ALRUD

TMT Legal Digest

Key regulatory news in the TMT industry from June 2023 to February 2024

Contents

Introduction

Dear Readers,

We would like to share with you an updated digest of the most significant laws and bills and regulatory innovations in the TMT sector for the period from June 2023 to February 2024, as well as trends in the future regulation of this industry.

The TMT industry is currently experiencing significant regulatory pressure with changes constantly being made for both its service providers and the customers who use their products. As such, the regulation of hosting providers' operations in Russia indirectly extends to a large number of companies that use the services of foreign providers.

Given the growing role of information technology in the economy and the resulting threats to data security, there is an obvious trend towards regulating the TMT industry, searching for solutions to ensure the greater security and transparency of processes in the online environment, as well as increased liability for violations of requirements for individual players, such as social networks, hosting providers, people who work with biometric data, as well as the rules for working with information.

The changes affect both major players on the Russian and international markets, as well as small companies that are forced to provide virtually the same level of response.

This digest presents current legislative and regulatory changes in the TMT sector, namely in information technology, media content, advertising, personal data, telecommunications, e-commerce, retail, and antitrust regulation. It provides details about the main changes and initiatives over the past year, as well as the key findings of law enforcement practice in this regard.

Maria Ostashenko
Partner

Commercial, Intellectual Property, Data Protection and Cybersecurity

MOstashenko@alrud.com

Information technologies

New law on hosting providers in Russia[1]

From 1 December 2023, new requirements for hosting providers came into force. In particular, the responsibilities of hosting providers include the following:

- Sending a notification about the commencement of hosting services to the DPA ("Roskomnadzor");
- Ensuring the implementation of information security requirements;
- Providing assistance to the state authorities in conducting operational and investigation activities and activities to ensure state security;
- Complying with the requirements of the "Sovereign Runet" Law and other specific provisions of the Russian Communications Law;
- Identifying or authenticating its clients using the methods prescribed by law.

These requirements apply to both Russian and foreign hosting providers if they provide hosting services to Russian users.

Based on the hosting provider's notification about the commencement of hosting services, the hosting provider is entered into a special register of Roskomnadzor. As of 1 February 2024, the absence of information in the register is an obstacle for the operation of hosting providers in Russia.

1 *For a more detailed overview, please refer to our newsletter on the subject.*

New rules for the authorization of Russian websites users[2]

From 1 December 2023, owners of websites, mobile applications, or other information systems that are Russian legal entities or citizens of the Russian Federation are obliged to authorize Russian users in one of the following ways:

- Via a phone number in accordance with the procedure prescribed by the Russian government based on an identification agreement concluded by the owner with a telecom operator;
- Via "Gosuslugi" (a Russian state services platform) or Unified Biometric System;
- Via another information system (IS) that meets information protection requirements. The owner of such a system may only be a citizen of the Russian Federation who does not have citizenship of another state, or a Russian legal entity.

As such, the use of various foreign authorization systems on Russian websites or applications, such as an Apple ID/Google account, is restricted.

There is also a transitional period until 1 January 2025 to adapt to the new requirements. During this time, authorization using an IS owned by the resource owner and/or a Russian legal entity affiliated with the resource owner is permitted.

New fines for the violation of obligations by social network owners[3]

On 1 September 2023, administrative liability was established for the violation of statutory obligations prescribed for owners of social networks[4]. Failure to comply with the following obligations will result in fines under the Code of Administrative Offenses of the Russian Federation ("CAO RF") from 50,000 RUB up to 8,000,000 RUB:

Article 13.50 of the CAO RF

- Annual posting of a report on the consideration of requests concerning information disseminated in violation of the law and the results of social network monitoring, and an electronic form for sending the relevant requests
- Posting the terms of use on a social network and informing users of any changes to it;
- Conducting social network monitoring and taking measures to restrict access to information whose distribution is prohibited under the Information Law;
- Cancellation of measures for restricting access to information at the request of Roskomnadzor.

2-3 For a more detailed overview, please refer to our newsletter on the subject.

4 Social network owners are defined as entities whose social networks are used to distribute advertising in the Russian language aimed at Russian consumers with a daily audience of more than 500,000 Russian users.

