ALRUD

TMT Legal Digest

Key regulatory news in the TMT industry in 2025

Table of Contents

Introduction

Dear Ladies and Gentlemen!

We present to your attention a digest of regulations and practices in the field of technology, media, and communications for 2025.

As is traditional, the past year saw a large number of regulatory initiatives and innovations in the TMT sector.

Significant changes to intellectual property regulations were adopted. The new procedure for calculating compensation for exclusive rights infringements directly reflects provisions previously established in court practice. Increasing the maximum thresholds for «fixed» compensation will lead to higher compensation awards. We expect other intellectual property developments to emerge in 2026, including the launch of a service for calculating average royalty rates. The Russian Government's roadmap, adopted at the end of the year, provides for the creation of this service.

Legislation in the field of personal data processing has also undergone changes. New regulations on depersonalizing personal data have emerged within the framework of the «Gosozero» data. In the coming years, we will see this institution applied and developed in practice. There is also a trend toward tighter control over data storage. This is evident in changes to the wording of localization requirements and a bill currently being considered by the State Duma that would amend the rules for determining foreign jurisdictions with an «adequate» level of personal data protection.

Serious amendments were made to the regulation of information technology and telecommunications. Last year, an active fight against fraud began with the adoption of the first «anti-fraud» regulatory package, which aims to prevent crimes and fraud using modern technologies. These amendments have resulted in significant changes and additional costs for businesses. However, according to regulators, the level of fraud has decreased. The State Duma is currently considering a second similar package, so we can expect the trend of combating fraud to continue in 2026.

Among the most anticipated changes for 2026 is the first bill on comprehensive artificial intelligence (AI) regulation. The draft is expected to address issues such as defining «Russian» AI, the rights, obligations, and responsibilities of companies using AI, labeling AI content, and determining copyrights for AI and its results.

We hope the information in this digest is useful and interesting to you.

Maria Ostashenko
Partner

Commercial, Intellectual Property, Data Protection and Cybersecurity practices

MOstashenko@alrud.com

IP, Media Content, and Advertising

Regulations on compensation for exclusive right infringement clarified[1]

In 2025, amendments were adopted to the Civil Code of the Russian Federation, changing the rules on compensation for infringements of exclusive rights. The upper limit of fixed compensation was increased from RUB 5 to 10 million, while for patent-law objects the minimum threshold was also increased — it now amounts to RUB 50,000.

New provisions were added that detailed the procedure for protecting exclusive rights. The most important changes are as follows:

- establishing a regime of joint and several liability for claims by the rightholder and the exclusive licensee;
- if a person engaged in business activities did not know and should not have known that it had infringed an exclusive right, then the upper limit of compensation will be RUB 500,000;
- introducing rules for calculating compensation in case of multiple infringements;
- infringers who used the same counterfeit physical media will be jointly and severally liable if there is a risk of unjust enrichment of the rightholder;
- no compensation is collected if the method of IP use is necessary to apply other method of use and has no independent economic value;
- courts will be able to change the method of calculating compensation to a fixed amount at their own discretion if they consider that other methods are not applicable.

The amendments took effect on 4 January 2026.

1 *Please see our Newsletter on this topic for more details (available in Russian only)*

Roadmap for IP regulation changes adopted[2]

By 2030, the Government intends to implement a number of measures to improve business conditions in the field of innovation and patents. In particular, it is planned to:

- allow the allocation of shares in exclusive rights;
- create a service for calculating the average rate of royalty for the use of intellectual property objects;
- expand patent protection for solutions implemented in programmable hardware;
- develop mechanisms that prevent the registration of a trademark without the intention to use it;
- ensure that online marketplaces are connected to resources of the Russian IP Office (Rospatent) to prevent the circulation of counterfeit goods;
- expand capabilities of businesses for administrative protection of exclusive rights;
- grant Rospatent the authority to draw up protocols on administrative offenses for infringements of patent rights and illegal use of brand identity;
- grant Rospatent the authority to maintain an anonymized database of royalty amounts.

Intellectual property fees raised

The state fees for registration and renewal of trademarks were raised.

The state fee amount now depends on the number of Nice Classification (NCL) classes, as well as on the specific goods/services listed within a single NCL class. For example:

- The cost of examination and decision-making on the claimed designation will be RUB 13,000, plus RUB 2,500 for each NCL class (if two or more classes are claimed). Moreover, if more than ten items are claimed within one class, each subsequent item is to be paid in the amount of RUB 500.
- Renewal of an exclusive right for one class costs RUB 22,000, for each additional class – RUB 2,000, and additional items within a class, if there are more than ten, cost RUB 500.

The changes are aimed at combating the registration of unused designations and stopping the practice of registering trademarks in relation to all items in the NCL class. From a practical point of view, this will mean that applicants will now take a more careful approach to choosing the names of goods/services within a single NCL class when filing trademark applications.

2 *Please see our Newsletter on this topic for more details (available in Russian only)*

Longer period granted for patenting disclosed inventions

Previously, a patent application could be submitted to Rospatent within six months from the date of the invention disclosure, which did not comply with the provisions of the Paris Convention for the Protection of Industrial Property, where the period was twice as long.

Starting from 23 July 2025, the Civil Code has been aligned with the Convention: now the period for filing a patent application is 12 months from the date of information disclosure.

Law to protect Russian language adopte[3]

On 17 June 2025, the State Duma adopted a law limiting the use of foreign words in public spaces. Starting from 1 March 2026, the Law of the Russian Federation "On Protection of Consumer Rights" (hereinafter, the "Law") will be supplemented with new Article 10.1.

From 1 March 2026, information intended **for public familiarization by consumers** must be displayed in public spaces and communicated to an unspecified group of consumers via signs, pointers, and other means of information display using the **Russian language** or the languages of the republics and peoples of Russia (if provided for by the legislation of the constituent entities of the Russian Federation).

Foreign languages may still be used, but only alongside the Russian language.

The scope of this provision excludes cases of dissemination of advertisements and information about the manufacturer (performer, seller), its operating hours, and the products it sells (Articles 8–10 of the Law).

The restriction also does not apply to cases involving the use of company names, trademarks, and service marks that are in a foreign language – such designations may be used without the need for translation into Russian.

Ban on advertising on undesirable resources[4]

Under the law that came into force on 1 September 2025, advertising is not permitted on the following information resources:

- those belonging to foreign and international organizations deemed undesirable in the Russian Federation;
- those linked to extremist and terrorist organizations;
- other resources access to which is restricted under the information laws of the Russian Federation.

Violating this ban entails fines of up to RUB 500,000 for legal entities.

