# The second package of measures against cyber fraud

*FAO the management and staff of telecom operators, credit institutions, and representatives of the business community, as well as individuals wishing to protect themselves from fraudsters.*

---

**Pepeliaev Group advises that the Russian Ministry of Digital Development has drawn up a new draft law aimed at combating cyber fraud (the "Draft Law")[1].**

As a reminder, on 1 April 2025, Law No. 41-FZ[2] was adopted, which contains the first package of measures in the fight against cyber fraud[3].

The current Draft Law has been prepared a view to further improving the regulation for combating cyber fraud, developing the mechanisms established by Law No. 41-FZ, and introducing additional measures of legal protection.

The new Draft Law is planned to enter into force on 1 March 2026, except for certain provisions.

Additionally, two accompanying draft laws have been prepared, which are aimed at introducing new types of offences in the Russian Code of Administrative Offences (the "Code of Administrative Offences") and the Russian Criminal Code (the "Criminal Code"), as well as toughening liability for a number of already existing provisions in the field of IT[4].

The entry into force of the amendments to the Code of Administrative Offences is also planned for 1 March 2026. The Draft Law does not specify the date when amendments to the Criminal Code and Russian Criminal Procedure Code will take effect. Therefore, the changes will come into effect 10 days after they were officially published.

## The state information system (SIS) for combating offences

### Expansion of information stored in the SIS

---

[1] The Draft Law "On amending certain legislative instruments of the Russian Federation (to the extent of combating offences committed using information and communication technologies)" // Draft ID: 159652

[2] Federal Law No. 41-FZ dated 1 April 2025, "On creating a state information system to combat offenses committed using information and communication technologies and on amending certain legislative instruments of the Russian Federation"

[3] For more details, see: https://www.pgplaw.ru/analytics-and-brochures/alerts/vstupil-v-silu-zakon-o-protivodeystvii-kibermoshennichestvu/

[4] The Draft Law "On amending the Criminal Code of the Russian Federation and the Criminal Procedure Code of the Russian Federation" // Draft ID: 159661

Under the current version of Law No. 41-FZ, information is stored about individuals who have committed illegal actions and about subscriber numbers used to commit such illegal actions.

The Draft Law proposes to reform the SIS by creating a registry of subscriber numbers where information will be stored about fraudulent individuals, their subscriber numbers, the subscriber numbers of victims of fraud, as well as recordings of conversations with signs of illegal actions.

This part of the amendments is planned to come into force from 1 January 2026.

## Measures to combat fraud relating to telecommunications operators' activities

### Establishing databases for identifiers of user equipment (end-user devices)

The Draft Law proposes that two databases of IMEI identifiers for mobile devices will be created:

1. an IMEI database formed by telecommunications operators when registering a subscriber device to provide communication services;

2. a central IMEI database under the supervision of the Russian Ministry of Digital Development, containing permissions or restrictions on using a device. It is assumed that this database will be formed using data sourced from telecommunications operator databases. The Ministry of Digital Development will determine the procedure for how they will interact. The Russian Government will establish the requirements for the central database.

Telecommunications operators will provide services only when a user is using a "permitted" device. If a device's IMEI is classified as "not permitted", telecommunications operators are obligated to suspend the provision of services. Devices deemed "not permitted" for use in the communication network include those with IMEIs:

- with respect to which a decision to ban them has been made;
- that do not meet the statutory requirements.

The Russian Ministry of Digital Development will determine the criteria for IMEI and the procedures to classify them as either permitted or not permitted.

In addition, it is not permitted to alter a device's IMEI through software. Such actions may be classified under article 13.6 of the Code of Administrative Offences (Unauthorised use of communication devices not meeting established requirements), potentially leading to a penalty including confiscation of the device and a fine of up to RUB 5,000 for individuals, RUB 30,000 rubles for a company’s officers, and RUB 300,000 for legal entities.

Furthermore, it is proposed to establish that concealing information about a user of communication services (i.e., altering the IMEI) be considered a qualifying feature of the bodies of two offences under articles 158(3) and 159(3) of the Criminal Code (theft and fraud). This could result in a penalty of up to six years' imprisonment.

These changes are intended to come into force starting from 1 March 2027.

**New duties for telecommunications operators in interacting with the SIS**

Telecom operators are required to independently identify subscriber numbers showing signs of carrying out illegal activities and to provide relevant information to the SIS:

- information about the subscriber number from which illegal actions are conducted;
- information about the subscriber number of the victim;
- information about the location of the device.

