ALRUD

TMT Legal Digest

Key regulatory news in the TMT industry in 2024

Dear Ladies and Gentlemen,

We are pleased to present an updated summary of the most important laws, bills, and regulatory changes in the TMT industry over the last year, as well as the trends arising in industry regulation in 2025.

IP, media content and advertising

Compulsory levy on internet advertising revenues

From **01 April, 2025**, there will be an obligation to pay a levy on income from online advertising targeting Russian consumers.

Those liable to pay the levy include the following:

- Advertisers;
- Operators of advertising systems;
- Persons distributing online advertising on behalf of, in the interests of, or at the expense of the advertiser or the distributor of the advertising;
- Advertisers who have concluded an agreement on advertising distribution in Russia with a foreign entity.

The levy is 3% of the quarterly revenues for the provision of online advertising services targeting Russian consumers.

The Federal Service for Supervision of Communications, Information Technology, and Mass Media (**Roskomnadzor**) will calculate the levy and monitor the timeliness of its complete payment based on information from the Unified Online Advertising Register.

The mechanism for patenting IT solutions has been clarified

The Ministry of Economic Development adopted a Decree establishing the specifics of registering and preliminarily searching for information in relation to patents for utility models and inventions in the IT field:

Specifically, the Decree stipulates:

- The concepts of utility models and inventions in the IT sphere, defining their key features;
- The requirements for the essence of utility models and inventions in the IT sphere;
- The criteria and procedure for checking the inventive stage of innovation in the IT field and the grounds for recognizing a claimed invention as non-compliant with the conditions for patentability under Clause 5 of Article 1350 of the Civil Code of the Russian Federation (**Civil Code**).

The changes came into force on **25 May 2024**.

Previously, the mechanism for protecting technical solutions in the IT field was arduous due to the difficulty of distinguishing between patentable and non-patentable solutions in this area. It is expected that these changes will simplify the patenting of IT solutions and help strengthen the protection of developers' rights, including in the field of artificial intelligence.

A new procedure for IP purchase from "unfriendly" rights holders

From 20 May 2024, on the basis of Decree of the Russian President No 430, a temporary restrictive procedure was introduced for the purchase by Russian residents of exclusive rights to the results of intellectual activity and the means of individualization from "unfriendly" foreign rights holders.

The execution and fulfillment of monetary obligations under such transactions requires permission from the Government Commission for Control over Foreign Investments in Russia (**Government Commission**).

Payment for these transactions is subject to transfer to a special "O"-type account. The subsequent transfer of funds to the bank accounts of the rights holders is conducted with the permission of the Government Commission.

The temporary procedure does not apply to transactions:

- for the purchase of exclusive rights to scientific, literary or artistic works, performances, phonograms, or the broadcasts of broadcasting or cable organizations;
- for which the purchasers' obligations does not exceed RUB 15 mln or the equivalent in foreign currency.

Banning "trash streams"

Changes have been adopted to combat so-called "trash streams", which is defined as information that is disseminated out of antisocial, mercenary or other sinister motives and:

- offends human dignity and public morals;
- expresses a clear disrespect for society;
- contains imagery of actions with signs of illegality, including violence.

For the dissemination of such information on the Internet, prosecution has been introduced in the form of fines and the confiscation of the equipment used for the production of such materials (Part 12 of Article 13.15 of the Code of Administrative Offenses of the Russian Federation (**CAO RF**):

- for citizens – up to RUB 100,000;
- for officials – up to RUB 200,000;

- for legal entities – up to RUB 1 mln.

In addition, according to the amendments to the Criminal Code of the Russian Federation (**CC RF**), the commission of an intentional crime involving public demonstration, including in the media or on the Internet, is considered an aggravating circumstance under a number of articles of the CC RF.

Online cinemas may be obliged to obtain distribution certificates

A bill has been submitted to the Russian Parliament which proposes to prohibit audiovisual services from distributing films without distribution certificates.

The bill also introduces a new reason for refusing to issue a distribution certificate – the inclusion in a film of material that promotes the denial or discreditation of traditional Russian spiritual and moral values.

Register of bloggers

From **01 November 2024**, owners of channels and pages in social networks with an audience of over 10,000 users are obliged to register with Roskomnadzor. This only applies to social networks included in Roskomnadzor's register of social networks.

As of **01 January 2025**, bloggers who have not submitted information to the register are prohibited from posting advertisements or information about funding (seen as "donations"), and other users cannot repost from their channels.

Proposal to ban advertising on prohibited resources

The bill on the prohibition of advertising distribution was adopted in the first reading. The bill prohibits advertising:

- On informational resources belonging to foreign/national organizations undesirable in the Russian Federation, as well as on the resources of extremist and terrorist organizations;
- On other informational resources, access to which is restricted in accordance with the legislation of the Russian Federation.

The penalties for spam calls have increased

From 17 April 2024, liability for non-compliance with the requirements for advertising distributed over telecommunications networks was introduced.

The new rules provide for significantly higher administrative fines (Part 4.1 of Article 14.3 of the CAO RF):

- for officials – up to RUB 100,000;
- for legal entities – up to RUB 1 mln.

This offence covers, in particular, non-consensual advertising via SMS messages, telephone calls, emails, automated calls and mailings.

New regulation for "orphaned" works

On 21 October 2024, a law came into force establishing the legal regulation of "orphan" works, i.e., objects of copyright and related rights in respect of which:

- the name (title) of the author (rights holder) has not been established; or
- there is no information about the place of residence/legal address of the author (copyright holder).

The governance of the use of "orphaned" works' is entrusted to accredited collective rights management organizations, which will maintain a register of orphaned works, grant licenses for their use to interested parties and make payments to the right holders in the event of their disclosure/identification.