3 *Please see our Newsletter on this topic for more details (available in Russian only)*

4 *Please see our Newsletter on this topic for more details (available in Russian only)*

According to clarifications issued by the Federal Antimonopoly Service (FAS), advertising placed on "banned" resources before 1 September 2025 will constitute a violation of the ban only if any actions are taken to disseminate the advertising after the said date. Actions that may be deemed as dissemination include:

- references (hyperlinks);
- placing advertisements in pinned posts;
- mentioning offers that remain valid after 1 September 2025;
- reposts;
- using recommendation algorithms.

However, simply failing to remove previously placed advertisements from a resource does not constitute a violation in itself.

Criteria for online advertising defined[5]

The Government of the Russian Federation approved criteria for distinguishing between information and advertising on the Internet. The criteria take effect from 25 July 2025 and apply to content posted on marketplaces and aggregator websites, as well as on Internet search engines and social media platforms.

Information is deemed to be advertising if it:

- draws attention, for example, to a product (work or service), creates or maintains interest, and promotes it in the market;
- is not of a reference, informational, or analytical nature (for example, when such information is not a search engine result, not product information on an official manufacturer's website, not a user's personal "non-advertising" opinion, etc.);
- is not an announcement unrelated to business activity (for example, an announcement about the gratuitous transfer of a product, or reviews with ratings of a product).

At the same time, the following are not considered advertising: search engine results, inclusion in a catalog without violating visual uniformity, information about manufactured products on the manufacturer's resource, recommendation technologies, and personal opinions on personal pages. In addition, reviews and announcements about, for example, the gratuitous transfer of belongings and animals will not be treated as advertising.

Regulations on a fee on revenue from Internet advertising and social advertising labeling come into effect

As of 1 April 2025, the provisions of the Federal Law "On Advertising" (Article 18.2) regarding the introduction of a fee on revenue from Internet advertising targeted at Russian consumers have come into force. Advertising distributors, advertising system controllers, and advertising agencies,

5 *Please see our Newsletter on this topic for more details (available in Russian only)*

as well as advertisers who disseminate advertising in the Russian Federation under contracts with foreign entities are obliged to pay a fee amounting to 3% of quarterly revenue derived from the dissemination of Internet advertising.

In addition, as from 1 March 2025, social Internet advertising must be labeled with an identifier (token) (Article 18.1 of the Federal Law "On Advertising").

Practice

Software distributor's liability when vendor discontinues technical support

In 2021, Inframatika LLC purchased several software (SW) technical support certificates from the supplier MKT LLC with validity periods ranging from 3 to 5 years. In March 2022, the software vendor ceased its business in Russia and blocked access to internal services, as a result of which the certificates can no longer be used.

The purchaser demanded that the supplier refund part of the payment for the unused period of the certificates, as the product had lost its consumer value. The courts of three instances rejected the claimant's demands, ruling that the supplier had fulfilled its obligations at the moment the certificates were transferred and was not liable for actions of the rightholder.

The Supreme Court of the Russian Federation overturned the judgments of the lower courts and sent the case for reconsideration:

- The court pointed out that the certificates have no independent value and are derivative documents confirming the possibility of receiving technical support within the timeframe agreed upon by the parties;
- The claimant is effectively arguing for a reduction in the purchase price of the product (software) for relevant period, since the product ceased to function before the term stipulated in the contract, which is a material characteristic of the product that the claimant relied upon when entering into the contract;
- In the case at hand, the intended outcome of supplying the certificates fit for their intended use within the period agreed upon by the parties has not been achieved, and, consequently, the value of the transferred certificates became disproportionate to the actual possibility of using them;
- The status of an intermediary does not exempt the supplier from its liability towards the purchaser, as under the rules of the Civil Code of the Russian Federation, a debtor is liable for actions of third parties (in this case, the software vendor) tasked with fulfilling the obligations, and the purchaser, in turn, must file claims against the party to the contract, not the vendor.

AI trademark creation argument failed in unfair competition dispute

The claimant filed a lawsuit with the Intellectual Property Rights Court claiming to overturn the resolution of the Federal Antimonopoly Service's Department that had recognized the registration of the BOJOYOID trademark as an act of unfair competition. The applicant argued that the disputed designation was generated by a neural network and was not copied from a competitor company.

However, the court rejected this argument, pointing out the existence of an identical trademark held by a competitor in the People's Republic of China (PRC), which had been known since 2014, as well as the active use of this designation by other sellers in the Russian Federation prior to the claimant's application. The court confirmed that the entrepreneur's actions were not aimed at creating a new brand, but rather at monopolizing the designation that was already well-known in the Russian market.

Moral standards of entertainment broadcasts

An individual entrepreneur filed a claim with the court demanding a refund of more than 1 million of royalties under a license agreement with the respondent for launching an entertainment streaming business. The claimant argued that the materials provided to him (studio selection guidelines, scripts, instructions for conducting streams, a model selection methodology, etc.) did not constitute a unique production secret, as this information was publicly available and lacked commercial value. Consequently, the license agreement was not concluded.

Lower courts dismissed the claim, citing the acceptance certificate confirming that relevant files were transferred to the entrepreneur.

However, the Supreme Court of the Russian Federation overturned these judgments and remanded the case for reconsideration:

- The court indicated that, to resolve the dispute, it is necessary to determine whether the transferred information genuinely constitutes confidential know-how or is in fact common public knowledge for which no fee may be charged;
- The court also raised the need to further verify whether the business model itself complies with the fundamental principles of public order and morality.

Personal Data

Embedded consent for personal data processing is not allowed[6]

Starting from 1 September 2025, consent for the processing of personal data must be drawn up separately from any information or documents that are signed or confirmed by a data subject.

The amendment effectively codifies the existing court practice regarding the recognition of consents embedded in contracts and other documents as unlawfully obtained.

This change aligns with the trend of reducing the use of consents as a legal basis for personal data processing and using other legal bases, in particular, personal data processing for the purposes of entering into and performing a contract, complying with legal requirements, and exercising rights and legitimate interests of data controller or third parties (legitimate interest).

Personal data localization rules tightened[7]

Starting from 1 July 2025, the requirements for personal data localization are in effect in a new version:

> "When collecting personal data, any recording, systematizing, accumulating, storing, updating (refreshing, modifying), or extracting personal data of Russian citizens using databases located outside the Russian Federation is prohibited" (Part 5, Article 8 of the Federal Law "On Personal Data").

Based on the content of the new provision, cross-border data transfers are not restricted, and the condition for their implementation remains the same as before: the primary localization of collected personal data in Russian databases. However, the key aspect for determining the legality of such transfers will be the moment of defining the "completion

6 *Please see our Newsletter on this topic for more details (available in Russian only)*

7 *Please see our Newsletter on this topic for more details*

of personal data collection" – in other words, when a cross-border transfer is considered to be carried out independently of the "personal data collection".

