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

Combating anti-competitive practices online, handling of personal data by technology

Monitoring No.9 (September 2024)

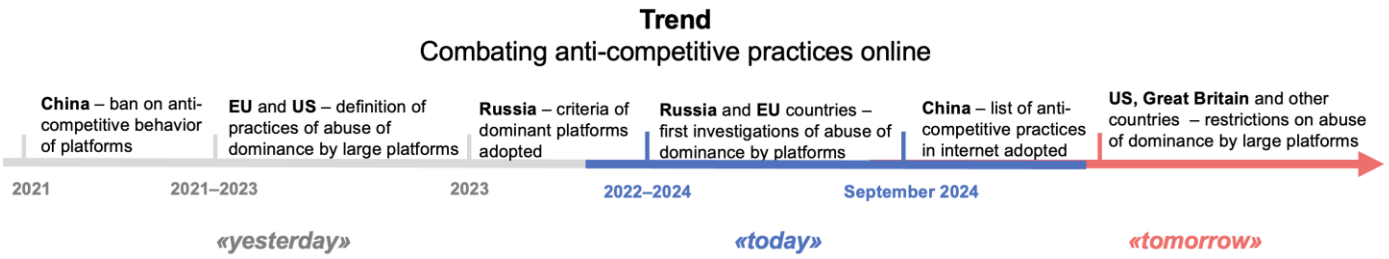
Monitoring was prepared by a team of experts of the Gaidar Institute for Economic Policy (the Gaidar Institute):
Antonina Levashenko, Senior Researcher, International Best Practices Analysis Department, Gaidar Institute.
Maria Girich, Researcher, International Best Practices Analysis Department, Gaidar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

"The unprecedented fall built a dome high,
The clouds were ordered not to darken the dome.
And people marveled at the passing of September,
And where have the cold, wet days gone?"
.
Anna Akhmatova

In September 2024, we can identify two events that define the trends in the development of digital economy regulation in the world.

Trend No. 1. Combating anti-competitive practices online

In September 2024, the next results of antitrust investigations of Google in the UK and Italy and Amazon in Germany were released. All investigations relate to the abuse of dominant position by platforms. In addition, on September 1, China enacted Temporary Regulations on Combating Unfair Competition on the internet, which are aimed at, among other things, refusing to ensure compatibility between the services of a dominant platform and those of other providers.



Trend No. 2. Handling of personal data by technology

In September 2024, regulators in four EU countries decided on principles for how companies should handle personal data for AI training, databases and cookies. For example, Germany has adopted a regulation for "consent management services" for the use of cookies that allows consent to be obtained only once for subsequent use of digital services. This will save users of digital services from repeated requests for cookies and reduce the number of possible infringements. The need to balance the development of the digital economy with the rights of personal data subjects will in the long run lead to an increase in the rights of regulators to clarify and implement legal requirements for the handling of personal data.

In addition, an important event in September 2024 was the signing of **the Council of Europe Framework Convention on Artificial Intelligence (AI) and Human Rights, Democracy and the Rule of Law** in Vilnius.[1,2] The Convention is the first legally binding international agreement on AI. Its scope

[1] https://rm.coe.int/1680afae3c.

[2] Euro commission singed the Convention in the name of EU (https://digital-strategy.ec.europa.eu/en/news/commission-signs-council-europe-framework-convention-artificial-intelligence), it was also signed by Andorra, Georgia, Island, Norway, Moldova, San-Marino, Israel, Great Britain and the USA (https://www.coe.int/en/web/portal/-/council-of-europe-opens-first-ever-global-treaty-on-ai-for-signature).
Argentina, Australia, Canada, Costa Rica, Vatican City, Israel, Japan, Mexico, Mexico, Peru, Uruguay, USA and Vatican City participated as observer countries in the drafting of the Convention by the Council of Europe's AI Committee (https://rm.coe.int/1680afae67

is wider than the EU AI Act, as it can be signed (and has already been signed) by countries outside the EU.[3]

Ita It should be noted that the definition of an AI system in the Convention (Article 2) coincides with the OECD definition updated in March 2024 (see Monitoring No. 3). The Convention contains several concepts already set out in the EU AI Law, in particular the risk-based approach and the possibility of imposing bans on AI systems.