The Russian Ministry of Digital Development will establish the procedure for identifying signs of illegal activities and will agree it with the Central Bank of Russia.

Upon receiving instructions from the SIS, telecom operators must suspend services to a subscriber for 24 hours.

Additionally, further to a request from the Ministry of Digital Development, operators are required to provide the SIS with recordings of telephone conversations that exhibit signs of illegal activities.

**Marking calls**

The Draft Law clarifies the rules that make the marking of calls from individual entrepreneurs and legal entities obligatory.

The current text of article 46 (9.1) of the Law on Telecommunications imposes duties to this effect solely on telecom operators, and there is no direct prohibition on unmarked calls in the legislation. Those involved in business activity are not subject to requirements for call marking.

The draft proposes adding a condition to article 46 (9.1) that calls can only be made after information about the caller is transmitted to the receiving party's telecom operator. Additionally, article 45 is to introduce a provision requiring that telephone calls from individual entrepreneurs or legal entities are permitted to be initiated only on condition of the mandatory transmission of caller information to the recipient's device.

**Pepeliaev Group's comment**

The requirement for call marking has sparked significant discussions since the first measures to combat fraud were adopted.

Firstly, the obligation provided for under the Law on Telecommunications for telecom operators to mark calls does not correspond with an obligation for legal entities and individual entrepreneurs to inform telecom operators or transmit to them the necessary information for marking. This has led operators to incentivise businesses to sign contracts with them in various ways, such as automatically withholding the marking cost to corporate subscribers or blocking calls classified as carried out on a mass level. Given that no criteria for a mass level of calls currently exist, each telecom operator has developed its own approach.

In addition, telecom operators are taking a cautious approach out of concern for non-compliance with the Telecommunications Law and have proposed that businesses implement call marking from all corporate numbers, even those used solely for internal communication. This requirement, however, contradicts the Russian Government's Resolution No. 1300 dated 28 August 2025, which specifies that only a list of subscriber numbers from which calls will be made needs to be transmitted to operators (i.e., not all subscriber numbers).

There is no specific provision at present in the Code of Administrative Offences that directly provides for telecom operators to be liable for not complying with call marking requirements. However, there remains a risk that non-compliance could lead to a severe penalty being applied, such as a licence being revoked for a breach of its conditions, since failure to adhere to provisions of the Law on Telecommunications, including call marking, is classed as a breach.

Additionally, the likelihood cannot be ruled out that calls without proper marking could be classified as mass calls without subscriber consent under article 14.3(4.1) of the Code of Administrative Offences, which pertains to "Violation of the requirements for advertising distributed via electronic communications networks". Under this article, any individual or entity could face liability. We remind you that, under article 14.3(4.1) of the Code of Administrative Offences, fines for individual entrepreneurs range from RUB 20,000 to RUB 100,000, while for organisations the fines range from RUB 300,000 to RUB 1 million.

In such circumstances, telecommunications operators are blocking calls they have classified as mass calls. This may include legitimate business communications, such as those originating from a company's call centre, for example handling customers' complaints.

## A self-imposed ban on foreign calls

It is proposed to give subscribers the opportunity to set a self-imposed ban on receiving calls from foreign numbers. Anton Gorelkin, a member of the State Duma's Committee on Information Policy, notes that this measure is similar to the self-imposed ban on loans and its implementation will be possible through the 'Gosuslugi' public services portal[5].

## Liability of telecom operators

1. Liability is established for telecom operators if they do not fulfil their duties during interactions with the SIS.

As stated above, telecom operators will have new duties, including identifying signs of violations using subscriber numbers, sending such information to the SIS, and suspending telecom services upon if it receives an instruction from the SIS. If an operator does not properly meet its obligations and this results in a theft of funds from a subscriber's mobile account, the telecom operator is required to compensate the subscriber for the damage incurred.

2. It is proposed to introduce new offences in both the Code of Administrative Offences and Criminal Code for telecom operators and their officers.

2.1. Code of Administrative Offences:

- not complying with the requirements regarding the number of SIM cards used by one individual;
- providing telecommunications services to foreign nationals or stateless individuals using devices whose IMEI numbers are not included in the service contract;
- violating the procedure for submitting information to the state information system for operators to perform their obligations when providing telecom services, or violating statutory requirements regarding the system's use.

2.2. In cases of a repeated violation concerning the inclusion of IMEI in service contracts, if such violations result in significant damage, the officers of telecom operators will face criminal liability.