The personal data localization requirements, as before, do not affect the processing of received personal data, i. e. situations when a data controller receives personal data not directly from a data subject. Thus, the new amendments do not in any way restrict the cross-border transfer of such personal data, including their processing in foreign databases.

New requirements and procedures for personal data depersonalization[8]

Personal data depersonalization within the Unified Information Platform of the National Data Management System (EIP NSUD)

Starting from 1 September 2025, data controllers and competent authorities are obliged, upon request from the Ministry of Digital Development to generate and transfer depersonalized personal data for subsequent use in the EIP NSUD. Relevant regulation is prescribed by Article 13.1 of the Federal Law "On Personal Data" and by subordinate acts of the Government of the Russian Federation.

The Government of the Russian Federation set requirements for personal data depersonalization when a data controller receives a request from the Ministry of Digital Development to provide personal data obtained through depersonalization for inclusion in the EIP NSUD.

For most depersonalization methods, the use of specialized software provided by the Ministry of Digital Development free of charge is required or alternative software, if its compliance with the prescribed requirements is confirmed.

Depersonalization according to procedures of the Federal Service for Supervision of Communications, Information Technology, and Mass Media ("Roskomnadzor")

Data controllers, including business companies, are entitled to carry out personal data depersonalization for their own processing purposes, provided they have appropriate legal grounds and comply with the requirements of the new Roskomnadzor order prescribing personal data depersonalization procedures. The order sets out general requirements and procedures for personal data depersonalization applicable to all data controllers. Previously, such requirements applied only to state and municipal authorities.

8 *Please see our Newsletter on this topic for more details (available in Russian only)*

Changes to state control rules in the personal data area[9]

A resolution of the Government of the Russian Federation clarified the risk-based approach to control in the personal data area, in particular:

- **Changes were made to the criteria for classifying control objects into specific risk categories.**

Among other changes, the high severity group A now also includes, for example, personal data processing based on the subject's consent in cases where the law does not provide for the duty to obtain such consent; cross-border transfers to "inadequate" jurisdictions; transfer to third parties of personal data anonymized in accordance with the depersonalization procedures prescribed by Roskomnadzor.

The severity group directly affects the risk category assigned to a data controller as a control object, and, consequently, the frequency of scheduled control measures.

- **The frequency of scheduled control measures was prescribed**

Depending on the assigned risk category, the frequency of scheduled control measures will be determined as follows:

	Scheduled control measures	Mandatory preventive visit
High-risk objects	Once every 2 years	Once a year
Significant-risk objects	Not conducted	Once every 3 years
Medium-risk objects		Once every 5 years
Moderate-risk objects		Once every 6 years
Low-risk objects		Not conducted

- **Mandatory preventive visits**

A mandatory preventive visit is conducted at the initiative of Roskomnadzor for controlled entities and their control objects classified into a specific risk category, taking into account the frequency of mandatory preventive measures:

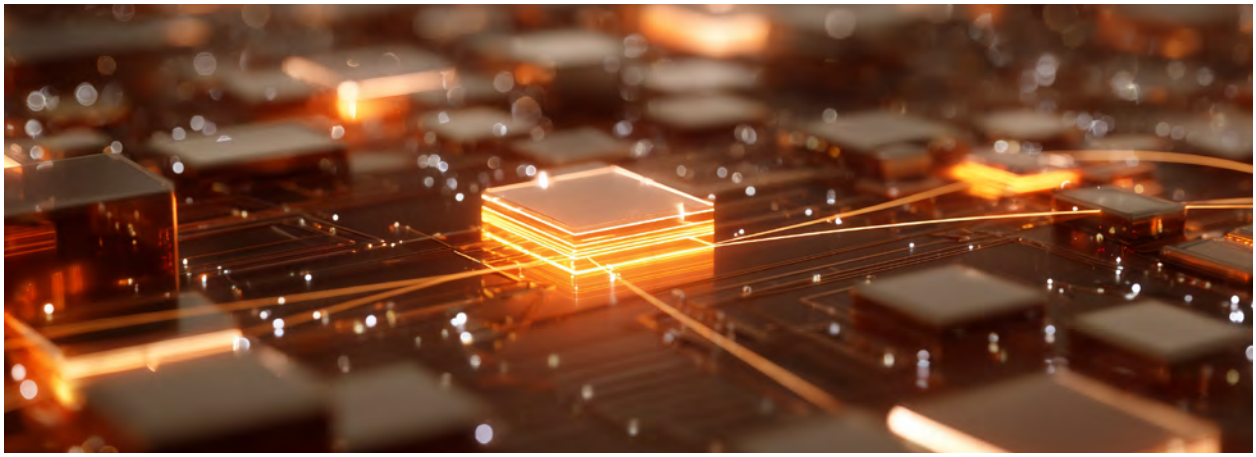
- at least 1 but no more than 2 scheduled control measures per year – for control objects classified as **extremely high risk**;
- 1 scheduled control measure every 2 years or 1 mandatory preventive visit per year – for control objects classified as **high risk**;
- the frequency of mandatory preventive visits, including for specific types of control, is determined by the Government of the Russian Federation – for control objects classified as **significant, medium or moderate risk**.

9 *Please see our Newsletter on this topic for more details (available in Russian only)*

Changes to criteria for recognizing foreign states as providing adequate protection of personal data for Russians

The State Duma has adopted a bill in the first reading tightening the criteria for recognizing foreign states as "adequate" in the context of cross-border transfer of Russian citizens' personal data.

It is proposed that the list of "adequate" foreign states will include jurisdictions whose legal regulation in the field of personal data and measures applied to protect personal data comply with the provisions of Council of Europe Convention No. 108. At present, members of this Convention are automatically included by Roskomnadzor in the relevant list by default.



Courts of general jurisdiction to resume handling personal data violation cases

Starting from 1 January 2026, arbitrazh courts have lost the authority to hear cases involving administrative offences in the field of personal data under Article 13.11 of the Code of Administrative Offences of the Russian Federation. From now on, such cases will again be handled by magistrates' courts of general jurisdiction – relevant amendments were made to Article 23.1 of the Code of Administrative Offences.

Arbitrazh courts handled cases of offences under Article 13.11 of the Code of Administrative Offences of the Russian Federation for a period of 7 months, starting from 30 May 2025. During this time, only a small number of court cases were heard, and for certain offences under Article 13.11 no resolutions were rendered at all.

Returning these cases to magistrates' courts will lead to more efficient case processing due to the distribution of caseload across judicial districts. In this connection, it is also possible that in the future we will see more cases initiated under the provisions of Article 13.11 of the Code of Administrative Offences of the Russian Federation, which were introduced in May 2025 (in particular, cases involving new fines for personal data breaches and cases related to repeated personal data breaches).