In order to obtain a license for an orphaned work, an interested party must take steps to identify the rightholder and the rightholder's domicile or location. If the rightholder cannot be found, the interested party should apply to the accredited organization with a request for the right to use the selected copyright or related object of rights.

After verification, the organization will place an announcement that it is searching for the author (right holder). If the author is not identified within 90 working days, the organization will issue a license. The object can be used only after the payment of remuneration to the the accredited organization.

The law only applies to:

- Literary and artistic works;
- Photographs and works obtained by similar means;
- Music, phonograms, and performances.

Proposal to protect voice rights

A bill has been submitted to the Russian Parliament proposing to supplement the Civil Code with a new Article 152.3, which establishes the protection of voice as an object of a citizen's personal non-property rights.

It is proposed to allow the publication and further use of a recording of a citizen's voice, created with the help of special technologies (e.g., artificial intelligence), only with the consent of the citizen.

Expected changes in advertising regulation

The Federal Antimonopoly Service (**FAS**) has proposed draft amendments to advertising legislation.

It is proposed to exclude several pieces of information from the definition of "advertising", in particular, information about a product, its manufacturer or seller published on an information resource of a seller or aggregator owner which does not contain information of an advertising nature.

For some violations, it will be mandatory for FAS to issue a warning, provided that two conditions are both met:

- If no warning has been issued to the same person in the last 12 months (for all violations for which such a measure is envisaged);
- If the disputed advertisement does not contain evidence of other violations for which the issuance of a warning is not envisaged.

Distinction between advertising and non-advertising information

FAS has published a Draft Government Decree approving the criteria for classifying information disseminated on marketplaces, classifieds and search engines as advertising.

The Draft Decree contains:

- general criteria for classifying information published in such resources as advertising;
- concepts of reference and analytical materials and announcements that cannot be classified as advertising.

If adopted, the Decree will enter into force on **01 April 2025** and will be valid for 6 years from the date of its entry into force.

Enforcement practices

For the first time, the court recovered compensation for stealing a reels video

The Moscow Arbitrazh Court recovered RUB 300,000 in compensation from a sole proprietor who copied someone else's video reels on a social network to advertise its own services.

The court stated that the defendant had unlawfully used the video, as it had completely copied the text, sequence, structure and content of the audiovisual clip, and placed similar images in the background of the text. The amount of compensation was justified, inter alia, by the costs incurred by the claimant in creating the video.

The decision on the recovery of compensation was upheld by the court of appeal and the court of cassation.

Borrowing patient reviews from someone else's website was found to be an infringement

A company that owns a patient review website has sued the other company for unlawfully copying reviews from its website.

The Intellectual Property Court found the claims to be justified. Even though the reviews were not created as creative work and do not meet the criteria of literary works, the claimant has exclusive rights to the website content.

As a result of the proceedings, the defendant's actions in borrowing reviews from the claimant's website were recognized as an infringement of the claimant's rights to the website content and the plaintiff's claims for compensation were satisfied.

Early termination of trademarks of foreign companies

The Intellectual Property Court upheld the claim of a Russian company against the Swedish telecommunication equipment manufacturer Telefonaktiebolaget LM Ericsson and terminated the legal protection of its Russian trademarks No. 205234, No. 207822, No. 253069 and international trademarks No. 1024858 within the Russian Federation in respect of goods of the 11th class of the Nice Classification due to their non-use.

The Presidium of the Intellectual Property Court, in an instance of cassation upheld the first instance decision.

Also in 2024, a number of lawsuits were filed for early termination of the trademarks of Amazon Technologies, Amazon Europe Core, Nokia Corporation, Nokia Solutions & Networks Oy, NEC Corporation and others.

In 2025, such disputes are expected to increase, especially in relation to foreign companies that have left the Russian market.

Information technologies

Ban on the dissemination of scientific information and statistics about VPN services

From **01 December 2024**, a ban on the dissemination of scientific, scientific-technical and statistical information about VPN services that provide access to information resources prohibited in Russia was established.

Information of this nature may be disseminated only in relation to VPN services as a means of information exchange using secure communication channels.

Roskomnadzor has already blocked about 200 VPN services. As part of this ban, Apple blocked mobile applications of VPN services in the App Store in Russia at the request of Roskomnadzor. According to public sources, about 100 apps have already been blocked.

New rules for inclusion in the register of domestic software

The Ministry of Digital Development has drafted amendments to the rules of forming the Russian software register.

Among the changes, it is proposed that software must be compatible with at least two Russian operating systems of different right holders that meet certain requirements, and software as part of an appliance must be compatible with one such operating system.

A transition period has been established The new requirements will be phased in between 1 June 2025 and 1 January 2027.

Office software and virtualization tools will be the first to be subject to the requirements, while industrial software and process management products will be the last.

New requirements for import substitution and categorization at CII facilities[1]

The Russian Parliament is considering a bill that partially changes the system of requirements for ensuring the protection of major facilities of critical information infrastructure (CII), providing for the

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

following provisions:

- the transition of CII subjects to preferentially use Russian software and radio-electronic products. It will be possible to use foreign software only upon approval of the Russian Government, which will establish the cases and procedure for approving such use;
- a new procedure for categorizing CII, which, inter alia, includes the use of lists of typical industry-specific CII facilities, as well as methodological guidelines regulating the industry-specific aspects of categorizing CII facilities;
- a new authority of the Russian Government to establish the requirements for software and electronic products used at CII facilities.

The consideration of the bill has been postponed until the spring 2025 session.

