大成 DENTONS

IP, IT and Telecommunications

Legislative developments: 2010-2020.

Major Russian legislation changes for 2020


authorities
special
set
patent
within
federation
devices
government
citizens
programs
procedure
changes
certain
must
new
users
elr
used
year
ip
equipment
decision
system
fines
rules
personal
russian
organizer
inspections
identification
resource
request
competent
distance
digital
data
selling
legal
consumer
protection
requirements
rf
communications
access
activity
owners
advertising
inspection
notification
dfas
made
processing
revenue
state
assets
only
regulation
rub
resolution
restrict
amendments
electronic
industrial
network
central
securities
application
subject
law
federal
business
employee
information
operator
technologies
public
networks
rights
social
article
andor
documents
example
messages
decree
also
owner
consent
dissemination
telecommunications
number
list
regulations
services
roscomnadzor
how
software
eurasian
concept
financial

Contents

LEGISLATIVE DEVELOPMENTS: 2010-2020

Total regulations adopted 2010–2020*

Federal laws and federal constitutional laws:

5 390

Published presidential decrees and orders:

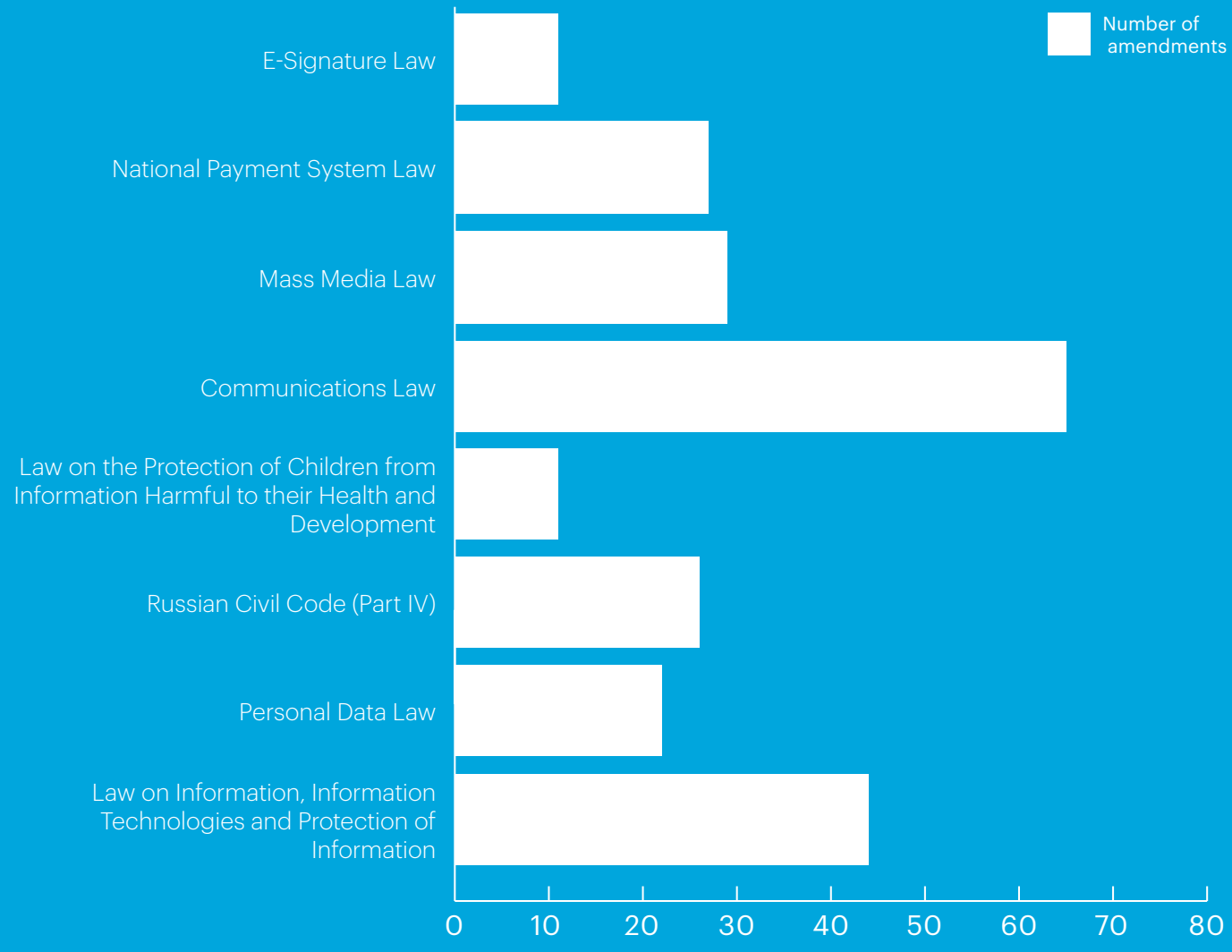
10 455

Published government resolutions and orders:

41 744

* Data from the Official online legal information portal

Number of amendments to key IP, information and communications laws 2010–2020



The period from 2010 to 2020 can rightly be called the decade of the development of information technology laws. We have identified three key legislative trends that we believe will continue to be relevant in the nearest future.

Information sovereignty

In the early 2010s, online activity wasn't considered an area in need of special regulation. 2012 could be called a tipping point when the first reasons and grounds for blocking information resources appeared. Increasing control over information disseminated on the Internet resulted in the appearance of new participants in information relationships. They were given a wide range of responsibilities, from content moderation to user identification. Some were even made responsible for complying with foreign control requirements.

The trend of increasing control over disseminated information is characterized by the adoption of three legislative acts: (1) the so-called Yarovaya law that required telecoms operators and information dissemination organizers to store certain data about users' communication for a long time, (2) the "sovereign Internet" law which will allow for direct control over information space in a number of cases, and (3) the law on the security of critical information infrastructure.

Another serious change in maintaining Russia's information sovereignty was the introduction of limits on storing certain data on foreign servers. The personal data laws underwent amendments for "localization" of Russian citizens' personal data in Russia. This step was further developed in the Yarovaya law. Considering that the idea of localizing certain categories of data in Russia is enshrined as a principle in the Strategy for the Development of an Information Society in the Russian Federation for 2017–2030[1] (the "**Strategy**"), limits on where one or another type of data are stored will likely be introduced to the laws in future.

Another important trend of the decade is the detailing of administrative offenses and the considerable increase in fines for violating information laws.

Focus on import substitution

In the mid-2010s, Russia began to focus on import substitution in IT. A number of amendments were passed to limit the use of foreign software and promote the use of Russian programs. At first those steps mainly had to do with restricting access for foreign software to participate in state and municipal procurement. A unified register of Russian computer software and databases was created to keep track of Russian programs. Referred to briefly as the Russian software register, in 2015 it counted more than 2,500 programs and databases, with around 9,000 by the end of 2020. The import substitution requirement has also been extended to embedded software that is provided to consumers, among others.

Digitization

Creating a digital economy in Russia is one of the key objectives defined in the Strategy. The main legislative initiatives in this area are intended to lift regulatory barriers, develop technically neutral laws and digitize legal relationships that traditionally occur only offline. Various legislative amendments have been adopted in recent years. Their objective is to support the transition to digital public services and online interaction with courts and notaries, the development of e-commerce and telemedicine, and the digitization of industry.

1 Order of the President of Russia No. 203 on the Strategy for the Development of an Information Society in the Russian Federation for 2017–2030 of May 9, 2017.

Statistics

Reasons for blocking information resources

4 → 24

2012 2020

Administrative offenses in communications and information

26 articles → 48 articles

2010 2020

Requirement to store data in Russia

3 → 7 + 1 and more (plans)

2014 2020

IT and computer information crimes

7 articles → 11 articles

2010 2020

Administrative fines for violation of personal data laws

10 000 → 18 million

2010 2020

Administrative fines for violation of the Information Law

500 000 → 1/5 total revenue

2014 2020

IP protection on the Internet

2013

Blocking for infringement of exclusive rights to films

2014

Blocking for infringement of the rights to any items subject to copyright and related rights (other than photos)

Permanent blocking for repeat offense

2020

Blocking of software apps illegally containing items subject to copyright and related rights (other than photos)

Key new developments

2010

Protection of children

Laws protecting children from information harmful to their health and development appear

2011

National payment system

Use of e-money first regulated

2013

Legalization of Open Source

Regulation of open licenses appears

2017

Critical infrastructure

Requirements for protecting the IT infrastructure of critical enterprises set

2018

PPP in IT

Software, databases, IT systems and sites become separate subjects for PPP and concession agreements