Practice

Data breach monitoring ≠ personal data processing

Roskomnadzor filed a claim with the Arbitrazh court seeking to hold DLBI LLC liable under Part 1 of Article 13.11 of the Code of Administrative Offences of the Russian Federation claiming the operation of a data breach monitoring service on the website dlbi.ru and the absence of verified legal grounds for personal data processing.

The company objected, arguing that the website dlbi.ru is of an information and analytical nature, and the functionality of the data breach monitoring service is not available directly on the website. Furthermore, the service only informs users about the potential breach of data based on hashed identifiers, without access to specific personal data and without the ability to identify data subjects.

Roskomnadzor insisted that the respondent's service does not merely provide information about compromised data, but rather uploads a file containing such data, stores it, and processes it in its own database.

The court supported the respondent noting that Roskomnadzor had not proven the elements of an administrative offence. The regulator presented evidence of personal data processing (uploading) by the service, drawing an analogy with the operation of other services and referring to the "established practice", which was qualified by the court as irrelevant and inadmissible evidence.

Roskomnadzor filed an appeal against the court decision, and the case is currently being reviewed by the court of appeals.

Bank was fined for sending personal data via a foreign messenger

Roskomnadzor filed a claim with the court seeking to hold BANK URALSIB PJSC administratively liable for sending a message to a client containing the client's personal data via the foreign messenger WhatsApp.

The respondent objected arguing that the sent message did not include the client's surname, and that the combination of first name, patronymic, and phone number was insufficient for unambiguous identification of the data subject. The bank insisted that no offence had been committed, and as an alternative, requested that the violation be recognized as minor.

The court did not accept the respondent's arguments and found the bank guilty, noting the following:

- The combination of first name, patronymic, and phone number constitutes information containing personal data;
- The use of a messenger included in Roskomnadzor's official list by credit institutions for transmitting such data to a client is explicitly prohibited under Part 8 of Article 10 of the Federal Law "On Information, Information Technologies and Information Protection";

- The bank's guilt is confirmed by the case files, including its own response to the regulator's inquiry, where the fact of using the messenger was not disputed.

As a result, the court imposed a fine of RUB 200,000 on the bank under Article 13.11.2 of the Code of Administrative Offences of the Russian Federation.

Fine for personal data breach affecting 26 million clients

Roskomnadzor filed a claim with the court seeking to hold Pochta Rossii JSC (Russian Post) administratively liable under Part 1 of Article 13.11 of the Code of Administrative Offences of the Russian Federation. The case was triggered by a large-scale data breach, as a result of which the personal data of more than 26 million clients was made publicly available online. As established, the incident was caused by the actions of an internal perpetrator, a fact that the company itself reported to the regulator.

During the proceedings, the court found that the violation was confirmed by the materials of an unscheduled inspection conducted by Roskomnadzor, as well as by a notice from the data controller itself. The court rejected any arguments about the minor nature of the offence stating that the data breach of such scale poses a substantial threat to protected public relations.

The respondent filed an appeal against the court decision, and the case is currently being reviewed by the court of appeals.

Information Technology

Liability for owners of VPN services[10]

A law was adopted that introduces administrative liability for owners of VPN services for failing to comply with the duties to connect to the Federal State Information System (FSIS) for blocked information resources in the Russian Federation and restrict access to them.

New Article 13.52 of the Code of Administrative Offences of the Russian Federation prescribes administrative liability in the form of fines for the following offences:

- Failure to follow the prescribed procedure for interaction with Roskomnadzor: a fine of RUB 80,000–150,000 for officials and RUB 200,000–500,000 for legal entities.
- Failure to comply with Roskomnadzor's requirement to connect to the FSIS for information resources with restricted access: a fine of RUB 80,000–150,000 for officials and RUB 200,000–500,000 for legal entities.
- Violation of the prohibition on failing to restrict access to information resources blocked in the Russian Federation: a fine of RUB 80,000–150,000 for officials and RUB 200,000–500,000 for legal entities.
- Repeated commission of an administrative offence under any of the above offences: a fine of RUB 200,000–300,000 for officials or RUB 800,000–1,000,000 for legal entities

New requirements for protecting critical information infrastructure (CII)

The government amended the rules for categorizing CII facilities. Now, facilities that correspond to the types of information systems included in the lists of standard sector-specific CII facilities are subject to categorization.

10 *Please see our Newsletter on this topic for more details (available in Russian only)*

In addition, the new procedure expands the control powers of the FSTEC (Federal Service for Technical and Export Control). Now, governmental authorities and legal entities are obliged to provide the FSTEC with information about:

- violations of sector-specific peculiarities of categorization;
- breaches of deadlines for categorization work;
- submission of outdated or inaccurate information to the FSTEC;
- identified information systems that correspond to standard CII facilities.

The resolution also introduces other innovations: the list of initial data for categorization was revised; the indicators of significance criteria were updated; the scope of information provided based on the results of assigning a CII facility to one of the significance categories was adjusted (including information about domain names and network addresses).

New fines for hosting providers[11]

Starting from 1 January 2026, new elements of administrative offences for hosting providers shall be in effect under the Code of Administrative Offences of the Russian Federation – a new Article 13.54 of the Code was introduced for this purpose.

Among other provisions, fines are introduced for operating without being included in the register of Roskomnadzor of hosting providers: a fine of RUB 200,000–500,000 for officials and RUB 600,000–1,000,000 for legal entities.

Fines are also provided for violations in the area of interaction with operational investigative bodies and state security bodies of the Russian Federation when developing an action plan for the implementation of technical means and conducting activities of operational investigative bodies.

Furthermore, starting from 1 March 2026, hosting providers may be held liable under Articles 13.43 and 13.44 of the Code of Administrative Offences of the Russian Federation for the following offences:

A) failure to use traffic exchange points, the details of which are included in the register of traffic exchange points for transmission of telecommunication messages;

B) non-compliance with requirements for the stable operation of communication tools to ensure interaction with communication tools of other owners of technological communications networks;

C) failure to fulfill the obligation to use technical and software tools (including communication tools) that function in accordance with the prescribed requirements, as well as the national domain name system, for the purpose of identifying network addresses on the Internet that correspond to domain names.

11 *Please see our Newsletter on this topic for more details (available in Russian only)*

Procedure of transition to Russian software for critical information infrastructure (CII) entities

The Ministry of Digital Development, Communications and Mass Media of the Russian Federation initiated a discussion of amendments aimed at regulating the use of Russian software in the field of critical information infrastructure (CII):

- It is proposed to provide for a procedure and timeframe for the transition of CII entities to the use of Russian software in CII;
- Additionally, it is planned to develop a bill providing for administrative (turnover) fines for CII entities that violate the deadlines for transitioning to Russian software.

It is expected that CII entities will be required to submit a report on completion of the transition by no later than 1 January 2028. The transition deadline may be extended until 1 December 2030, but only in cases specified by the Government.