Enforcement practices

Restrictions on foreign services

In the summer of 2024, the speed of YouTube was reduced. Roskomnadzor commented that Google's violations of Russian law were the basis for the measures taken. In response to ISPs' attempts to speed up YouTube, Roskomnadzor reported the risk of their licenses being revoked.

Also in the second half of 2024, Roskomnadzor restricted access to Discord and Viber due to violations of Russian legislation on information distribution organizers and failure to remove banned content.

WhatsApp, Skype and 10 more services are included in the ODI register

Roskomnadzor included the messengers WhatsApp, Skype, Wire, Element, KakaoTalk, Session, Crypviser, DUST, Pinngle Safe Messenger, Status, Keybase, and Trillian in the register of information distribution organizers (**ODI**), which obliges them to store data on users' correspondence and calls and provide it to state authorities upon request.

Note that in 2024, Roskomnadzor received the right to forcibly add companies to the ODI register in the event of repeated failure to fulfill the requirement to be included in the register. Earlier in 2024, about 20 foreign companies, including WhatsApp, Snapchat, and Skype, were fined for repeated failure to be included in the register of ODIs.

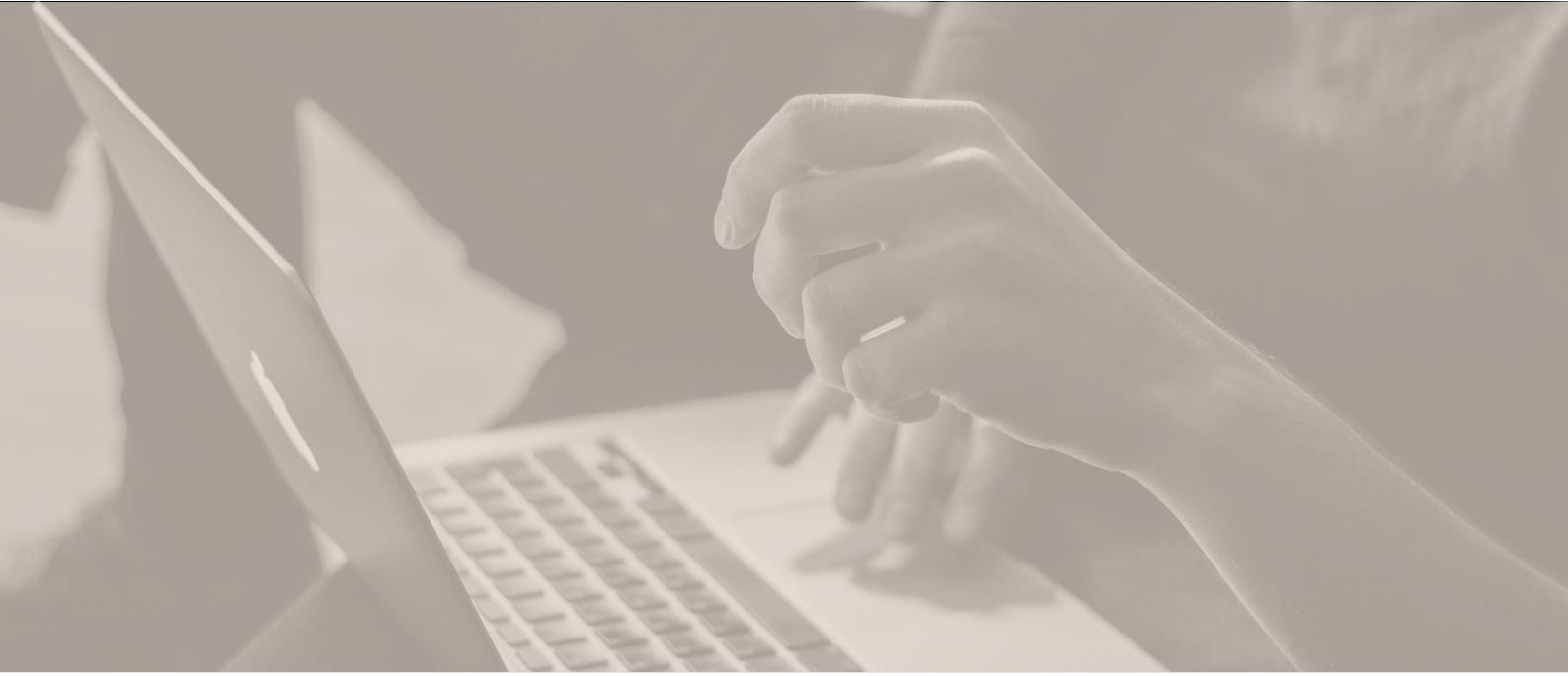
Roskomnadzor started blocking the websites of "unlanded" companies

In spring 2024, Roskomnadzor blocked access to the websites of 12 hosting providers: Kamatera, WPEngine, HostGator.com, Network Solutions, DreamHost, Bluehost, Ionos, DigitalOcean, GoDaddy, Amazon Web Services, Fastcomet and Hetzner.

Earlier, coercive measures were taken against all the above providers: noting their violation of the Russian legislation in search engines, as well as banning them from search engine optimization.

For the first time, the reason for the blocking was non-compliance with the requirements of the "landing" law, among the main requirements of which is for foreign IT companies to open a local office in Russia.

In addition, for non-compliance with the requirements of the "landing" law in January 2024, "unlanded" hosting providers were prosecuted under Part 2 of Article 13.49 of the CAO RF with a total of RUB 370 mln in fines collected.



Personal data

Enhancing liability for data breaches[2]

Federal laws designed to enhance administrative liability and introduce new criminal offences in personal data processing have been adopted.

Amendments to the CAO RF

Additional administrative offences in the field of personal data violations in the CAO RF and increase of fines for existing offences as set out in Article 13.11 of the CAO RF will come into force on **30 May 2024**.