Article 19.7.10 of the CAO RF

- Providing Roskomnadzor with information about a social network owner or other information needed to maintain the relevant register of social networks.

Article 19.7.10-4 of the CAO RF

- Fulfilment of Roskomnadzor's request to monitor a social network to identify information that is confusingly similar to information that was to be deleted by a social network owner based on an earlier request from Roskomnadzor.

Enforcement practice

Clarifications from the Ministry of Digital Development about the qualification of SaaS, CDNs, and file storage as hosting services

With the introduction of new regulations for hosting providers, the Ministry of Digital Development has provided clarifications in response to enquiries regarding the qualification of certain services as hosting services.

As such, file storage and SaaS (software as a service) services are not regarded as hosting services, since they do not imply the placement of a user's information system. In addition, activities to support one's own websites do not qualify as hosting services.

At the same time, Content Delivery Network (CDN) services are considered hosting services, as the CDN involves the provision of computing power to third parties for the purpose of placing information in an information system.

The first video game in the ODI register

Proxima Beta Pte. Limited's mobile video game, PUBG Mobile, was added to the register of organizers of information dissemination on the Internet ("ODI")[5] in 2023.

The register contains several hundred ODIs, with the key feature being the ability to share information between users over the Internet (social networks, forums). PUBG Mobile is currently the only video game in the register.

Foreign hosting providers in Russia: The Landing Law and the boycott of the new register

In 2023, Roskomnadzor expanded the list of foreign companies subject to "landing" by including 12 foreign hosting providers. By January 2024, over 395 million RUB in fines were imposed on 11 companies from the list were fined for the failure to comply with the Landing Law.

However, according to Roskomnadzor's own reports, not a single foreign hosting provider has been entered into Roskomnadzor's new register of hosting providers. The register currently lists approximately 300 Russian hosting providers.

5 *The Organizer of information dissemination on the Internet is an entity engaged in activities to ensure the functioning of information systems and/or programmes for electronic computers, which are designed and/or used to receive, transmit, deliver, and/or process electronic messages of Internet users.*

The antivirus warning does not affect the company's business reputation

A microfinance organization (MFO)[6] has filed a lawsuit to protect its business reputation against the owner of the Dr.Web anti-virus software. Before visiting the MFO's website, users were informed by the anti-virus software that the website provided "bondage terms of cooperation". The MFO believed that this created a negative image of the company and asked a court to order the defendant to remove its website from the database of unrecommended websites and not to create obstacles for users to visit it.

The court rejected the claims, stating that the anti-virus software did infringe on the company's business reputation, as 1) it did not mention the owners of the website, 2) it did not make evaluative or other judgements about the MFO's activities, and 3) the information message about an unrecommended website did not actually prevent users from visiting it.

6 *Microfinance organization – a legal entity which carries out microfinance activities and provides microloans (microfinancing).*

Media content and advertisement

Liability for the violation of online advertisement labelling[7]

On 1 September 2023, administrative liability was introduced for the failure to comply with online advertisement labelling requirements.

Fines ranging from 200,000 RUB to 500,000 RUB are imposed on advertisers, advertisement distributors, and advertising system operators for:

- The failure to submit information about online advertisement to the Unified Register of Online Advertisement (the "Register");
- A violation of the terms for the submission of online advertisement information to the Register;
- The submission of incomplete, unreliable, or irrelevant online advertisement information to the Register;
- The distribution of online advertisement without an identifier or violating the requirements for the placement of an identifier.

Fines ranging from 300,000 RUB to 700,000 RUB are also imposed on advertising data operators for specific violations of the procedure for interaction with the Register and requirements for online advertisement identifier.

Regulation of recommendation technologies[8]

As of 1 October 2023, when using recommendation (profiling) technologies[9], owners of websites, mobile applications, or other information systems are obliged to:

- Prevent the use of recommendation technologies that violate the rights and legitimate interests of citizens and organizations, including the use of such technologies in violation of the law;

7 *For a more detailed overview, please refer to our newsletter on the subject.*

8 *For a more detailed overview, please refer to our newsletter on the subject.*

9 *Recommendation technologies are information technologies used to provide information based on the collection, systematization, and analysis of information relating to the preferences of users located in Russia.*

- Inform users about the use of recommendation technologies;
- Provide an email address for users to send requests;
- Publish the policy for the use of recommendation technologies in the Russian language with public access.