Generative AI solutions in the Russian software register

The Government developed additional requirements for manufacturers of hardware-software systems (HSS) for generative artificial intelligence, namely:

- ownership of at least one data processing centre located in Russia with an electrical capacity of no less than 10 megawatts;
- the software included in the HSS must ensure data storage of no less than one exabyte and handle machine learning tasks using no fewer than 1,000 graphics processing units (GPU).

In addition, the requirements for technical equipment included in HSS for generative AI were clarified.

Liability for searching for extremist content online[12]

Starting from 1 September 2025, administrative liability will be imposed on individuals for intentionally searching for or accessing extremist materials included in relevant list, or other extremist materials.

The fine for individuals amounts to RUB 3,000–5,000 (Article 13.53 of the Code of Administrative Offences of the Russian Federation).

Fines for violating user authentication and recommendation technology (user profiling) requirements

The State Duma adopted a bill in the first reading that introduces new elements of administrative offences for website owners:

12 *Please see our Newsletter on this topic for more details (available in Russian only)*

- Failure by website owners to comply with user authentication requirements on Russian websites entails liability in the form of an administrative fine: RUB 30,000–50,000 for officials and RUB 500,000–700,000 for legal entities.
- The bill also introduces new elements of administrative offences for non-compliance with the rules for using recommendation technologies.

For example, in the event of failure to inform users about the use of recommendation technologies or the absence of rules for their use on an information resource where recommendation technologies are used, the fine for officials will be from RUB 30,000 to 50,000 and for legal entities – from RUB 500,000 to 700,000.

Repeated violations may result in a fine of RUB 60,000 to 100,000 for officials and RUB 1 million to 1.4 million for legal entities.

Roskomnadzor's powers to manage the Runet expanded

Starting from 1 March 2026, new rules approved by the Government of the Russian Federation will come into force. These rules modernise the regime of centralised management of the public communications network (commonly referred to as the "Runet management rules"). The rules formalise the types of threats to the stability, security and integrity of the Runet's operation, and grant the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) the powers to swiftly counter such threats.

As the body responsible for centralised management of public communications networks, Roskomnadzor is authorised to:

- take organisational and technical measures to restore the functionality of public communications networks;
- change the routing of telecommunication messages;
- ensure backup of communication lines and channels within public communications networks;
- modify the configurations of communications tools within public communications networks;
- deploy information security tools within public communications networks.

Examples of threats to the stability, security, and integrity of the Runet include: access to resources blocked in the Russian Federation; hosting services provided by providers not included in the register of the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) and/or not complying with the information laws of the Russian Federation; and computer attacks on communication tools and networks that could disrupt the Runet's functioning.

The expansion of Roskomnadzor's powers is accompanied by increased regulatory activity in preventing violations in the online environment and restricting access to information resources. According to publicly available data for 2025, Roskomnadzor blocked over 1 million internet resources – a 50% increase compared to the previous year.

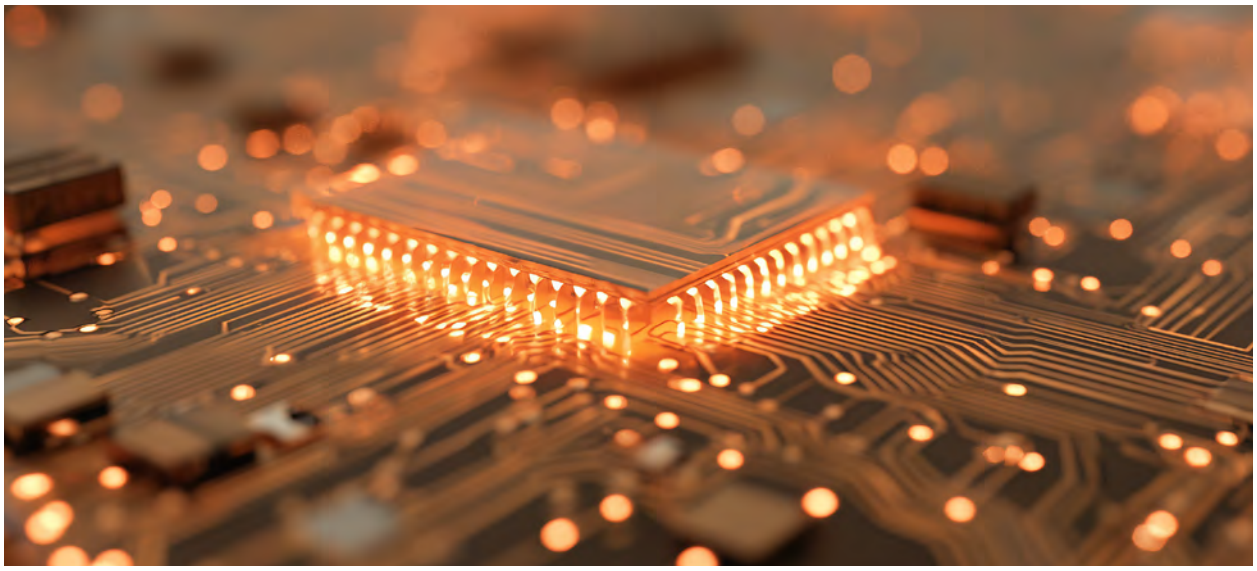
Mandatory labelling of AI-generated video content

The State Duma adopted a bill obliging owners of social networks, video hosting platforms and other websites and web pages (resources) on the Internet to label video materials that have been fully or partially created, altered or processed using AI technologies.

The bill stipulates that such labelling must include:

- A visible notification about the AI-assisted creation of the content, displayed prominently throughout the entire playback of the video material;
- A machine-readable tag in the metadata of the video file, containing information about the use of AI technologies, the date the tag was created, and the identifier of the resource owner. This machine-readable tag must be technically preserved during any operations with the material (copying, downloading, or other use) and cannot be removed without special technical intervention.

Consideration of the bill was included in the spring session agenda. The Legal Department of the State Duma prepared a reply noting the need to amend and clarify the text of the document, due to which the bill may be revised before it is considered.



New data storage periods for information dissemination organizers (IDOs)[13]

Starting from 1 January 2026, data storage periods for IDOs were extended. Now, information about the receipt, transmission, delivery and/or processing of voice data, written text, images, sounds, videos or other electronic user messages, as well as information about these users must be stored for a period of **3 years**.