The provisions of the Convention are of a general nature due to the need for flexible application in a rapidly changing environment, when the details of the measures to be implemented (in particular, on the protection of privacy and personal data, informing people that they are interacting with AI, people challenging decisions made using AI) are left to the discretion of the signatories. At the same time, each party within 2 years from the date of signing the Convention should submit a report with measures for its implementation (clause 1 of Article 24). In general, the Convention may contribute to the dissemination in the countries of the approaches to AI regulation set out in the EU AI Law adopted in 2024.

Russia has not been a member of the Council of Europe since March 2022,[4] so it cannot join the Convention yet.

September 2024 also saw a significant development in Russia's digital economy regulation, with **proposed legislation to regulate deepfakes, including the use of voice to create a deepfake:**

1. The use of deepfakes to commit felony offenses.

Draft bill No. 718538-8[5] proposes to punish, within the framework of the Criminal Code, crimes committed with the use of image or voice (including falsified or artificially created - including deepfakes), as well as with the use of biometric personal data of the victim or another individual, including defamation, theft, fraud, extortion, causing property damage by deception or breach of trust. In addition, it is proposed to introduce liability for the use of biometric personal data for the purpose of fraud in the field of computer information to steal other people's property by entering, deleting, blocking, modifying computer information and so on.

It should be noted that criminal punishment for theft or other offense using deepfakes does not cancel the liability within the framework of personal data legislation. This means that, for example, a fraudster will receive not only a term of imprisonment for theft using a deepfake, but also a fine for illegal handling of personal data within the framework of administrative liability.

2. Individual voice right regulation, including voice processing.

The draft bill 718834-8[6] proposes to amend the Civil Code (art. 152.3) to recognize the "right to voice protection" (a similar provision has already been adopted with respect to the facial image). It is proposed to stipulate that the publication (including on the internet) and use of an individual's voice (for example, in the form of a recording), including with the help of special technology (for example, AI to create deepfakes), is allowed only with the consent of this individual, and after his death - with the consent of his spouse, children, parents. A similar norm exists for the image of an individual, but the difference is that the proposed norms for the use of voice are more modern, as they include "special technology", which implies the use of deepfakes and any other voice synthesis technology. In fact, 3 important aspects are set up: (1) an individual's personal right to the voice; (2) a property right, including the ability to transfer his/her voice to heirs, including the right to use it for intellectual property objects; (3) a ban to create deepfakes without the consent of the individual.

Consent is not required when:

- The voice is used in the state, social other public interests.
- The voice is recorded by video or audio recording, which is played in places of free attendance, public events (meetings, conferences, concerts, etc.).

[3] The Convention is open for signature by the member states of the Council of Europe and other countries that participated in its drafting (Article 30 par. 1). Subsequently, if the member states agree, all other countries will be invited to accede to it (Article 31 par. 1).

[4] https://www.coe.int/en/web/portal/46-members-states.

[5] https://sozd.duma.gov.ru/bill/718538-8#bh_histras

[6] https://storage.consultant.ru/site20/202409/17/pr_170924_834.pdf

– Commercial voice recording.

If an individual's voice was obtained without his or her consent and disseminated on the internet, it is possible to make demands to delete the recording and stop its use and dissemination. In general, the proposed norms may reduce the risks of creating deepfakes for illegal use, in fact, a deepfake can be created only with the consent of the owner of personal and property rights to the voice.

In many respects, this approach is close to the regulation of deepfakes in the United States (analyzed by the authors in Monitoring No. 2), where the No AI Fraud Act[7] was published in January 2024. In the US it is proposed to establish an individual's property right to his/her voice and image (likeness), i.e. actually property rights. Such a right is equated with intellectual property rights and can be freely inherited and does not terminate after death for another 10 years, regardless of whether such rights were used by the individual during his/her lifetime. An individual may transfer his or her image or voice to create a digital image[8] or a copy of the voice[9] by entering into a written agreement.