Offence	**Fine amount for legal entities and individual entrepreneurs[3], RUB**
New offences under Article 13.11 of the CAO RF	
Data breach *Parts 12-14 of Article 13.11 of the CAO RF*	
from 1,000 to 10,000 personal data subjects and/or from 10,000 to 100,000 identifiers [4]	from 3 mln to 5 mln

[2] *For a more detailed overview, please refer to our newsletter on the subject via the link.*

[3] *Please note that, in accordance with Parts 1.1 and 8-18 of Article 13.11 of the CAO RF,* ***individual entrepreneurs are held liable as legal entities.*** *However, the elements of Parts 10-18 of the CAO RF* ***do not extend liability*** *to the officials of non-governmental organizations (e.g., DPOs).*

[4] *An identifier is a unique designation of information about an individual contained in the controller's personal data information system and related to such a person.*

Offence	Fine amount for legal entities and individual entrepreneurs[3], 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
more than 100,000 personal data subjects and/or more than 1,000,000 identifiers	from 10 mln to 15 mln
Repeated data breaches, if the individual has been held liable under Parts 12–15 or 16–18 of Article 13.11 of the CAO RF *Part 15 of Article 13.11 of the CAO RF*	from 1 to 3 % of annual income, but no less than 20 mln and no more than 500 mln
Data breaches of sensitive personal data *Part 16 of Article 13.11 of the CAO RF*	from 10 mln to 15 mln * *regardless of the number of personal data subjects whose personal data was leaked*
Data breaches of biometric personal data *Part 17 of Article 13.11 of the CAO RF*	from 15 mln to 20 mln * *regardless of the number of personal data subjects whose personal data was leaked*
Repeated data breaches of sensitive personal data or biometric personal data, if the individual has been held liable under Parts 12–18 of Article 13.11 of the CAO RF. *Part 18 of Article 13.11 of the CAO RF*	from 1 to 3 % of annual income, but no less than 25 mln and no more than 500 mln
Failure to notify and/or late notification of Roskomnadzor about a data breach *Part 11 of Article 13.11 of the CAO RF*	from 1 mln to 3 mln
Failure to notify and/or late notification of Roskomnadzor about the intention to process personal data *Part 10 of Article 13.11 of the CAO RF*	from 100,000 to 300,000
Increased fines under Article 13.11 of the CAO RF	
Unlawful personal data processing / personal data processing is incompatible with the purposes of its collection *Part 1 of Article 13.11 of the CAO RF*	from 150,000 to 300,000 Repeated offence: from 300,000 to 500,000

Some other changes to the CAO RF are as follows:

- Mitigating and aggravating circumstances are established separately for repeated data breaches of the specified offences;
- Cancellation of the previously valid discount of 50% for the payment of a fine for an offence under Article 13.11 of the CAO RF, identified during state or municipal monitoring;
- The jurisdiction of the offences of Article 13.11 of the CAO RF will be attributed to arbitrage courts. Up till now, these cases were considered by magistrates;
- Introduction of new offences related to violations of biometric personal data processing in the Unified Biometric System (**UBS**) and other information systems (Parts 2–4 of Article 13.11[3] of the CAO RF).

Amendments to the CC RF

As of **11 December 2024**, a new criminal offence set out in Article 272.1 relating to the illicit trafficking of personal data has been introduced in the CC RF.

Examples of offences under Article 272.1 of the CC RF	**Punishment**
Unlawful use and/or transfer (provision, distribution, or access), collection and/or storage of computer information containing personal data obtained through unlawful access to the means of its processing or storage, other interference in its functioning, or through other unlawful means[5] *Part 1 of Article 272.1 of the CC RF*	• *a* fine of up to RUB 300,000 or in the amount of other income for the period up to 1 year • forced labour for up to 4 years • or imprisonment for up to 4 years If the case involves the cross-border transfer of personal data or a personal data carrier[6]: • imprisonment for up to 8 years and a fine of up to RUB 2 mln / in the amount of other income for the period up to 3 years and deprivation of the right to hold certain positions / engage in certain activities for up to 4 years
Creation and/or maintenance of an information resource (on the Internet, an information system or software) for the purpose of facilitating the deliberate storage, transfer (distribution, provision, access) of computer information obtained illegally.	a fine of up to RUB 700,000 or in the amount of other income for the period up to 2 year with deprivation of

[5] *In certain cases, stricter liability is imposed, such as in cases where these criminal acts are perpetrated using sensitive categories of personal data, biometric personal data, or personal data of minors.*

[6] *The cross-border movement of a personal data carrier is defined as the importation into the Russian Federation and/or exportation from the Russian Federation of a machine-readable carrier (including magnetic or electronic) on which information is recorded and stored.*

Part 6 of Article 272.1 of the CC RF	the right to hold certain positions / engage in certain activities and • forced labour for up to 5 years; or • imprisonment for up to 5 years

The law on the anonymization of personal data and new requirements for their destruction has been adopted

Starting from **1 September 2025**, at the request of the Ministry of Digital Development, data controllers will be obliged to provide a list of personal data obtained as a result of anonymisation for the formation of anonymised data compositions in a specially created state information system (**GIS**).

The request from the Ministry of Digital Development must contain a list of the requested anonymized personal data, as well as the deadline by which they are to be provided.

Upon receipt of the request, the data controller must anonymise the personal data in accordance with the relevant requirements and anonymisation methods and provide the data to the GIS. Once the data has been submitted to the GIS, no further retrieval is possible.

The law also introduces new requirements for the destruction of personal data. As of **8 August 2024**, data controllers are obliged to use means of information protection that comply with the established procedure of conformity assessment and include the method of information destruction.