13 *Please see our Newsletter on this topic for more details*

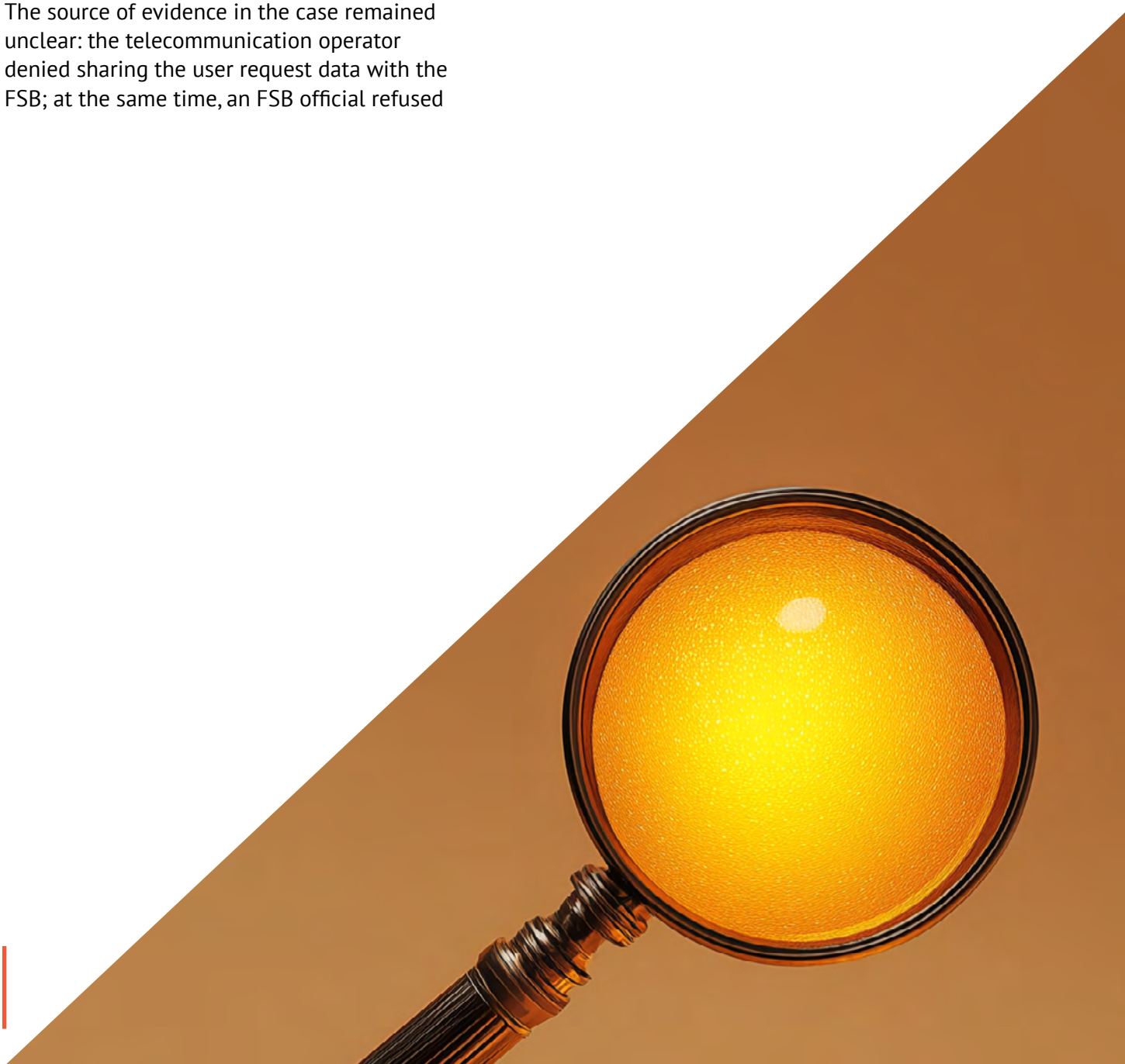
Practice

First practice of fines for searching for knowingly extremist materials

A protocol was drawn up against a citizen under Article 13.53 of the Code of Administrative Offences of the Russian Federation, which came into force on 1 September 2025 and provides for liability for searching for and accessing knowingly extremist materials. According to publicly available information, the citizen claims to have come across the articles by accident and did not intentionally search for extremist materials.

The source of evidence in the case remained unclear: the telecommunication operator denied sharing the user request data with the FSB; at the same time, an FSB official refused to disclose the methods used to intercept traffic in court, referring to state secrets.

Initially, the court returned the protocol drawn up against the citizen. After the protocol was revised and resubmitted to the court, the citizen was fined RUB 3,000.



Telecom

Fight against fraud

In the past year, a number of important measures was adopted to combat fraud in the provision of telecommunications services for both businesses and individuals.

- **Rules for mandatory labelling of business phone calls**

Starting from 1 September 2025, new call identification rules came into effect for all companies and individual entrepreneurs making outgoing calls. According to amendments to the Federal Law "On Communications," when a call comes from an organization, information about the caller will be displayed on the phone screen: the company name, as well as the call category. This innovation became one more measure aimed at protecting people from phone fraud.

To identify calls on the subscriber's end, businesses will need to sign an agreement with the telecommunication operator and provide the latter with information about its identification numbers, company name, commercial designation, a list of numbers used, and relevant business category, as well as the text to be displayed on the subscriber's screen during an incoming call. Unlabelled calls may face enhanced control by telecommunication operators.

- **Cooling-off period**

Starting from 10 November 2025, Russian telecommunication operators introduced a procedure known as the "cooling-off period". This period refers to restrictions on access to the mobile Internet and sending SMS when returning from abroad or if the SIM card is not used for more than 72 hours.

The block is set for 24 hours and can be removed by passing the verification. In addition, voice calls and incoming SMS remain available. The Ministry of Digital Development explained that this measure was introduced at the regulators' request to combat the use of SIM cards for navigating unmanned aerial vehicles.

Users can lift the restrictions before the 24-hour period expires by using a captcha accessible via a link in an SMS from the operator, or by identifying themselves at the operator's call center.

- **Limit on the number of SIM cards**

Starting from 1 November 2025, legislative changes have come into force targeting mobile phone users. These changes aim to strengthen the fight against phone fraud and the illegal distribution of SIM cards.

The new rules set a limit on the number of SIM cards registered to a single individual – no more than 20 SIM cards per person. If a subscriber has more than 20 numbers registered, telecommunication operators are obliged to terminate service under all contracts held by that individual.

New fines for telecommunication operators effective from 1 January 2026

Amendments to the Code of Administrative Offences of the Russian Federation came into force on 1 January 2026 tightening liability for telecommunication operators:

- Specifically, significant fines are introduced for violating service rules: companies will be required to pay between RUB 300,000 and 500,000 for issuing SIM cards in excess of the prescribed limit, as well as for poor verification of users' personal data, the presence of so-called "self-prohibitions," and the lack of information about equipment identifiers in contracts (Article 13.29 of the Code of Administrative Offenses of the Russian Federation).