2019

Digital rights and crowdfunding

Digital rights appear and the first type of digital rights is defined in crowdfunding laws

2020

Experimental legal regimes

Special legal regulation adopted for "digital sandboxes" where innovative technologies will be developed

New decade, new signature

First e-signature law enacted

2002

2011

New e-signature regulation goes into effect

Substantially revised provisions on e-signatures enter into force

2020

Major Russian legislation changes for 2020

1. Changes in the rules for processing publicly available personal data

On March 1, 2021,[2] amendments to the Federal Law on Personal Data[3] (the "**Personal Data Law**") regarding the processing of personal data subject to dissemination (**"Law No. 519**"[4]) went into effect.

Law No. 519 introduces a new term: "*personal data permitted for dissemination.*" This means data the subject has allowed the public to access by giving a special consent. With this comes the repeal of the provision of Article 6(1)(10) of the Personal Data Law that was a separate ground for processing personal data that a subject had made public. So there has been a transition from the subject taking **practical** steps to disclose their personal data toward **formal permission** for certain use of the data disclosed by the subject.

According to the new Article 10.1 of the Personal Data Law, a separate consent to processing personal data permitted for dissemination (the "**Consent**") is to be given. It may be submitted to the operator directly or using the information system of the Federal Service for Supervision of Communications, Information Technologies and Mass Media ("**Roskomnadzor**").[5]

The Consent must clearly give permission to disseminate personal data and state that there are no special conditions for processing or personal data that cannot be processed. Within three business days of receiving the Consent, the operator is required to publish information about the processing terms and any prohibitions on public processing of his/her personal data that the subject has established.

The changes are not retroactive and do not require operators to obtain (or update) the consents of users whose data are already processed when Law No. 519 goes into effect. However, starting March 1, 2021, a data subject may request at any time that any person processing their personal data illegally stop transmitting (disseminating, providing, accessing) their personal data. The operator must stop transmitting such personal data within three business days of receiving the subject's request. If the subject has filed with a court, then the transmission must cease within the time specified in the effective court decision (and if the decision does not state a time, within three business days of when the decision becomes effective).

Law No. 519 does not contain clear rules on the correlation between the new Article 10.1 and Article 6(1) of the Personal Data Law in terms of possible grounds for processing personal data other than the Consent. From an overall interpretation of the provisions, it seems that Article 10.1 should generally cover relations associated with processing personal data to which access is granted *by the subject voluntarily* and that the new rules do not apply to personal data that might be disseminated regardless of the subject's will (for example, due to a requirement of federal law on mandatory publication of personal data). This seems to be the case considering the statement in Article 10.1 that if a subject discloses personal data to the public without giving a Consent, or if the data were disclosed due to circumstances beyond the subject's control (e.g., wrongdoing or force majeure), each person who disseminated or otherwise processed the personal data must prove that they did so lawfully.

2 Except for the provision regarding the possibility of getting consent via Roskomnadzor's information system; that provision becomes effective on July 1, 2021.
3 Federal Law No. 152-FZ on Personal Data of July 27, 2006.
4 Federal Law No. 519-FZ of December 30, 2020, on Amendments to the Federal Law on Personal Data.
5 Roskomnadzor has drafted an order with requirements to the contents of the Consent: https://regulation.gov.ru/projects#npa=112660.

2. Additional social media responsibilities

February 1, 2021, saw the entry into force of amendments to the Federal Law on Information, Information Technologies and Protection of Information[6] (the "**Information Law**") involving the regulation of social networks ("**Law No. 530**"[7]).

Law No. 530 impose obligations on owners of social networks with fines up to RUB 8 million and fines of 1/10 total annual revenue for failure to comply. Law No. 530 defines the owner of a social network as being among the following group: (1) a site owner; (2) a webpage owner; (3) an information system owner; (4) an owner of software ("**software**").

Social Network Owners are subject to the new rules if:

1. the site, webpage, information system or computer software (the "**Social Network**") are intended and/or used by users to provide and/or disseminate information via the personal pages they have created themselves;
2. the information is disseminated in Russian and in the state languages of the republics or other languages of the peoples of the Russian Federation;
3. the Social Network may disseminate advertising intended to get the attention of consumers who live in the Russian Federation;
4. more than 500,000 users located in the Russian Federation access the Social Network daily.