## Other measures to combat cyber fraud in relation to telecom operators' activities

1. New requirements for virtual automatic telephone stations (VATS)

The Draft Law introduces new regulations governing the operation of a VATS.

When using network addresses for interaction with a VATS, these addresses must align with Russia's national domain name system. Additionally, when

[5] https://realnoevremya.ru/news/353731-gosduma-predlozhit-rossiyanam-samozapret-na-inostrannye-zvonki

engaging services from hosting providers, they must be included in the official provider hosting registry maintained by the telecoms regulator Roskomnadzor. Similar requirements are proposed to be established under article 10.2-1 of the Law on Protecting Information ("Special features of regulating the activities of hosting providers").

2. Expanded obligations for telecom operators

The proposed law increases the volume of information that telecom operators must provide to the monitoring system.

Operators will be required to supply data on subscriber numbers used in subscriber traffic pass-through terminals (SIM boxes), specifying the type of equipment, radio device identifiers, installation addresses, and the purposes of usage. The monitoring system must also receive information regarding VATS subscriber numbers and the network addresses used for providing communication services.

## Measures to combat fraud involving activity of banking institutions

The Draft Law is proposing to amend the Federal Law "On the national payment system" in terms of regulating activities of banking institutions or operators of transfers of monetary funds (OTMF).

### New powers and requirements for an OTMF: strengthening control over transfers without a client's consent

1. Subscriber numbers

The provisions of the Draft Law oblige an OTMF to obtain information as follows from the SIS when verifying that transfers of funds by clients are voluntary:

- about subscriber numbers used to carry out actions exhibiting illegal characteristics;
- about subscriber numbers receiving such actions (telephone calls or short messages), which display illegal traits.

If information about potential illegal actions associated with client subscriber numbers exists, an OTMF will have the right to suspend the use of electronic means of payment by such clients during the period when the number is listed in the unified registry of numbers used for illegal activities. The procedure for suspension must be stipulated in the agreement with the client.

At the same time, an OTMF is required to independently forward information about such subscriber numbers to the SIS. The composition of this information and the procedure for forwarding it will be established by the Central Bank of Russia in coordination with the Russian Ministry of Digital Development.

2. Malicious software

Operators of Payment Systems (OPS) must use information about the impact of malicious code on software that clients apply to transfer for monetary funds.

Upon detecting the impact of malicious code, OPS are obliged to refuse to carry out a customer's instruction or to complete the transaction (transfer). The client is immediately notified of the reasons for refusal. In such cases, the client or their representative may complete the transfer only by personally visiting the OPS.

Additionally, OPS must ensure that their software (including mobile apps and websites) used by clients is protected from malicious code and must identify instances of such attacks before any funds are deducted, including operations involving payment cards, electronic money transfers, or through the Fast Payments System.

The contract with the client must contain provisions allowing the client to either agree to or opt-out of such protective measures.

**Liability of payment system operators for improperly verifying voluntary transfers**

According to the Draft Law, an OPS that executes a transfer or operation despite having received information about illegal actions risks facing negative financial consequences. The OPS will be obliged to fully reimburse the transfer amount to a client who is an individual if there exists a resolution initiating a criminal case relating to the embezzlement of funds. The reimbursement must be completed no later than 30 days from when the client's communication is received.

**Limitation on the number of payment cards**

The Draft Law sets limitations on issuing payment cards to a single client who is an individual:

- no more than 5 payment cards can be issued by a single OPS.
- all Russian credit institutions and foreign banks operating in Russia can collectively issue, in total, no more than 10 payment cards to an individual.

The board of directors of the Central Bank of Russia can increase these limits.

**Pepeliaev Group's comment**

The draft law is silent on what will happen to payment cards held by clients who have more than five payment cards with a single OPS or more than ten across different OPS as at 1 March 2026. We believe that the restriction will apply only to the issuance of payment cards after the law comes into force.

## Anti-fraud measures in the field of information security

### New obligations for owners of online platforms interacting with the SIS

The Draft Law introduces an obligation for:

- organisers of instant messaging exchange services,
- hosting providers,
- owners of social networks, and
- owners of advertising placement services

to take measures aimed at preventing and stopping violations of the law, as well as transmitting to the SIS information about signs of illegal actions having been committed.

The Russian Government will determine the list of the above measures and the composition of the data to be transmitted.

### The list has been expanded of information to which access is restricted

The Draft Law proposes to expand the list of information that is distributed in violation of the law and that is subject to restriction. Specifically, this includes:

- information that is intended for unauthorised interference in software or spreading malicious software;
- information designed to mislead. This category covers messages that are presented as authentic but are capable of causing financial harm to the user or damage to their property. The Russian Government will establish detailed criteria for what constitutes such information.