Roskomnadzor will monitor compliance with the above-mentioned requirements. If the identified violations are not addressed, Roskomnadzor may restrict access to the relevant information resource.

Practice

Court recovers compensation for use of a deepfake video

A court ordered a company to pay 500,000 RUB as compensation for using a deepfake video without a copyright holder's consent.

The defendant argued that the deepfake video was not subject to copyright due to the use of deepfake technology in its creation, in an attempt to prove that there was no infringement.

Eventually, the court of first instance upheld the claim for compensation and stated the following:

- Deepfake technology is a tool for processing videos, not for creating them;
- Editing a video using deepfake technology does not imply that it is available for free use or that there was no creative input in its creation.

Liability of website owner for defamatory comments

A user posted a negative review about a company's activities and its CEO on the 2gis.ru website. The company took legal action against 2GIS, seeking to have the information recognized as false, to force its removal, and to recover court costs.

When upholding the claimant's demands, courts stated that 2GIS should not only delete the negative review, but should also cover all of the claimant's legal expenses, since:

- 2GIS is responsible for the failure to delete defamatory information from its website;
- The payment of court expenses is not a penalty, but a legal consequence of the court's decision in favour of a particular party in the case;
- 2GIS's exemption from the reimbursement of court expenses is not consistent with the objectives of fair justice.

Personal data

Violations of biometric personal data processing and collection of written consent

On 12 December 2023, administrative liability was introduced for violations of the placement of biometric personal data in the Unified Biometric System (UBS). Fines for the illegal placement and updating of biometric personal data in the UBS are up to 1 mln RUB (for legal entities).

In addition, administrative fines were substantially increased for processing personal data without written consent when it is legally required or for violating the requirements for its content:

- For officials – up to 300,000 RUB for the first offence and up to 500,000 RUB for a repeat offence;
- For legal entities – up to 700,000 RUB for the first offence and up to 1.5 mln RUB for a repeat offence.

Greater fines and criminal liability for personal data breaches[10]

In December 2023, a draft law significantly increasing liability for personal data breaches, including for the failure to notify Roskomnadzor of a data breach, was submitted to the Russian parliament.

The draft law also proposes to supplement the CAO RF with other administrative offences and increase fines for offences already envisaged under the existing provisions of Article 13.11 of the CAO RF.

10 *For a more detailed overview of the expected changes in administrative and criminal liability for personal data breaches, please refer to our newsletter on the topic.*

Administrative offence	Fines for legal entities	
	Number of personal data subjects and/or identifiers	*Fine amount*
Action (inaction) resulting in the unlawful transfer (provision, distribution, or access) of personal data («data breach»)	From 1,000 to 10,000 personal data subjects and/or From 10,000 to 100,000 identifiers	from 3 mln to 5 mln RUB
	From 10,000 to 100,000 personal data subjects and/or From 100,000 to 1,000,000 identifiers	from 5 mln to 10 mln RUB
	More than 100,000 personal data subjects and/or More than 1,000,000 identifiers	from 10 mln to 15 mln RUB
	Repeat data breach: From 0.1% to 3% of annual income, but no less than 15 mln RUB and no more than 500 mln RUB	
Data breach of sensitive personal data	From 10 mln to 15 mln RUB **Repeat data breach:** From 0.1% to 3% of annual income, but no less than 20 mln RUB and no more than 500 mln RUB	
Failure to notify Roskomnadzor about a data breach	From 1 mln to 3 mln RUB	
Failure to notify Roskomnadzor about the intention to process personal data	From 100,000 to 300,000 RUB	
Unlawful personal data processing or personal data processing that is inconsistent with the purposes of its collection	From 150,000 to 300,000 RUB **Repeat offence:** From 300,000 to 500,000 RUB	

A separate draft law proposes to introduce criminal liability for offences related to unlawful personal data trafficking and data breaches.

For this purpose, there is a proposal to add Article 272.1 ("Unlawful actions with computer information containing personal data") to the Criminal Code of the Russian Federation. The article envisages a fine of up to 700,000 RUB, or forced labour for up to 4 years, or imprisonment for up to 4 years.