Roskomnadzor runs the register of Social Network Owners itself based on Internet monitoring. Roskomnadzor may request information to identify Social Network Owners from hosting providers and others hosting the Social Networks.

Law No. 530 gives Social Network Owners a long list of responsibilities:

1. **Don't allow the resource to be used** to commit crimes or disseminate certain categories of information (legally protected secrets, extremist materials, pornography, explicit language, information defaming a citizen or certain categories of citizens).
2. **Conduct monitoring to identify prohibited materials** (in particular, child pornography, information on how to make and use drugs, information about appeals for mass riots, extremist activity, participation in unapproved public events, fake news).
3. **Comply with** bans and restrictions of the laws on elections and referendums; rights and legitimate interests of citizens and organizations, including the honor, dignity and business reputation of citizens and business reputation of organizations.
4. **Post** certain contact information, a document stating the rules for using the social network, and an e-form for reports of information disseminated illegally (Roskomnadzor will specify the requirements to the form) and a statement on the outcome of reviewing reports.
5. **Inform every user** of changes to the rules for using the social network within three days of the changes; of steps taken to restrict access to the user's information and the grounds for the restriction.
6. **Install** one of the Roskomnadzor-suggested programs to count the number of users.

If information disseminated in violation of Law No. 530 is discovered, the Social Network Owner must restrict access to it immediately. If it has doubts as to how to evaluate the information, the Social Network Owner must forward it to Roskomnadzor and temporarily restrict access to the information within 24 hours of discovering it.

If a user's information has been wrongfully restricted, the user may submit a complaint to the Social Network Owner, then to Roskomnadzor. The user may also seek damages, including non-pecuniary damages in court as legal remedies.

Law No. 530 also requires that accessible rules for using the social network be published in Russian. There are also mandatory contents, including sections on rights and obligations, how monitoring is done and user requests are reviewed.

6 Federal Law No. 149-FZ on Information, Information Technologies and Protection of Information of July 27, 2006

7 Federal Law No. 530-FZ of December 30, 2020, on Amendments to the Federal Law on Information, Information Technologies and Protection of Information.

3. Issuance and circulation of digital financial assets regulated and cryptocurrencies defined

On July 31, 2020, the President of Russia signed Law No. 259-FZ on Digital Financial Assets, Digital Currency and Amendments to Certain Legislative Acts of the Russian Federation[8] ("**Law No. 259**"), which introduces regulation of digital financial asset circulation and defines some basic cryptocurrency concepts.

Russia is gradually putting together the puzzle of regulating the digital assets market. Law No. 259, which appeared in 2020, is already the third special law in that area. The first two pieces of the puzzle appeared earlier, in 2019: first a law introducing digital rights to Chapter 6 of the Civil Code was passed,[9] then a law on raising investments via investment platforms[10] (the "**Crowdfunding Law**"). The last major piece is missing: a separate law governing the issuance and regulation of cryptocurrencies, although the prospects of a "digital" ruble appearing are becoming ever more real.

Law No. 259 not only defined the types of digital financial assets ("**DFA**") but also introduced a system for regulating their issuance and circulation. At the same time, it changed the laws on joint stock companies, the securities market, advertising, against money laundering and corruption, and a number of other laws. Law No. 259 is aimed at creating a new financing market that is more flexible and more lightly regulated than the securities market.

Law No. 259 defines DFAs as a type of digital rights provided for under Article 141.1 of the Civil Code. They include monetary claims, the ability to exercise rights attaching to issuable securities, interest in the capital of a non-public JSC and the right to require transfer of issuable securities under a decision to issue DFAs. Digital financial assets are issued and advertised subject to posting an online decision to issue that meets the requirements of Law No. 259 and Russia's Central Bank.

8 Federal Law No. 259-FZ on Digital Financial Assets, Digital Currency and Amendments to Certain Legislative Acts of the Russian Federation of July 31, 2020.
9 Federal Law No. 34-FZ on Amendments to Parts One and Two and Article 1124 of Part Three of the Russian Federation Civil Code of March 18, 2019.
10 Federal Law No. 259-FZ on Raising Investments via Investment Platforms and on Amendments to Certain Legislative Acts of the Russian Federation of August 2, 2019.

We emphasize that DFAs are not isolated from utility digital rights and the securities market. *Hybrid* digital rights that simultaneously certify the rights named in Law No. 259, rights provided for utility digital rights by the Crowdfunding Law and other rights may be issued. It is also possible to issue DFAs whose underlying asset is classic securities, and DFAs which allow the exercise of rights to those securities.