Bill on separate consent for personal data processing

The bill which imposes an obligation on data controllers to obtain consent for the processing of personal data separately from any other information and documents confirmed and/or signed by the personal data subject was adopted in its first reading.

It also introduces a ban on restricting consumers from accessing information on goods due to a consumer's refusal to provide personal data.

It is important to note that data controllers are already obliged to collect consent separately from other documents. In other words, consent for data processing cannot be included into other documents (contracts, user agreements). The law essentially consolidates a long-established business practice and the regulator's enforcement.

Bill on a form of withdrawing consent

The bill specifies the form in which consent may be withdrawn and obliges the data controller to ensure that consent may be withdrawn in the same form in which it was given. Thus, if consent is given in electronic form, it must also be possible to withdraw it in electronic form.

Data controllers collecting personal data via the Internet must ensure that consent can be withdrawn both in writing and electronically.

Bill on the criminalization of deepfake offences

The bill introduces amendments to several articles of the CC RF, imposing criminal liability for:

- defamation with the use of fake images, voice or biometric data (Art. 128.1);
- theft with the use of fake images, voice or biometric data (Art. 158);
- fraud, extortion and causing property damage with the use of falsified data (in particular, biometrics, as well as the image or

voice of the victim or his/her relatives)
(Articles 159, 159.6, 163, 165).

Expected updates of the grounds for personal data processing and the introduction of new institutions in privacy legislation

According to Roskomnadzor and State Duma officials, the concept of introducing the institution of special data controllers is currently being developed. It is assumed that only those data controllers who have duly passed state accreditation/certification will be allowed to process personal data. According to the authors of the initiative, this will ensure the security of processed personal data, as they will be processed by "professional data controllers".

Another initiative under development is the introduction of industry standards and templates for the processing of personal data. As part of this initiative, it is proposed to conduct a global review of the grounds for processing personal data provided by the current privacy legislation.

The templates and standards should be developed after a thorough study of each industry, which will ultimately minimize the amount of personal data collected from individuals. One of the main objectives of the authors of the initiative is to eliminate processing by consent alone, as this leads to uncontrolled and excessive processing of personal data by data controllers.

Enforcement practices

Assignment as a legitimate interest

Where there is a legitimate interest, the transfer of personal data by an employer cannot be made conditional on obtaining the employee's consent. Such a conclusion reached by a court in a dispute between an employer and an employee.

A company transferred an employee's personal data to a personnel administration and payroll agency without the employee's consent, which was required to comply with the requirements of the labor legislation.

The employee considered the transfer of personal data to be unlawful. However, the court noted that the processing of personal data was carried out within the framework of the company's legitimate interests and could not be made conditional on obtaining the employee's consent to the processing of personal data. Otherwise, the rights of the company itself would have been violated; it would have faced prosecution for failure to comply with labor law obligations.

Data transfer for the purposes of a court dispute with an employee

A former employee claimed moral damages for the disclosure of his personal data, without consent, to a lawyer who had rendered services to the employer in another dispute with the employee.

The court decided in favor of the company, relying on the employer's legitimate interest. Transfer of information on the employee's labor activity and a traffic accident caused by the employee, which was the reason for the dispute, was within the limit of the information needed for the lawyers to assess the employer's claims.

The case of a medical clinic: when legitimate interests should not be relied upon

A patient submitted a pre-trial claim to a medical clinic on the quality of medical services rendered. The clinic engaged lawyers to defend its rights and shared the patient's claim with them.

The lawyers received the text of the pre-litigation claim without access to the patient's medical information. The client and the clinic then entered into a pre-litigation settlement agreement. However, the patient believed that his personal data had been illegally disclosed to the lawyers and filed a complaint with Roskomnadzor. The regulator issued an order to the clinic to ensure that the lawyers stopped processing the patient's personal data.

The clinic challenged Roskomnadzor's decision in court, arguing, inter alia, that it had a legitimate interest in disclosing patient data to the lawyers.

However, the Appeals Court rejected this argument, noting that the use of legitimate interest as a basis for processing personal data must necessarily respect the rights and freedoms of the data subject. According to the court, the clinic had failed to prove that the transfer of personal data without the patient's consent did not violate the patient's right to confidentiality and did not contradict the purposes of Federal Law "On Personal Data".

The clinic appealed to the Supreme Court of the Russian Federation, but the court rejected the appeal and upheld the decisions of the lower courts.

Telecommunications

Changes in the regulation of communications

New rules and requirements for the activities of telecom operators have been introduced. Some of the specifics are as follows:

- changes to the rules of traffic flow through technical means of counteracting threats (TSPU);
- the obligation to provide data on the terminal equipment of subscribers;
- authorizing Roskomnadzor to manage communication networks at the request of the Prosecutor General or his deputies;
- changes in the rules on licensing of activities in communications services.

For instance, new rules on licensing in the field of communications services provide that a license request shall be supported by a construction schematic of the communications network, as well as agreement on this schematic with the Federal Security Service (**FSB**).

If the territory in which communication services are provided changes, the application for amendments to the register of licenses in the field of communication is to be accompanied by a construction schematic of the communication network, as well as approval of the schematic by the FSB. An application for an extension of a license's validity period is to be accompanied by a construction schematic of the communication network, as well as the agreement wit this schematic from the FSB.

Bill for the regulation of mass calls and the labeling thereof

The Ministry of Digital Development has developed a bill to amend the Federal Law "On Communications" regarding the regulation of mass phone calls.