There is stricter liability for committing offences with grave consequences, which include the temporary suspension or disruption of a data controller's activity, the disruption of the integrity of information systems with personal data, or the distribution of computer information containing personal data to an unlimited number of third parties.

In certain cases, stricter liability is also envisaged, for example, if these criminal acts are committed with the use of special categories and biometric personal data, or are associated with the cross-border transfer of illegally obtained computer information with personal data or with the cross-border movement of carriers of such information.

The draft law also establishes criminal liability for creating and/or supporting the functioning of information resources on the Internet, an information system, or software for the illegal storage and the transmission of computer information containing personal data.

Unscheduled inspections by Roskomnadzor: New grounds during the moratorium period

In 2023, exceptions were introduced to the moratorium on business inspections, allowing Roskomnadzor, in agreement with the prosecution authorities, to conduct unscheduled inspections of data controllers in certain cases.

Unscheduled inspections by Roskomnadzor are possible when:

- Roskomnadzor has established a breach of a database containing personal data on the Internet;
- Roskomnadzor has identified three or more inconsistencies between a data controller's previously filed notification of intention to process personal data or carry out cross-border transfers and the privacy policy on the data controller's website.

There is a proposal to expand the grounds for unscheduled inspections to include cases where the regulator identifies the use of recommendation technologies with violations of the law.

In 2024, a draft law will be considered to grant Roskomnadzor the right to conduct on-site unscheduled inspections upon receipt of information about a data breach.

Enforcement practice

The first warning for a foreign company for a localization offence

A court issued a warning to Agoda Company Pte (a subsidiary of Booking Holdings) for the violation of personal data localization requirements.

The court ruled the following circumstances mitigated the company's liability:

- Lack of actual capacity to rent servers for localization of personal data collected through its website (due to the refusal by foreign providers to provide the relevant services and problems with accepting payment for services from Russian providers);
- Voluntary compliance with the localization requirements from the introduction of the requirements in 2015 until 2022 (i.e., until the termination of the server lease agreement by the foreign provider);
- The company's endeavour to comply with the requirements of Russian law.

Furthermore, the court noted that the company strives to sustain its presence in the Russian market, refrains from imposing any restrictions on Russian nationals, and continues to offer services to them.

Presumption about the user's actions under the account

When hearing a case on the lawfulness of sending a direct marketing message to a user, a court stated, among other things, that:

- Email is personal data, which is confirmed by the positions of the Russian government and the Ministry of Digital Development;
- Actions performed under a user's account on the website are deemed to have been performed by the user;
- Website owners are not obliged to verify whether an email address belongs to a specific person (except when required by law).

Telecommunications

Fines for telecom operators' failure to install SORM

Since 1 January 2024, turnover-based fines have been established for telecom operators for violating the requirements for the installation of a system of operational investigative measures (SORM)[11].

Failure to fulfil the obligation to connect to SORM is punishable by an administrative fine in the amount:

- From 1/1000 to 3/1000 of annual revenue for the first offence
- From 1/100 to 3/100 of annual revenue for a repeat offence

In both cases, the minimum fine is at least 1 million RUB.

Revenue is determined based on the market of communication service corresponding to the respective communication licence in the region of the Russian Federation where the offence was detected.

Significant increase in fees for licences to provide communications services

From 1 January 2024, the amount of the state duty for a licence for the provision of telecommunications services, which contain conditions to ensure the implementation of requirements for communication networks and SORM, is 1 mln RUB (the duty was previously 7,500 RUB).

The changes aim to prevent bad faith communications providers that fail to comply with mandatory licence requirements in terms of introducing SORM from entering the telecom services market.

11 *The system of operational investigative measures (SORM) is a set of technical means designed to carry out operational and investigative measures in telephone, mobile, and wireless communication and radio networks.*

New obligations for owners of technology networks[12]

On 1 September 2023, new requirements were established for owners of technological communication networks having an Autonomous System Number (ASN).

The new law actually extends some provisions of the "Yarovaya Law"[13] to the owners of technological communication networks with ASN, obliging them to comply with certain requirements regarding information storage and granting access to it for law enforcement bodies. Similar obligations apply to communication providers.