In Russia, similar norms are proposed - the establishment of property rights to the voice, including the possibility of its use for the creation of intellectual property objects, taking into account the fact that the deepfakes can also be an object of intellectual property rights. At the same time, Russia does not directly set up the norm on the use of voice within the framework of intellectual property, but this norm is implied, as the right to voice becomes a property right as well.

In Russia, such legal issues should be specified:

1) Whether the individual's written consent is required, for example, if such use is planned for commercial purposes. Such consent will confirm the right of the third party to use the voice, including for the creation of intellectual property.

2) Whether in this case intellectual property rights to the voice arise, including the possibility of transferring such rights to heirs. In this case, it is necessary to establish the term of validity of intellectual property rights.

[7] https://www.congress.gov/bill/118th-congress/house-bill/6943/text?s=1&r=3

[8] Digital depiction - an exact copy, imitation or approximation of a human being (living or deceased) that is created or altered in whole or in part using digital technology.

[9] Digital voice replica - an audio recording that is created or altered in whole or in part using digital technology and recorded in a sound recording or audiovisual work that includes repetitions, facial imitations that the individual did not actually voice.

/ Key aspects

1. Combating anti-competitive practices online

In Monitoring No. 3 we examined the norms of regulation in individual countries of various practices of abuse by platform dominance. Let us now consider the application of these norms in specific proceedings.

The EU and Great Britain experience

In September 2024, a number of antitrust proceedings were conducted against Google and Amazon in the UK, Germany and Italy.

In a case against Google (UK),[10] the Competition and Markets Authority alleged Google's abuse of dominance in three parts of the ad tech stack chain:[11] Google operates ad buying tools (Google Ads and DV360) and the DFP server for advertisers to publish ads, as well as the AdX ad exchange.

Advertising exchanges auction advertising space by aggregating requests from advertisers (sites where ads are published) and responsive bids from advertisers (with prices at which they are willing to buy advertising space). An auction is then held where an auction fee of 20% of the bid amount is charged. All 3 platforms are owned by Google, which dominates the market.

In September, an investigation began against Google for giving preferential treatment to its own services:

- Providing AdX with exclusive or preferential access to advertisers that use Google Ads' platform.
- Manipulating advertiser bids so that they have a higher value when submitted into AdX's auction than when submitted into rival exchanges' auctions.
- Allowing AdX to bid first in auctions run by DFP for online advertising space, effectively giving it an 'right of first refusal' - with rivals potentially not having any chance to submit bids.

To date, a verdict has not yet been issued against Google, the investigation is ongoing.

In Italy, in September, the Advocate General published an assessment of Google's abuse of its dominance in the operating system market.[12] Google developed the Android open-source operating system. In 2015, Google launched Android Auto, an app for mobile devices with an Android operating system that enables users to access certain apps on their smartphone through a car's integrated displays, was launched in 2015. Third-party developers can create their versions of their own apps that are compatible with Android Auto by using templates provided by Google. Enel X reported that Google refused to connect its JuicePass app with features for electric cars because the app is not compatible with Android Auto (Enel did not use a specific Google template for compatibility).

Interestingly, the Advocate General used the Bronner[13] criteria to assess Google's market position - the practice whereby a dominant undertaking denies access to infrastructure developed by that dominant undertaking for its operations. In doing so, such a refusal has the effect of eliminating competition in the relevant market because there is no alternative infrastructure provided by other undertakings. However, counsel recognized the Bronner criteria as inapplicable because the platform (Android Auto) was not developed by the dominant Google for its own exclusive use, but for connecting third-party applications.

