Commission of the People's Republic of China stated that existing AI in the medical field lacks data and transparency of algorithm performance for medical care.[13] It is unclear how to determine liability for patient harm caused by AI. Therefore, China has set restrictions on the use of AI in medicine:[14]

1) A medical institution cannot utilize AI by impersonating a practitioner or substituting a practitioner qualified to provide diagnostic and treatment services in person (Art. 13).

2) Prescriptions for medicines must be written by the attending practitioner, the use of AI or other ways of automatic prescription writing is strictly prohibited (Art. 21).

Russia’s experience

Russia has 2 experimental legal modes for testing AI medical technologies and has adopted GOST R 59921.2-2021 "Artificial Intelligence Systems in Bedside Medicine".

However, there is no specific legal regulation of the use of AI systems in healthcare. Nevertheless, AI can be used as part of software in a medical device (Order of the Ministry of Health of Russia dated 06.06.2012 No. 4n). Such software is categorized as high-risk software with special conditions of use and licensing. The rules for the registration of such systems are defined by the Decree of the Government of the Russian Federation No. 1416 dated 27.12.2012.

To apply AI in medical practice in Russia, it is necessary to introduce risk identification and management systems, as well as to establish a requirement for human control over decisions made by AI. This will enable the use of AI in medicine, for example, the use of AI for diagnosis can reduce medical expenses by up to 50%. At the same time, human control will reduce the risks of errors in diagnosis or prescribing medication.

2. Combating anti-competitive behavior of smartphone software providers

In June 2024, Japan adopted law limiting abuses coming from market dominance of software used in smartphones.[15] The law effectively targets Apple (46.6% of the market) and Google (53.4%) - oligopolists in the market for basic operating systems for smartphones, browsers and app stores. And in the EU, an investigation into Apple's abuse of its dominance in the app store market initiated in June.[16]

Japan's regulation only applies to providers of 4 types of applications in smartphones:[17] basic operating software (operating systems and drivers), app stores, browsers and search engines.

The Japan Fair Trade Commission (antimonopoly body) plans to develop quantitative criteria for determining the dominance of the listed 4 types of software providers, including an assessment of the number of transactions or the provider's market share with respect to each type of software. The

[13] http://www.cn-witmed.com/list/13/9702.html

[14] Notice of issuance of detailed rules for oversight of internet-based diagnosis and treatment, 2022. http://www.nhc.gov.cn/yzygj/s3594q/202203/fa87807fa6e1411e9afeb82a4211f287.shtml

[15] https://www.sangiin.go.jp/japanese/joho1/kousei/gian/213/pdf/s08021130622130.pdf

[16] https://ec.europa.eu/commission/presscorner/detail/en/IP_24_3433

[17] Smartphone is a terminal:

- Of a size that it can be carried around and used at any time.
- Has installed software that one can use.
- The terminal allows one to use telephone and internet.

Commission will define a specific list of operators (service providers) that have a dominance.

In many ways Japan's law is similar to the EU's Digital Markets Law, but it is sectoral and only targets specific practices of dominance abuse by smartphone software vendors. One reason is the size of the smartphone application market, for example, more than 90% of entertainment content is consumed via smartphones.[18]

Japan defined and prohibited abusive practices specific to the smartphone software market:

1) Using data accumulated by business users (third-party software vendors, app developers in app stores) to compete with them, as well as transferring this data to subsidiaries or their other services. For example, sales data on third-party applications sold through the dominance of vendor's app store (number of downloads, region, price, etc.).

2) Introduction of technical restrictions. For example, dominant operators of the basic operating software cannot impose restrictions on the installation of third-party application stores or browsers. Apple cannot restrict the ability to install Google Play instead of the App Store.

3) Imposing restrictions on the use of payment services. For example, introducing a condition that the user cannot utilize payment systems of other providers than those recommended or embedded in the payment system of this app store.

4) Prohibition of giving advantages to your own services. For example, when searching in the app store offer your own services first and then those of competitors.

5) Imposing restrictions for displaying prices for services sold in the app store, as well as displaying links to other download sites (e.g., another app store or the software vendor's own site) so that the user can download software through third-party sites.

This practice triggered new EU proceeding against Apple in June 2024. Apple restricted the option for developers distributing apps through the App Store to be able to inform their customers about free alternative, cheaper app purchase options, and to leave links for customers to other purchase channels, such as the developers' own websites, third-party app stores. Developers could leave links not in the App Store, but within the app, but then Apple would charge developers €0.50 - a commission for the fact that the user buys the app not in the App Store, but in another store by clicking on the developer's link.

The Commission has now found a violation of Article 6(4) of the EU Digital Markets Act. The risk of punishment for Apple is a fine of up to 10% of total global turnover, proceedings pending.

In Japan, fines can hit up to 20% of a company's turnover in Japan for violating the listed prohibitions.

It is worth noting that in Japan dominant operators are required to implement practices that will equalize competition:

1) Disclose the data management system. For example, app stores should disclose data about the sale of third-party software, the terms and conditions under which such software is purchased and used.

2) Provide the right to transfer data from one user's device/service to another device/service, for example, to transfer photos or messages from one application to another.

3) Ensure the user's right to change default settings, uninstall the pre-installed software by the dominance of supplier.