In particular, owners of technological communication networks with ASN are obliged to store the following information for 3 years in the territory of the Russian Federation and grant access to it to the state security bodies and agencies that carry out operative and search activities:

- Message metadata.[14]
- Information on interaction between users of informational systems and/or software operating in technological communication networks.
- User data, including information about the user identifier in the information system, user registration data, telephone numbers, email addresses, network addresses, etc.

12 *Please see the detailed overview in our newsletter.*

13 *In the media and public discussions, "Yarovaya Law" refers to Federal Law No. 374-FZ dated 6 July 2016 and Federal Law No. 375-FZ dated 6 July 2016.*

14 *Information about the receipt, transmission, delivery, and/or processing of voice information, text messages, images, sounds, video, or other electronic messages.*

E-commerce and retail

Law on a simplified procedure for online purchases in foreign online stores

As of 18 March 2023, the Law on Countering the Legalization of Illegal Earnings (Money Laundering) has been amended to exclude an additional verification procedure when making a purchase in a foreign online store for an amount of up to 15,000 RUB.

Exceptions will be made in cases where bank employees suspect money laundering or when transferring funds to an individual or a non-profit organization.

Previously, simplified identification (provision of personal data) was needed when placing an order in a foreign online store.

Updates to the pre-installation of Russian software on IT devices

In October 2023, the Russian government included the Chestny Znak (Honest Sign) app in the list of programmes that must be pre-installed on Android and IOS devices prior to their sale in 2023-2024.

Previously, the list of mandatory pre-installed programmes was supplemented with the RuStore app store. Rules for mandatory pre-installation on electronic devices sold in Russia were also approved for RuStore, even in the event of a ban by the right holders of operating systems.

From 30 August 2023, if a copyright holder of an operating system or its affiliate has banned or restricted the pre-installation of software, the producer of an electronic device or its authorized persons (sellers, distributors, etc.) must install it. Sales of electronic devices in violation of the pre-installation requirements may lead to fines of up to 200,000 RUB.

Enforcement practice

Risks of online sales: technical errors and consumer rights

DNS CASE[15]

In early 2022, a customer purchased electronics on the DNS store's website, but the seller refused to transfer the goods to the customer due to a technical error and a discrepancy between the price indicated on the store's website at the time the order was made and the actual price of the goods.

The court of first instance satisfied the buyer's claim, whereas the courts of appeal and cassation instances supported the seller.

When reversing the decisions of the courts of appeal and cassation instances, the Supreme Court of the Russian Federation sent the case back to be reheard, taking into account the following:

- An offer for the sale of goods published on a website that is directed to an unspecified number of parties contains information about the goods and the price (substantial terms and conditions of the agreement), and therefore constitutes a public offer, which is binding on the seller;
- Despite the technical errors, it was the prices generated by the seller that were stated in the public offer on the website, which the buyer agreed to by accepting the offer;
- The moment when the agreement was concluded in the online store constitutes the moment when the order was placed and a number was assigned to it. The price is fixed at the moment the agreement was concluded;
- The seller has no right to unilaterally change the price specified at the time the order was placed.

With this ruling, the Supreme Court of the Russian Federation essentially reaffirmed its position from similar disputes, which states that the seller has no right to unilaterally terminate an online retail sale contract, even despite technical errors in its conclusion.

AEROFLOT CASE

In October 2023, Aeroflot sold several thousand tickets for the route Yekaterinburg-Phuket at significantly low prices. Subsequently, the company annulled the ticket bookings, citing a technical error on its website when the orders were placed. After annulment, the ticket prices on the website for this route increased by several times.

Consumers then initiated a number of disputes, including a class action lawsuit against Aeroflot in the Presnensky District Court of Moscow. Several cases have already been resolved.

For example, the Verkh-Isetsky District Court of Yekaterinburg ruled in favour of a consumer's claim against Aeroflot and ordered the company to fulfil its obligation to transport passengers to and from Phuket (case No. 2-10084/2023).

15 *For a detailed overview of this case, please see our "Case in Practice" newsletter.*

The court stated the following[16]:

- An air carriage contract was concluded between the parties, and consumers were provided with a bill and itinerary receipt upon payment;

- The lists of cases involving the unilateral refusal to execute an air carriage contract and the cancellation of passenger reservations are exhaustive, and technical errors during the ordering process are not listed among them.