It is worth noting that there was an investigation in Russia against Apple[14] in 2020, when Apple introduced technical restrictions to iOS in terms of configuration profile settings, which forced Kaspersky Lab to degrade the functionality of the Safe Kids app (some technological components had to be removed, otherwise access to the App Store was banned). The FAS recognized an abuse of Apple's dominant position using criteria like Bronner's - the App Store was the only distribution channel

[10] https://www.gov.uk/government/news/cma-objects-to-googles-ad-tech-practices-in-bid-to-help-uk-advertisers-and-publishers

[11] The advertising stack consists of intermediaries that provide services aimed at buying and selling advertising spots and advertising space online. For example, such intermediaries include ad servers for advertisers (selling spots on their sites to place advertisements); ad buying services (used by advertisers to purchase ad space from an advertiser); ad exchanges (conducting real-time auctions to buy and sell advertising)

[12] https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-09/cp240132en.pdf

[13] judgment of the Court of Justice of 26 November 1998 in Case C-7/97 Bronner

[14] https://docs.cntd.ru/document/565727153

for iOS apps, with the App Store being the only way for third-party app developers to gain access to iOS devices.

Nevertheless, in Italy, Google's actions were found to be abusive because the denial of the Enel application was not objectively justified. Such a refusal could be “objectively justified” if access to the Android Auto platform was technically impossible or would affect its performance. However, the denial due to the need to develop a special template for the Enel application does not result in the technical risks cited, but only requires time and cost on Google's part.

In fact, the Russian FAS recognized the App Store as the only platform for access to iOS devices, using the Bronner criteria, whereas in Italy the lawyer took a different position (referring to the technical capabilities of the platform), although Android Auto, like the App Store for iOS, is the only way for app providers to gain access to Android machines. In both cases, however, the platforms were created not only for the companies' own app-hosting activities, but also to connect third-party apps to the devices.

Amazon is under 2 ongoing proceedings in Germany (launched in 2022): [15]

1) In connection with Amazon's implementation of algorithm control of price by third-party sellers on the Amazon marketplace. As a result, Amazon may block or restrict sales of items from such sellers if the items are overpriced.

2) Regarding the system of brandgating issue: Amazon creates a register of brands and their distributors who can confirm their intellectual rights to sell goods with the corresponding trademark. This is necessary to exclude sellers from the site who do not have intellectual property rights to the trademark of the goods sold. The antimonopoly authority plans to check the conditions for the admission or exclusion of sellers from Amazon's site, taking into account whether they have rights to use the brand (trademark).

In September 2024, the antitrust authority Bundeskartellamt launched an online survey of 2,000 third-party retailers to examine the impact of Amazon's prices on access to the platform.

Experience of China

On September 1, 2024, China's Interim Provisions on Combating Unfair Competition on the Internet[16] that defines banned practices, will take effect:

1) Use of false and misleading advertising: dissemination of false information about transactions, ratings of sellers and their products, traffic; misleading by offering discounts to consumers only for positive reviews.

2) Falsification of user reviews and other practices with reviews, such as using images to disguise negative reviews, placing positive ratings at the beginning of the list of reviews, etc.

3) Damaging the business reputation of competitors, e.g., distributing false risk warnings, letters of complaint, etc.

4) Inserting links, including forcing links to interfere with other vendors' products.

5) Creating products that are incompatible with other vendors' products.

6) Buying up a vendor's own products to leave positive reviews or downgrade other vendors.

7) Malicious actions of taking possession (adding to a shopping cart on the marketplace or booking) of goods for a short period of time without payment.

8) Wholesale purchases with subsequent return or refusal to receive the goods, etc.

9) Use of frequent pop-up windows that cannot be closed, etc.

10) Disrupting the normal operation of other suppliers' products, e.g. by launching other applications against the user's wishes, failure to provide functions for uninstalling applications, etc.

Russia’s experience

To date, the FAS has developed a set of market practices that define abuses in digital markets.[17] However, unlike the approach of China or EU countries, such principles do not include a list of abuses related to the anti-competitive use of data accumulated by platforms or the refusal of interoperability with third-party services, etc.