The bill suggests that the following provisions should be introduced into the law:

- obligation of a subscriber (legal entity or individual entrepreneur) that initiates mass phone calls to inform the telecom operator in advance about itself and the purpose of the calls;
- obligation of the telecom operator to label all calls and transmit the labeling to the network of another telecom operator without any changes;
- obligation of the mobile operator to block a phone call if no labeling is specified;

- obligation of the mobile operator to ensure the display of the labeling received on the screen of the users' (terminal) device.

Thus, according to the draft, any phone call from legal entities and individual entrepreneurs is to be labeled.

Procedure for collecting network addresses from telecom operators

Roskomnadzor has developed a draft order on the collection of information, which allows it to identify the means of communication and user equipment.

The order sets forth an obligation for telecom operators to submit to Roskomnadzor:

- information that allows it to identify means of communication and user's (terminal) devices over the Internet;
- the network addresses allocated for the use of these means of communication;
- information on changes to the above.

The draft order is applicable to (i) telecom operators granting access to the Internet and (or) services connecting another telecom operator to their communication network, as well as (ii) telecom operators rendering services of connection to their data transfer network to the data transfer network of another telecom operator providing access to the Internet.

The purpose of the innovation is to determine the attribution of Internet traffic to a particular user and his/her terminal device.

Revocation of IP telephone licenses

At the end of December 2024, the Russian Government excluded communication services on data transfer intended for the transfer of voice information from the list of licensed communication services.

In the view of the Government, such licensed communication services were actively exploited by fraudsters who used the Internet to contact a person on a fixed phone or mobile communication network. Therefore, it was decided to disallow the connection of data transfer networks to phone communication networks.

Note that the Ministry of Economic Development criticized this initiative. This exclusion from the list of services obliges current licensees to obtain a license to render local phone communication services, resulting in unreasonably high expenses for the operators.

These changes will come into effect as of 1 September 2025.

New rules for rendering phone communication services

On 1 September 2024, the new Rules for rendering phone communication services, approved by the Russian Government, came into force.

Some of the main changes are as follows:

- Distinguishing the definitions of "tariff" and "tariff plan". According to the new Rules, a tariff is a price set by the telecom operator for a separate unit of communication services, while a tariff plan is a set of conditions under which the operator offers the use of one or several of its communication services. The operator may change a tariff, but not a tariff plan.
- Introducing the obligation of a telecom operator to notify subscribers of tariff changes at least 10 days prior to the change.
- Extending the means of concluding an agreement on rendering communication services. Agreements are to be concluded in writing, inter alia, via the Internet, or through the implicative actions of the subscriber.

The new Rules also provide subscribers with an opportunity to change operators while keeping their existing numbers.

Introduction a disposal fee on foreign equipment is postponed

According to the comments of the head of the Ministry of Digital Development, the Russian Government has postponed the introduction of a disposal fee on the import of foreign telecommunication equipment.

In 2023, the issue of introducting a disposal fee on telecommunication equipment was included in the Strategy of development of the telecommunication industry up to 2035.

This initiative was aimed at supporting Russian industry: it was planned to invest the funds raised from the fee in the development, modernization and support of the production of Russian analogues of such equipment.

A system for collecting and processing the anonymized geo-metrics of mobile devices

Based on information from public sources, the Ministry of Digital Development intends to create a system to collect and process anonymized data on the location of subscribers and their movements. These data will be collected from mobile operators.

As of now, the system is being developed on the Russian unified platform for state services and information systems of public authorities, "Gostech". The system may be launched in 2025.

The text of the relevant regulation has not been published yet.

Blocking calls in messengers

Based on the public comments of senators and Roskomnadzor, a ban on calls from foreign states via messengers may be introduced in the bylaws to prevent fraud.

Telecom operators can already block calls from abroad. Users have the option to unblock all of them or only those received from the numbers in their contacts.

The state regulator is currently working on two possible options for regulatory changes:

- blocking voice traffic in messengers from abroad only;
- a complete ban on voice calls in messengers.

Based on Roskomnadzor's comments, some telecom operators are currently actively working on imposing autonomous bans on incoming calls from users abroad.