- In addition, liability in the form of a fine of RUB 300,000 to 500,000 is introduced for legal entities for failure to provide data, violation of deadlines for its provision, as well as for submitting false information to the unified monitoring system GIS KSIM (information system for monitoring the performance of duties by telecommunication operators in the provision of communication services) (Article 13.29.4 of the Code of Administrative Offenses of the Russian Federation).

- Owners of traffic exchange points are required to install technical means of countering threats. Failure to comply with this requirement is punishable by a fine of up to RUB 1 million (Article 13.42 of the Code of Administrative Offenses of the Russian Federation).

- New requirements also apply to owners of communication lines crossing the Russian border: violations related to failure to comply with requirements for such communication lines, failure to notify about compliance with requirements, and connection of lines not registered in the register may result in fines of up to 300,000, and for some violations, suspension of operations for up to 90 days (Article 13.43.1 of the Code of Administrative Offenses of the Russian Federation).

- Additionally, fines of RUB 300,000 to 500,000 are introduced for failure to provide information identifying communication tools and user equipment. In case of a repeated violation, the fine increases: from RUB 600,000 to 1 million (Article 19.7.10 of the Code of Administrative Offenses of the Russian Federation).

Changes to mandatory app pre-installation rules

Starting from 1 September 2025, rules for pre-installing software on new devices have changed: The national messenger MAX, which has replaced VK Messenger on the list of so-called "essential software," is now mandatory on smartphones and tablets running Android, iOS, and HarmonyOS. Additionally, the requirements for the RuStore app store were expanded: its pre-installation is now mandatory for iOS and HyperOS devices.

Starting from 1 January 2026, the list of "mandatory software" for Smart TVs was supplemented with the Lime HD TV app.

At the same time, the already familiar set of "essential applications," including Gosuslugi, voice assistants, and antiviruses, will remain the same.

New regulation of data processing centres (DPCs)

On 15 July 2025, a law was adopted introducing regulation of the data processing centers (DPC) industry. Amendments to the Federal Law "On Communications" define the concept of DPCs, permit their construction under concession agreements and within the framework of public-private partnerships (PPPs), and also provide for the creation of a separate register of DPCs. In pursuance of the law, the Government of the Russian Federation adopted a resolution prescribing the procedure for the development and operation of the DPC Register, requirements for DPCs, their owners and operators. The registry will be maintained by the Ministry of Digital Development.

The law also prohibits the placement of cryptocurrency mining infrastructure and the operation of cryptocurrency mining activities in DPCs located in Russia and included in relevant register.

These regulatory changes will come into force on 1 March 2026.

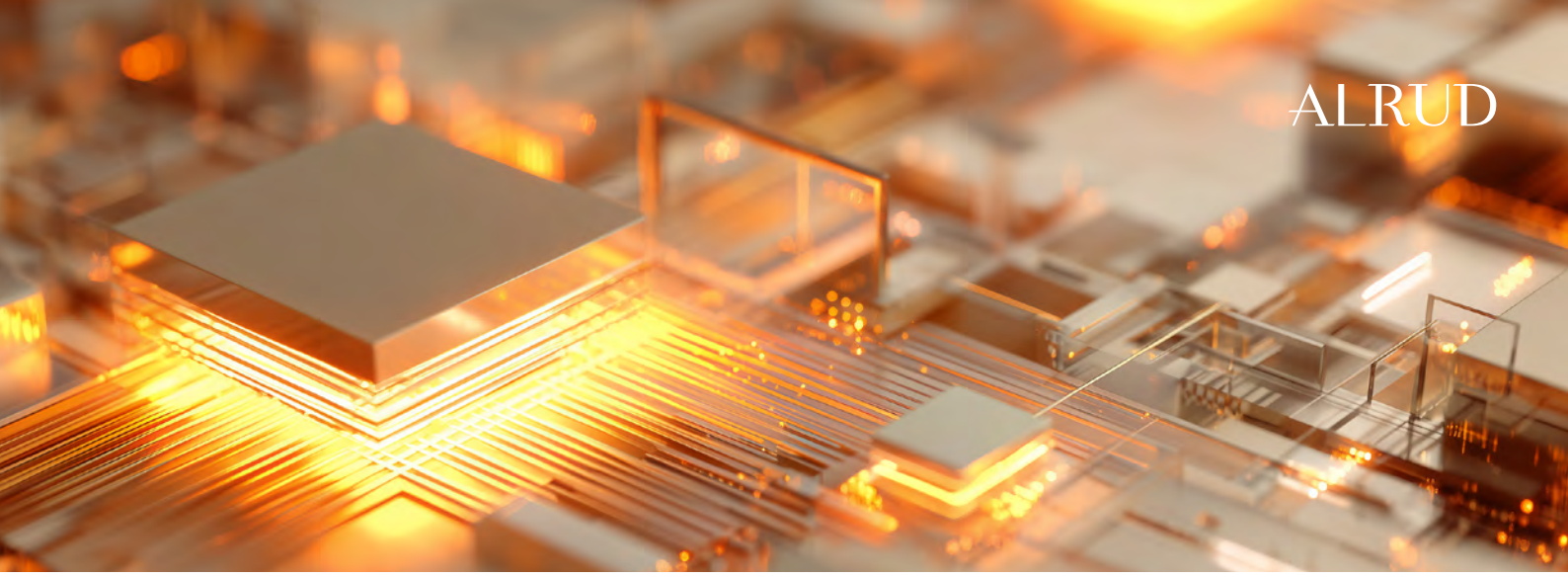
Practice

Ban on a voice-changing app

The court, at the request of the city's prosecutor's office, considered a case regarding the recognition of prohibited information on the page of the Voice Changer Prank Call app in the App Store. This app is intended to change a user's voice during phone calls.

The prosecutor's office argued that information about such a service violates the telecommunication and anti-terrorism laws, as it enables malicious actors to make calls while concealing their identity. The court agreed with these arguments finding that the ability to distort one's voice could indeed facilitate criminal activity.

In deciding to ban the app's distribution, the court stated that the software's functionality, which distorts the caller's voice, hinders caller identification and creates the impression that extremist and terrorist crimes are likely to be committed.



E-commerce

Law on digital platforms adopted[14]

The President of the Russian Federation signed Federal Law No. 289-FZ "On Certain Issues of Regulating Platform Economy in the Russian Federation" (the "**Platform Economy Law**"), which will come into force on 1 October 2026.

The law is intended to comprehensively regulate relations between digital platform owners, their partners (sellers of products and service providers), and end users (buyers and customers), covering popular marketplaces such as Ozon, Wildberries, Yandex Market, as well as taxi and courier service aggregators.

The law sets a unified conceptual framework in the area of platform economics, the key one being the concept of an "intermediary digital platform," which:

- ensures interaction between the operator, partners and users for the purpose of entering into civil law contracts;
- provides technical capabilities for placing orders and/or cards for products, works, services, concluding transactions, and making payments for products, works or services by the user in favor of the partner;
- is included in the Register of Intermediary Digital Platforms.