[15] https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2022/14_11_2022_Amazon_19a.html

[16] https://scjgj.beijing.gov.cn/ztzl/gpjzyqjc/zjyq/202405/t20240524_3693717.html

[17] https://fas.gov.ru/p/protocols/1666

2. Handling of personal data by technology

Personal data is a significant resource for the development of the digital economy, but it also belongs to individuals who have a right to privacy. In September 2024, regulators in several EU countries, following investigations, decided on rules for the use of personal data for AI training, databases and cookie banners.

Experience of the EU countries

On September 4, 2024, the Irish[18] DPC concluded the proceedings against X (formerly Twitter), which began in the High Court[19] on August 8.[20] The cause was the processing by X, between May 7 and August 1, 2024, of personal data from the public posts of Europeans to train its AI tool Grok.[21] The Commission[22] sued X, seeking an urgent order to compel the company to suspend, restrict or prohibit their processing. This was the first time this had been undertaken

On August 8, 2024, X agreed to suspend the contested processing of personal data. As a result, the proceedings were concluded on the basis of X's agreement to adhere to the terms of the undertakings on the permanent basis, the specific content of which the Commission does not disclose.

In doing so, the Commission has requested clarification from the European Data Protection Board[23] pursuant to Article 64(2) GDPR[24] on the extent to which personal data may be processed for the development and training of AI and the legal basis for such processing. The clarification has not yet been released.

This case shows that at the current stage the regulation of the use of personal data has gaps, the filling of which in practice depends on agreements between the regulator and the data processor.

Also in September 2024, the Dutch Data Protection Authority[25] imposed a €30.5 million fine on the US company Clearview AI.[26]

Clearview AI, a for-profit company with no presence in Europe, offers facial recognition services to intelligence and investigation agencies. The company's customers provide it with images to find out the identity of the people in the pictures. For this purpose, the company has a database of more than 30 billion photos of people, which it automatically collects from the Internet and then creates a unique biometric code for each face without people's knowledge or consent.

Thus, any person whose photo is available on the Internet can end up in this database. Note that the automatic collection and storage of information from the Internet (scraping) by private companies and individuals is generally unacceptable in the Netherlands.[27] In addition, according to the Authority, Clearview AI violated the GDPR in terms of: 1) the processing of biometric personal data, as the company does not fall under the exceptions to the general prohibition in the law (e.g., where the data subject has given explicit consent to the processing or the processing is necessary to protect the vital interests of the data subject); and 2) the awareness of data subjects, as it does not cooperate with requests for access to the data. If the company does not stop the violations, it must pay an additional fine of up to €5.1 million in addition to the main fine.

Clearview AI has already been fined €20 million in 2022 by the Greek data protection authority for similar GDPR[28] violations, which did not change the company's practices. In this regard, the Dutch Data Protection Authority is looking for ways to influence the company, including exploring ways to impose liability on its directors who were aware of the violations but did not prevent them within the scope of their authority. Thus, this case confirms the practice in the case of Mr. Durov and Telegram: If European regulators cannot “reach” a company, they try to influence its managers.

On September 6, 2024, the Belgian Data Protection Authority[29] ruled on Mediahuis' illegal

[18] Data Protection Commission.
[19] Irish High Court.
[20] https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-welcomes-conclusion-proceedings-relating-xs-ai-tool-grok
[21] https://www.dataprotection.ie/en/news-media/press-releases/dpc-welcomes-xs-agreement-suspend-its-processing-personal-data-purpose-training-ai-tool-grok
[22] Data Protection Act 2018, https://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html
[23] European Data Protection Board.
[24] Общие положения о защите данных (Регламент ЕС 2016/679), https://eur-lex.europa.eu/eli/reg/2016/679/oj
[25] Autoriteit Persoonsgegevens.
[26] https://www.autoriteitpersoonsgegevens.nl/actueel/ap-legt-clearview-boete-op-voor-illegale-dataverzameling-voor-gezichtsherkenning
[27] https://www.autoriteitpersoonsgegevens.nl/actueel/ap-scraping-bijna-altijd-illegaal
[28] https://www.edpb.europa.eu/news/national-news/2022/hellenic-dpa-fines-clearview-ai-20-million-euros_en
[29] Gegevensbeschermingsautoriteit.