16 *Please note that an appeal has now been filed against this ruling, and a higher court may rule otherwise.*

Antitrust regulation

New Antimonopoly Package affecting digital platforms[17]

On 1 September 2023, the Fifth Antimonopoly Package came into force, which aims to prevent and suppress the monopolization of digital markets.

The package introduces the following key changes to antitrust regulation

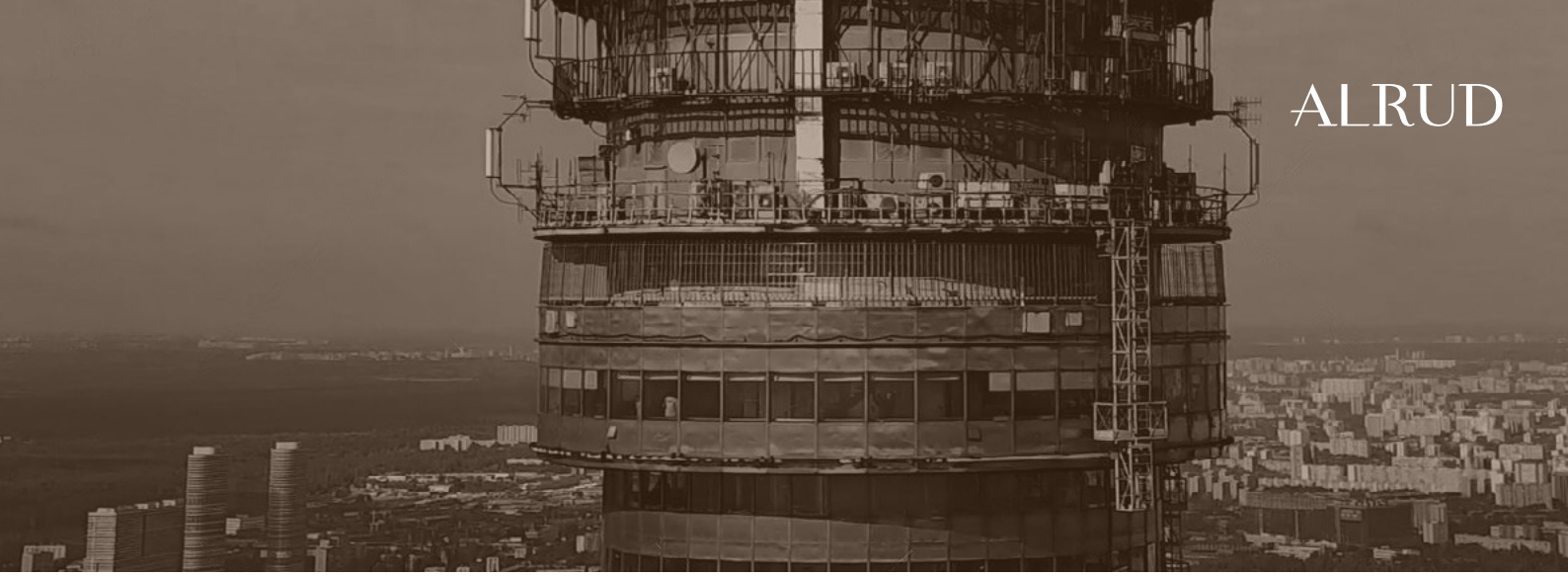
- Ban of monopolistic activities in digital markets if several factors are met:
  - The presence of a network effect[18];
  - The share of transactions via digital platforms is more than 35 % of the total volume of transactions on the commodity market;
  - The subject's revenue exceeds 2 billion RUB over the last year.
- Mandatory approval by the Federal Antimonopoly Service of transactions exceeding 7 billion RUB.

A business entity holding a dominant position may provide evidence that its actions (inaction) in the following forms may be recognized as admissible:

- An economically or technologically unjustified reduction or cessation of the production of goods;
- Creation of discriminatory conditions;
- Creation of obstacles to access or exit the commodity market for other business entities;
- Manipulation of prices on the wholesale and/or retail electricity (capacity) markets.

17 *Please see the detailed overview in our newsletter.*

18 *A special feature of a product market in which the consumer value of a computer programme within information and telecommunication networks, including the Internet, that enables transactions between sellers and customers of a certain product, depends on the number of such sellers and customers.*



TMT trends in 2024

Regulation of Big Data

A draft law on the regulation of the circulation of Big Data is expected to be adopted in 2024.