## Other measures to combat fraud

### Integrating the management of personal data with 'Gosuslugi'

The Draft Law provides that subjects of personal data (PD) have an opportunity to manage their PD through the public services portal 'Gosuslugi' service. A PD subject will have the right to:

- give consent to the processing of PD through 'Gosuslugi' (the regulator Roskomnadzor will draw up a standard form for this);
- revoke his/her consent to the processing of PD through 'Gosuslugi';
- receive through 'Gosuslugi' information confirming the fact that PD is being processed;

- complain about the actions of PD operators in a case where the rights and freedoms of the PD subject are have been infringed.

At the same time, it is planned to oblige operators to transfer information to 'Gosuslugi' about the facts of PD being processed when they collect PD. Operators who have carried out the processing of PD before the rule came into force (before 1 March 2028) are obliged to submit such data to 'Gosuslugi'.

This part of the amendments is planned to come into force on 1 March 2028.

**Pepeliaev Group's comment**

The proposed changes raise questions from the standpoint of how they will be implemented in practical terms.

Firstly, the requirement to transmit information about each fact of PD being processed at the time it is collected seems excessive. A PD operator may collect PD from the same subject on several occasions. It would be sufficient to limit transmission to information that the subject's consent has been obtained, as consent determines that processing is lawful.

Secondly, transferring all information about PD being processed upon its collection before the rule enters into force is difficult to achieve. A PD operator is not required to record facts that relate to collecting PD (unlike obtaining consent to processing), meaning that it cannot transmit the corresponding data.

## Certificates of safety from the national certification centre (NCC)

Among the planned changes, it is proposed to create a new category of digital certificates, namely 'NCC Safety Certificates'. These will be issued via the SIS.

An NCC Safety Certificate will be used for:

- ensuring robust and secure interaction with:
    - an information system;
    - a website in the internet;
- authenticating:
    - an information system;
    - a website;
    - a participant in electronic interaction within a corporate system;

- verifying:
    - ownership of an information system or a website;
    - the integrity and authenticity of the origin of software for electronic computers;
    - arranging a secure interaction with participants in an electronic exchange within corporate information systems.

For government agencies, ensuring the possibility of interaction through NCC safety certificates will be mandatory. In addition, the Russian Government has the right to extend this requirement to other entities or persons.

This part of the amendments is scheduled to come into effect on 1 July 2026.

**A list has been established of the ways to restore access to a 'Gosuslugi' account**

According to the proposed amendments, if access is restricted to an individual's account in 'Gosuslugi' because the fact of unauthorised access has been detected, access can be restored via the following methods:

- using biometric authentication;
- through a bank's official website or a banking application;
- via the messenger service 'Max';
- by appearing in person at a 'Gosuslugi' center.

**Restrictions on the state registration of rights to real estate**

The Draft Law provides for amendments according to which the deadlines for carrying out state cadastral record keeping and the state registration of rights can be extended up to 20 days in a case where there are signs of unequal mutual performance. The state registration of rights to real estate is suspended if the transaction contains features of a suspicious transaction that have been established by the Russian Government.

## What to think about and what to do

Telecom operators should prepare for the implementation of an IMEI database, ensure that it is integrated with the central database, and integrate with the SIS taking the planned changes into account. They should also inform their employees that liability has been strengthened for offences in the field of telecommunications.

It is important for credit institutions to review their systems for monitoring transfers and to implement mechanisms to verify whether operations are voluntary based on data from the SIS.

Personal data operators need to collect information regarding instances of personal data being processed and be ready to transmit such information to 'Gosuslugi'.

### Help from your adviser

The lawyers of Pepeliaev Group have extensive experience in advising telecom operators, credit institutions, and other organisations on legal matters.

We are ready to offer comprehensive legal support to organisations in the following areas:

- determining the risks in the event that the Draft Law is adopted;
- preparing legal positions on controversial issues that arise as a consequence of the Draft Law;
- drawing up internal regulations and procedures that are necessary to comply with the requirements that are planned to be introduced;
- representing businesses in disputes with government agencies.

---

## Contact details


**Natalia Kovalenko**
Partner

Tel: +7 (495) 767 00 07
n.kovalenko@pgplaw.ru

**Lidia Gorshkova**
Partner

Tel: +7 (495) 767 00 07
l.gorshkova@pgplaw.ru