use of cookie notification banners on 4 press websites, such as the Antwerp newspaper.[30,31] The Authority received a complaint from a user that the sites did not have a “reject all” button that was quickly enough distinguishable and used deceptive practices (misleading button colors) and that it was not easy to withdraw consent to the use of cookie banners. The Authority concluded that:

1) Consent cannot be considered freely given (as required by the GDPR) if the choice to “accept/reject all” is not offered at the same level, e.g. buttons side by side. It is also not unambiguous, as the user does not know that the “reject all” button is on the next step.

2) On the websites in question, the “accept all” button is highlighted in a bright color, which encourages the user to click it. In this way, the principle of fairness prescribed by GDPR is violated and therefore the consent is invalid.

3) Withdrawal of consent is only possible after several clicks, whereas one click is sufficient for consent, which is a violation of the GDPR.

The Data Protection Authority gives the company 45 days to correct these deficiencies, including by setting an opt-out cookie button and not using misleading button colors. After this period expires, the company will be fined €25,000 per day for each deficiency on each of the sites. The company may appeal this decision in court.[32]

It should be noted that in Monitoring No. 7 we have already discussed deceptive practices related to illegal data collection.

The Mediahuis case shows that the use of personal data, even by companies whose activities are open to an unlimited number of people (mass media), can significantly violate the current legislation, which gives reason to search for alternative solutions.

Germany, for example, is creating an alternative to cookie notification banners: on September 4, 2024, the German government passed a Decree on the establishment of consent management services.[33] These services save the user's settings when they first use a digital service and allow them to review the decision at any time, and digital service providers who voluntarily join the service will be informed of the users' decision upon request. This new, EU-wide tool is expected to relieve digital content users of repetitive cookie requests, enable better website design by reducing banners and reduce the flow of cookies. The success of the approach depends on the emergence of consent service providers on the market, which will be favored by users and digital service providers. The effectiveness of the approach is planned to be evaluated 2 years after the Regulation comes into force.

Users have the right to change the consent management service at any time, for which purpose the latter shall save the settings in machine-readable format and transfer them free of charge to another service of the user's choice.

To increase trust, consent management services must be recognized by the federal data protection and freedom of information[34] commissioner, who includes them in a public register. To do so, they must submit an electronic notification with information about themselves, including name, legal form and economic structure, including funding sources. The notification is required to be accompanied by a statement that the consent management service provider will not process users' personal data for other purposes. It is also required to provide a security concept including, inter alia, information on the place of storage of personal data, technical and organizational measures for data protection and risk management. The notified body has the right to withdraw the recognition of a consent management service provider if it fails to comply with the requirements.

This tool, by reducing the flow of cookie banners, can reduce personal data breaches.

Russia’s experience

In Russia, according to Roskomnadzor's position, cookie data is also recognized as personal data, i.e. the subject's consent is required for its processing, and failure to inform about the use of such files is considered a

[30] Gazet van Antwerpen.
[31] https://www.gegevensbeschermingsautoriteit.be/burger/gba-neemt-maatregelen-tegen-mediahuis-voor-onrechtmatig-gebruik-van-cookiebanners-op-perssites
[32] Marktenhof.
[33] https://bmdv.bund.de/SharedDocs/DE/Pressemitteilungen/2024/073-wissing-wir-wollen-die-cookie-flut-reduzieren.html; https://bmdv.bund.de/SharedDocs/DE/Anlage/K/veordnung-nach-26-absatz-2-tdddg-und-zur-aenderung-der-besonderen-gebuehrenverordnung-telekommunikation.pdf?__blob=publicationFile
[34] Bundesbeauftragte für den Datenschutz und die Informationsfreiheit.

violation. At the same time, there is no information about relevant cases, as well as about cases related to the use of personal data for illegal creation of databases and training of AI in court practice.