By the second reading in parliament, the draft law was amended with provisions regulating the use and circulation of anonymized data. In particular, at the request of the Ministry of Digital Development, there is a proposal for data controllers to transfer datasets generated based on the personal data of their clients, employees, and counterparties to a government information system (GIS).

Before transferring the data to the Ministry of Digital Development, data controllers must anonymize them. If anonymization is not technically possible, the data may be sent in its original form for subsequent anonymization in the GIS.

The datasets contained in the GIS will then be made available to state and municipal bodies and organizations, as well as to individuals and legal entities, including for the purposes of public administration and the development of AI services.

In addition, the draft law grants Roskomnadzor the right to establish requirements and methods for data anonymization.

Governmental clearance of IP transactions with foreign persons

The Draft Presidential Decree amending Presidential Decree No. 81 dated 1 March 2022 ("Decree No. 81") has been published.

The Draft decree extends the procedure established by Decree No. 81 for the clearance of transactions concluded between Russian residents and foreign persons of unfriendly states and persons they control to transactions involving (IP Transactions):

- The assignment of exclusive rights to the results of intellectual activity or means of individualization;
- The pledge of the exclusive rights to results of intellectual activity or means of individualization.

If the Draft is adopted, the conclusion and/or execution of IP Transactions will require

approval from the Government Commission for Control over Foreign Investments in Russia.

The failure to obtain approval may invalidate any IP Transactions that are concluded.

New procedure for including ODIs in Roskomnadzor's register

The Ministry of Digital Development has published a draft order granting Roskomnadzor the right to include in the register of ODIs Internet resources whose owners have twice failed to comply with the requirement for voluntary inclusion in the ODI register. Roskomnadzor will be able to enter information into the register after a repeated ruling on an administrative offence.

Bill on the regulation of marketplace activities

A bill regulating the activities of marketplaces has been submitted to the Russian parliament.

The bill proposes defining the legal status of marketplaces, introducing liability for inaccurate information and defective goods on marketplaces, regulating the imposition of fines by marketplaces, and limiting the options for changing an offer, among other things.

A draft law for regulating paid online subscriptions

A draft law to protect the rights of users with paid online subscriptions has been submitted to the Russian parliament.

The document requires sellers to notify users at least one day before the next debit for a paid subscription. If the seller fails to provide notification, they must return the money to the consumer. Additionally, the draft law grants Roskomnadzor control powers in this regard.

Limit on advertising in video games

A bill submitted to the Russian parliament proposes limiting advertising in video games to 15 seconds and showing it no more than once every 20 minutes.

There is also a proposal to place an additional restriction on video games for children so that adverts correspond to the same age category of children for which the video game itself is intended.

Combating piracy

A bill simplifying the procedure for taking down "mirrors" of pirate websites has been submitted to the Russian parliament. The bill proposes simplifying the mechanism for blocking "mirrors" by transferring this power from the Ministry of Digital Development to Roskomnadzor.

It also extends obligations for the deletion of "mirror" websites from search results to all search engines (the obligation currently only applies to Russian search engines).

Contacts

Maria Ostashenko
Partner

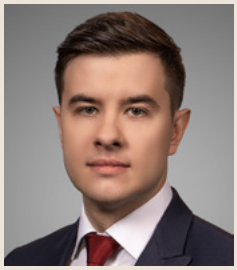
Commercial, Intellectual Property,
Data Protection and Cybersecurity

MOstashenko@alrud.com

Anastasia Petrova
Of Counsel

Data Protection and Cybersecurity

APetrova@alrud.com



Ilya Khodakov
Senior Associate

Intellectual Property

IKhodakov@alrud.com

Olga Gorokhova
Senior Associate

Competition/Antitrust

OGorokhova@alrud.com

Elizaveta Kostyuchenko
Associate

Intellectual Property,
Data Protection and Cybersecurity

EKostyuchenko@alrud.com

Skakovaya str., 17, bld. 2, 6th fl., Moscow, Russia, 125040
E: info@alrud.com | www.alrud.com | T: +7 495 234-9692

ALRUD