The key innovation is the mandatory conclusion of a contract between platform operators and their partners, with a clear definition of requirements for partners, liability measures, payment procedures, etc., which the operator is obliged to publish, indicating the period of its validity, and also provide to the partner and the owner of the pickup point.

The law also prescribes rules for unilateral changes to the contract requiring advance notification of partners or owners of pickup points about planned changes. Particular attention is paid to the requirements for the placement of product (work or service) cards.

In accordance with the law, platform operators are required to provide equal access to services for all partners, ensure transparent search results, and establish a pre-trial complaint review system. The law also prescribes special rules for working with partners-individuals emphasizing their independence and the absence of an employment relationship with the platform.

14 *See a detailed overview of Federal Law No. 289-FZ in our information material*

Intermediary platforms: new rules for interaction with the Federal Tax Service (FTS)

The Ministry of Finance developed a draft Government Resolution on the procedures and requirements for information exchange between operators of intermediary digital platforms and tax authorities.

The document implements the provisions of the Platform Economy Law and is intended to strengthen the FTS's control functions in the digital environment setting the following key rules:

- data exchange must be conducted exclusively in electronic form via platforms accessible to the FTS;
- platforms are obliged to send information about the risks of the partner (seller) and transfer of their explanations to the FTS;
- FTS requirements must be posted in the partner's personal account.

For marketplace operators, aggregators, delivery services, and other platforms, this means the establishment of new administrative duties for automated data exchange with the FTS. Platforms will need to integrate with tax service systems and develop internal procedures to identify risky partners in due time.

If the draft resolution is adopted, the new rules will come into force on 1 October 2026.

Regulation of instalment services

A new law was adopted amending several legislative acts to tighten rules for instalment service operators.

Starting from 1 April 2026:

- merchants will be prohibited from setting different prices for the same product depending on whether the consumer buys it directly or via an instalment service;
- instalment service operators will be included in the list of organizations regulated by the Central Bank of Russia;
- information about the conclusion and performance of instalment agreements will be reported to credit bureaus.

ДThese changes aim to protect consumers and bring these platforms out of the "grey" regulatory zone.

Amendments to the Law on Protection of Consumer Rights to combat "consumer extremism"

A law was adopted introducing changes to protect businesses from unfair consumer actions. The main provisions aim to limit excessive financial claims and abuses by buyers.

The law introduces the following key changes from 1 February 2026:

- The following circumstances will serve as grounds for refusal to collect a fine in the amount of 50% of the claim amount:
  - the consumer's claim is not satisfied due to the consumer's own fault;
  - the violation is caused by supply chain disruptions;
  - the parties entered into a mediation agreement before litigatio.
- The amount of penalty for delayed satisfaction of consumer claims may not exceed the price paid for the product.
- Consumers are prohibited from transferring the right to claim fines to third parties before a court decision enters into legal force. Such transactions will be deemed void.
- When returning a technically complex product of improper quality, the consumer will be able to claim the difference between the purchase price and the market price of a like product (taking into account its previous use) at the time of the request.

The Government of the Russian Federation is also granted the right to prescribe special rules for fulfilling obligations and applying fines for certain product categories, which may mitigate the liability of sellers.

Practice:

Using multiple photos constitutes multiple copyright infringements

The rightholder of 15 photos, individual entrepreneur Milovanov, filed a lawsuit against a seller who had posted the disputed photos in the product card. The claimant initially sought compensation for all 15 infringements.

The court of the first instance found that placing all the photos in one product card pursues a single economic purpose (sale of one product) and constitutes a single violation. The court of appeals re-qualified the respondent's actions stating that 15 different works were used, meaning that 15 separate infringements were committed. The court reduced the claimed compensation amount.

The Intellectual Property Rights Court dismissed the respondent's appeal claim upholding the findings of the court of appeals:

- The concept of "unity of intent", which allows multiple actions to be qualified as a single infringement, applies only to repeated use of the same object.
- In this case, 15 distinct objects (photos) were used. Even if they were posted together to promote one product, this constitutes multiple infringements, one for each rights-protected object.
- The court distinguished between the concepts of "single economic purpose," meaning the use of one object in different ways, and "unity of intent," meaning the multiple use of one object in one way.

Business is liable for actions of duplicate websites

A consumer contacted a service company via an Internet website and handed over an all-in-one computer for repair to a courier who presented himself as an employee of the service center. After multiple delays in the repair process, the equipment was disposed of without her consent.

Subsequently, the claimant filed a claim against the respondent for consumer rights protection, recovery of funds, and compensation for non-pecuniary damage. In response, the respondent filed a counterclaim seeking to have the service agreement declared invalid, as, in reality, it had never entered into a contract with the claimant: the website the consumer had used was a duplicate website.

The lower courts dismissed the claimant's claim ruling that the service agreement was void. The courts concluded that the agreement was signed on behalf of the Respondent by an unauthorized person, the seal imprints on it did not match the samples of the Respondent's seals, and therefore there was no contractual relationship between the parties.

The Civil Cases Judicial Panel of the Supreme Court of the Russian Federation overturned the lower courts' decisions and stated the following:

- In this case, the courier's authority as the respondent's representative arose from the circumstances. The claimant, having found the respondent's website and agreed on the terms, had no reason to doubt that she was handing the all-in-one computer to the Respondent for repair via the courier.

- Since the offer of services was made on behalf of the Respondent, the duty of refuting the ownership of the website and telephone number, as well as proving the discrepancy between the address, Principal State Registration Number (OGRN) and Taxpayer Identification Number (INN) of the service center and the details of the respondent, was to be imposed on the Respondent. The lower courts had wrongly shifted this duty of proof onto the Claimant, who lacked relevant information and means to detect a fraudulent service offer made in the Respondent's name.

- As a participant in the professional market, the Respondent is obliged to monitor offers of services made in its name on the Internet.

The Supreme Court of the Russian Federation remanded the case for a new trial in the court of the first instance. No decision has yet been issued in the new round.

The authors of the Digest

Maria Ostashenko

Partner

Commercial, Intellectual Property, Data Protection and Cybersecurity practices

mostashenko@alrud.com

Elizaveta Kostyuchenko

Senior Associate

Intellectual Property, Data Protection and Cybersecurity practices

ekostyuchenko@alrud.com

Yuliya Agafonova

Junior associate

Intellectual Property practice

yagafonova@alrud.com

Darya Kashkarova

Junior associate

Commercial law practice

dkashkarova@alrud.com

Dmitry Zimin

Trainee

Intellectual Property practice

dzimin@alrud.com

Арина Ломакина

Trainee

Intellectual Property practice

alomakina@alrud.com

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

ALRUD