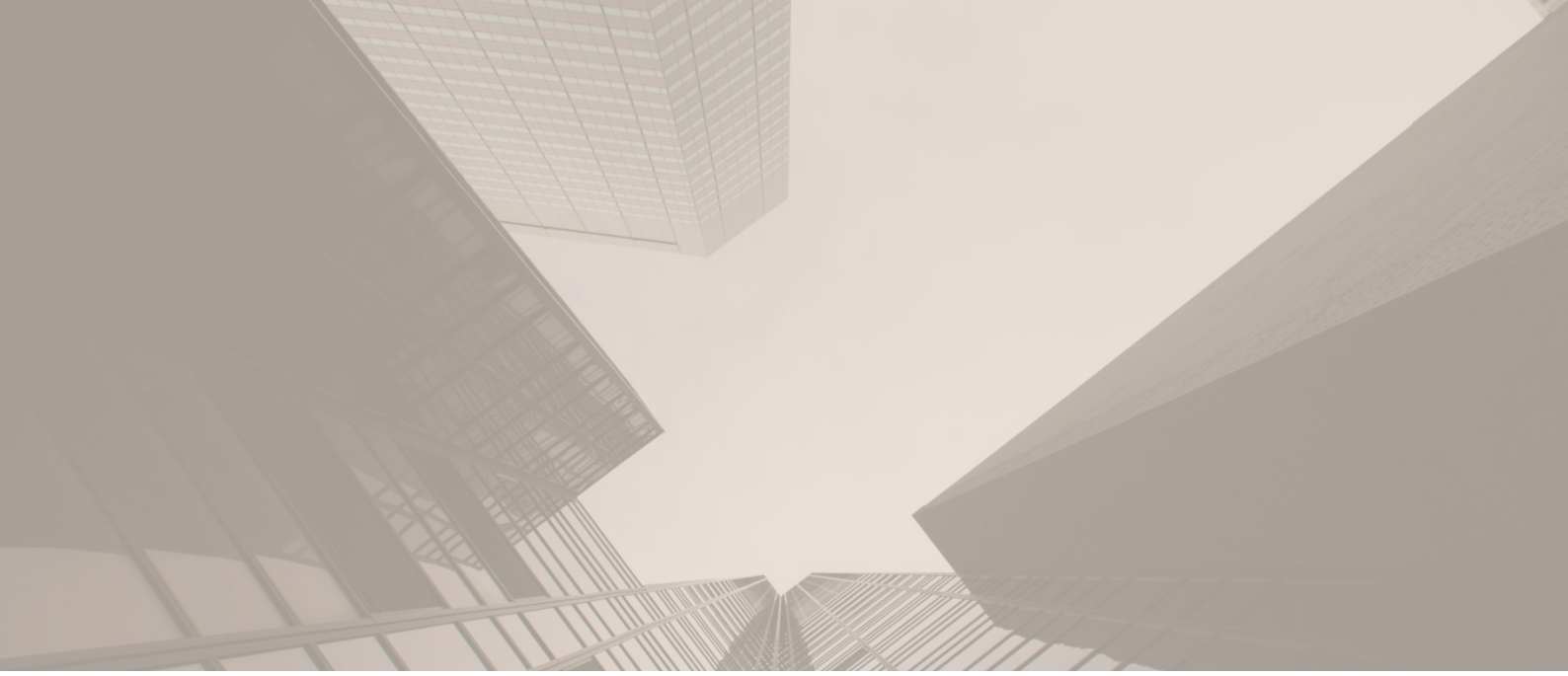
Enforcement practices

First lawsuit against a telecom operator for the theft of money by fraudsters

Telecom operators are obliged to prevent their subscribers from receiving calls in certain cases, including blocking traffic from substitute numbers that are often used by fraudsters. Failure to fulfill this obligation entails liability and a large fine for the operator under Part 2 of Article 13.2.1 of the CAO RF.

Court decisions on holding operators liable under this Article are quite common in practice. However, in June 2024, the Prosecutor's Office of the Leningrad Region filed a claim against Megafon PJSC, creating a very serious precedent. The prosecutor's office filed a claim to collect monetary funds stolen by phone fraudsters in favor of the injured party.

Subsequently, the parties entered into a settlement agreement. The risk of a telecom operator being held liable for overlooking the substitute numbers of fraudsters or the mistakes of its subscribers is worthy of attention.



Business Inspections

Key changes for business inspections

On 28 December 2024, Federal Law No. 540-FZ was adopted and came into effect, introducing key changes to the rules for business inspections.

Grounds for inspections

Some amendments were made to the list of general grounds for conducting control and supervisory measures (**CSM**):

- Now, to conduct a CSM based on a review of information on the risk of harm to legally protected values (inter alia, based on a citizen's claim), there should be reliable information on:
  - a threat of causing harm to life or grievous or moderate bodily injuries to citizens / state defense and security / the environment / cultural heritage sites;
  - violation of mandatory requirements for activities subject to licensing, certification, accreditation, inclusion in the register, etc.

  If the foregoing criteria are met, the authorized body shall initiate an unscheduled CSM within 24 hours with mandatory notification of the prosecutor's office.
- The following new grounds were added:
  - carrying out entrepreneurial activities without mandatory notification / without a license / without mandatory submission of information to the state information system on the mandatory labeling of goods;
  - evasion of a mandatory preventive visit (**profvisit**).

The list of cases in which the controlling authority shall decide to conduct a CSM was extended with the following:

- risk of natural disasters / technogenic emergencies;
- detection of a data breach on Internet, etc.

An unscheduled documentary inspection or an unscheduled on-site inspection, as a general rule, can be conducted only subject to the approval of the prosecutor's office.

Frequency of inspections

The following frequency of scheduled CSMs and mandatory profvisits has been set:

- no less than 1 but not more than 2 scheduled CSMs per year for controlled objects of extremely high risk (can be replaced by a mandatory profvisit);
- one CSM in two years or one profvisit per year for high-risk objects;
- for objects of a significant, medium or moderate risk category, the frequency is determined by the Russian Government.

Preventive visits

A fundamentally new regulation on conducting profvisits has been introduced.

The types of profvisits are as follows:

- **Voluntary profvisit** initiated by the controlled person – only for small businesses, socially oriented non-profit organizations or state/municipal entities.

The monitored person has the right to cancel a voluntary profvisit at least 5 business days prior to the date of the visit.

Explanations received by the monitored person during a profvisit made on its initiative are of a recommendatory nature.

- A new institution is **mandatory profvisits**, which cannot be canceled by the monitored person.

A Mandatory profvisit is conducted:

- For high-risk monitored objects- once a year[7];
- Within 6 months of the notification of the launch of certain types of entrepreneurial activity[8];
- Upon an event specified in the program of inspections;
- By order of the President of the Russian Federation, the Head of the Russian Government or his deputy, the Governor, etc.

As a general rule, the period for conducting a mandatory profvisit is not to exceed 10 business days. Violations revealed during the mandatory profvisit shall be eliminated within the specified timeframe, otherwise the monitored person may receive a writ.

Public assessment of compliance with requirements

Inspectors will have a right to issue a public assessment of the level of compliance with mandatory requirements to the monitored persons or objects of monitoring (e.g., in the form of a publication on the website of the monitoring body). The rating depends on the outcome of a preventive or supervisory event.