The above practices and prohibitions are also used in the EU (analytics is given in the Monitoring No. 3 (March 2024). However, there is a difference - Japan singles out a group of measures related to changing specifications or terms and conditions for a particular software. For example, if the dominant operating system provider changes the software specifications (e.g. requirements for programs that can be installed), if the terms of use of the system or the dominant app store refuses to cooperate with individual software developers, or if a browser refuses to display a web page, such actions must be agreed with the Fair Trade Commission.

[18] https://www.kantei.go.jp/jp/singi/digitalmarket/kyosokaigi/dai7/siryou1.pdf

Russia's experience

In Russia, Article 10.1 of the Law on Protection of Competition establishes a ban on monopoly of platforms occupying a dominant position. There is also FAS guidance, however, it does not address practices related to data usage and interoperability, as is the case in Japan or the EU.

However, FAS has initiated investigations like the Apple case in the EU regarding abuses in the software market power including for smartphones.

In 2015, for example, Google was investigated because its Android operating system (over 50% of the market) mandated pre-installation of Google apps, restricting the installation of apps from alternative vendors. In a similar investigation in 2020, Apple (100% of the iOS app store market) was found to have imposed technical restrictions on third-party apps while promoting its own.

The investigations resulted in Google and Apple being recognized as dominance and fined for abuse of market power.

3. Protection of personal data in a blockchain

Blockchain technology is a blockchain with databases including personal data. In June 2024, the European Blockchain Sandbox released a report on the application of European legislation to the technology, including personal data protection issues.[19] Back in 2018. France provided guidance on how to comply with European personal data law when using blockchain technology.[20]

It is important to note that the recommendations on the application of personal data legislation are primarily designed for private blockchain networks (e.g. Ethereum Enterprise), regulators note that the application of the recommendations to public blockchain networks (e.g. Bitcoin) requires further elaboration.

The EU and France experience

Personal data is data that directly or indirectly identifies a specific natural person. The EU and France highlight the following aspects impacting the protection of personal data in blockchain:

1. Types of data that are deemed to be personal data:

- Private keys (allowing confirmation of a transaction or action on blockchain) that belong to a specific individual. For example, a cryptocurrency wallet password.

- Hashed transaction/action data (any data processed by the blockchain's encryption function). For example, data on the transfer of crypto-assets or other information between crypto-wallets.

- Data stored on the blockchain that is associated with user's credentials or data located outside the blockchain (e.g., account login data on the blockchain such as login and password).

- Product-specific data on the blockchain that may not be recognized as personal but is associated with an identifiable person. For example, data about a user's IP address.

The above types of data that can be used in a blockchain become personalized if they allow the data controller to identify the person to whom they belong. For example, the operator can determine who owns the hash (identifying the person who created the hash and the time) or who owns the private key used in the blockchain. This is possible due to the use of the "commit" function in the blockchain, which allows data to be "frozen" (hashed) in such a way that it is possible to recognize encrypted data if additional information (e.g., data from other databases) is available.

In the 2016 Breyer case, the EU Court of Justice already recognized that an IP address relates to personal data if the platform provider has the technical means to identify the specific person to whom the IP address belongs including by using data from third parties like internet service providers.

2. Blockchain participants that must comply with privacy regulations.

In blockchain, participants who define purposes and record data on blockchain or decide to send data for validation by miners are controllers under the EU personal data law. For example, a notary (as a natural person) who

[19] https://ec.europa.eu/digital-building-blocks/sites/display/EBSISANDCOLLAB/Best+practices+report+2023+-+Part+B?preview=/753860727/753860735/European%20Blockchain%20Sandbox%20-%20Best%20practices%20report%20-%20Part%20B%20-%20Jun.2024.pdf

[20] https://www.cnil.fr/sites/cnil/files/atoms/files/la_blockchain.pdf

makes a blockchain entry to record the transaction, determining that data is recorded in execution of such a transaction. Or a bank (as a legal entity) that enters its customers' data into blockchain (recording third-party data in the system). At the same time, a person cannot have the status of a controller over their own data. For example, a person who buys or sells bitcoin in their own name.

Miners will be recognized as processors of personal data within the meaning of EU law because they have access to transaction data (including hashes) that may include personal data, as well as a smart contract developer who processes personal data received from the person collecting such data (the controller). For example, when a smart contract developer for a transaction receives data from a notary public and a miner validates and writes that transaction to the blockchain.

At the same time, data processors do not include:

- Smart contract parties, as natural persons are not considered processors of their own data.
- Developers of smart contract algorithm unless they have access to personal data, but only technically develop IT solutions.

3. Ita Ensuring the right to delete data from the blockchain (EU, France).

The right of the personal data subject to deletion means the right to request the controller to destroy the collected data. The right to personal data erasure on the blockchain is realized when a private key or hash that may contain personal data, including those encrypted via hash, is deleted.

Russia’s experience

In Russia, there are no special regulations of the authorities on personal data protection in blockchain, which creates risks of law violation. Also, unlike in the EU and France, the status of data controller and data processor is not differentiated. This means that in practice in Russia, any blockchain participants who are involved in working with data fall under the definition of a data controller under Russian law (e.g., miners). However, in practice, each blockchain participant can comply with the requirements for personal data operators only to the extent that is part of their function as a participant in the blockchain system. For example, the developer of a smart contract can ensure security measures for data processing but cannot control the legality of the grounds for collecting personal data recorded in the blockchain (e.g., the existence of consent of the data subject).