The procedure and criteria for assigning a rating are specified in the regulation on the type of monitoring. The government has the right to determine the cases in which the assignment of a rating is mandatory.

Mobile Supervisor

The law introduces the opportunity to use the mobile application Inspector for remote inspections.

It may be used to conduct an inspectorial or preventive visit, an on-site inspection or a raid inspection.

[7] The frequency of mandatory profvisits, including for certain types of monitoring, is set by the Russian Government for monitored objects of significant, medium or moderate risk.

[8] In accordance with Article 8 of Federal Law No. 294-FZ dated 26 December 2008. The list of types of entrepreneurial activity in respect of which such notifications are submitted is approved by the regulation on the type of control.

A history of all conducted monitoring measures will be available in the app.

Unified Register of Inspections

The unified register will include information on the objects under monitoring. It is expected that this will significantly simplify the monitoring of inspection plans for monitored entities (at the moment, plans are published on the websites of each separate monitoring body).

The Russian Government authorized inspections of IT companies for the purposes of antitrust monitoring[9]

A moratorium on state monitoring of accredited IT organizations was introduced in 2022.

However, the Resolution of the Russian Government, which came into force in March 2024, lifted the moratorium on antitrust inspections of IT companies in certain cases.

FAS and its territorial bodies are entitled to conduct unscheduled inspections of compliance with antitrust legislation by accredited IT companies for certain violations. According to a report from the Ministry of Digital Development, lifting the moratorium affected only a small number of IT companies, as the innovations primarily aim to prevent the abuse of a dominant position by the companies that meet the following criteria:

- the company has a digital platform;
- the share of transactions between the buyer and seller makes up more than 35% of all transactions in a given market;
- revenue exceeds RUB 2 bln.

At the same time, the moratorium remains in force for all scheduled inspections.

A new risk level in the field of communications

The Russian Government introduced a new level of risk in the field of communications.

Under the new regulation, companies included in the new "high risk" category are subject to an inspection, documentary or on-site, once every two years. This category is now higher than that of "significant risk".

The criteria for inclusion in the new "high risk" category were also introduced. Among them are cases of holding both the telecom operator itself and its officials administratively liable (inter alia, under Articles 13.2.1 and 19.7.10 of the CAO RF), as well as non-compliance with the requirements for communication channels that cross the state border of the Russian Federation.

New indicators of the risk of violation in the field of personal data

In 2024, a list of risk indicators, the identification of which may lead to unscheduled inspections of data controllers, was extended.

At present, unscheduled inspections by Roskomnadzor are also permitted if the regulator identifies at least 2 cases of non-compliance with the rules for recommendatory algorithms published by a data controller on its website within 1 calendar year.

The Ministry of Digital Development has also elaborated a draft order which introduces a new indicator in the cross-border transfer of personal data. An unscheduled inspection may be conducted if Roskomnadzor identifies at least 2 cases of data transfer via foreign software within 1 calendar year without notifying the regulator of such a transfer.

[9] *For a more detailed overview, please refer to our newsletter on the subject via the link.*

Regulation of video games

A fundamentally new regulation for the video games industry

In December 2024, a bill aimed at regulating video game development and distribution was submitted to the Russian Parliament.

The bill includes the following key proposals:

- Introducing definitions of "video game", "game assets", "video game distribution service", "organizer of a video game distribution service", and "video game distributor";
- Defining the obligations of an organizer of a video game distribution service and a video game distributor;
- Mandatory categorization of video games in order to indicate the specifics of their content and conduct examinations of video games to assess their content and conformity with the assigned categories;
- Mandatory identification of video game users by one of the envisaged means;
- Forms of state support for the video game industry, as well as the procedure for exercising control over video game distribution.

One of the most debatable issues of the proposed regulation is the obligation of platforms for video game distribution to identify Russian users - by phone number, via "Gosuslugi" (the Russian state services platform) / Unified Biometric System or another Russian information system. Experts assume that this can have a significant impact on the presence of foreign platforms oand video game distributors on the Russian market.

A bill on limiting advertising in video games

The Russian Parliament is considering a bill that proposes limiting advertising in video games to 15 seconds and displaying 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 age category of the children for which the video game is intended.

Enforcement practices

Class action lawsuit against Sony PlayStation

Users of the Sony PlayStation game platform filed a class action lawsuit against Sony in connection with the suspension of paid transactions in Russia.

The consumers demanded the restoration of access to the software, compensation for moral damages and the recovery of penalties in defence of the rights and legitimate interests of a group of individuals.

During the dispute, more than 300 users joined the class action and the total amount of property claims exceeded RUB 3 billion.

As a result, the court terminated the proceedings of the case (the full text and the reasoning of the decision has not been published).

Contacts

Maria Ostashenko
Partner
Commercial, Intellectual Property,
Data Protection and Cybersecurity

E: mostashenko@alrud.com

Anastasia Petrova
Of Counsel
Data Protection and Cybersecurity

E: apetrova@alrud.com

Ilya Khodakov
Senior Associate
Intellectual Property

E: ikhodakov@alrud.com

Elizaveta Kostyuchenko
Associate
Intellectual Property,
Data Protection and Cybersecurity

E: ekostyuchenko@alrud.com

7 Lesnaya st., 12th fl., Moscow, Russia, 125196
T: +7 495 234 96 92, T: +7 495 926 16 48, info@alrud.com
www.alrud.com

Note: please be aware that all information provided in this letter is based on an analysis of publicly available information as well as our understanding and interpretation of legislation and law enforcement practices. Neither ALRUD Law Firm nor the authors of this letter bear any liability for the consequences of any decisions made in reliance upon this information.

ALRUD