Digital financial assets may be issued only in an information system whose rules are approved by the Central Bank for compliance with Law No. 259 (the "**Information System**"). All transactions with DFAs, including circulation, encumbrance and redemption, may be made only in the information system in which they were issued, and according to its rules (data may be exported to a different system in exceptional cases). Law No. 259 allows for Information Systems based not only on a distributed ledger-based system (blockchain) to be used.

Only a Russian legal entity listed in the Central Bank's register may be the operator of the Information System (the "**Operator**"). That entity sees to it that the system functions according to its rules, which are approved by the Central Bank. The operator's officers and participants must meet the requirements of Law No. 259. The Operator is liable, among other things, for malfunctions of the Information System, loss of information, failure to comply with the Information System rules, and misleading Information System users about its operation.

Digital financial assets must be traded either through the Operator of the relevant Information System, if its rules provide for that function, or through the digital financial asset exchange operator (the "**Exchange Operator**"), who plays a role similar to that of an exchange. Similarly, only a Russian legal entity that is listed in the Central Bank's register may be an Exchange Operator. There are additional requirements for the Exchange Operator regarding the size of its share capital and net assets, and restrictions on participation of companies from offshore jurisdictions.

Digital financial asset transactions made through an Exchange Operator must follow the exchange rules which, in turn, must meet a number of requirements and be approved by the Central Bank. Notably, Law No. 259 also applies to trading in Russia of DFAs issued on foreign information systems, although as yet there are no special rules regulating those transactions.

Anyone may acquire DFAs. However, Law No. 259 authorized the Central Bank to set restrictions on the acquisition of DFAs by unqualified investors. So, since early 2021, unqualified investors cannot acquire foreign DFAs; DFAs that allow a person to exercise rights to securities that may be acquired only by qualified investors; other DFAs that don't specify the deadline for fulfilling certified obligations. Unqualified investors are also not allowed to acquire more than RUB 600,000 in DFAs per year (except where specifically indicated). The status of qualified investor is determined according to the criteria of the securities market legislation.

Law No. 259 contains just a few rules on cryptocurrencies. Cryptocurrencies are considered property and are given a legal definition, i.e., "digital currency" is a set of electronic data in the Information System that are offered as a means of payment that is not the currency of the Russian Federation or a foreign currency, an international currency or unit of accounting, or as an investment, and in respect of which there is no person obligated to the owner of such electronic data other than the Operator and/or nodes of the Information System, which are only obliged to ensure compliance with the procedure for the release of this data and the taking of actions in relation to them to make entries in the Information System in accordance with its rules. A few other digital-currency related terms are defined, but it is stated that relations arising from the issuance, arrangement of an issue, recording and circulation of digital currencies must be regulated by a separate law.

Law No. 259 prohibits Russian entities and Russian branches (or representative offices) of foreign companies from accepting digital currency as consideration (payment) for goods, work and services. Also, information about acceptance (or offer) of digital currency as consideration in Russia cannot be disseminated.

4. Changes in the rules on circulation of information

4.1. New subjects

Amendments to Article 15.2 of the Information Law became effective on October 1, 2020. They affect the operations of mobile app aggregators.

Now, when information the dissemination of which infringes copyright and related rights is discovered, the rights holders may request that access to not only the information resources, but also to the applications used to access that information be restricted. The concept of "software application owner" was also introduced to the Information Law. It means the person/entity that independently and in its sole discretion determines how the relevant software application ("**software application**") is used.

As before, the rights holder may request that Roskomnadzor take steps to restrict access to information based on an effective judicial act. Roskomnadzor will then forward the request to restrict access to items subject to copyright and related rights to the owner of the information resource on which the software application is hosted, or to another entity that hosts it. Those entities in turn will have to notify the software application owner that it needs to restrict access to the item subject to copyright and related rights within one business day. The software application owner itself must also take steps within one business day.

If the software application owner does not comply with the request, the owner of the information resource will have to restrict access to the software application within three business days of receiving the request from Roskomnadzor. If that request is not fulfilled, the telecoms operator will restrict access.

4.2. New reasons and grounds for blocking information

The Information Law was amended in 2020 with a new reason to block information.[11] This reason is the dissemination of information containing an offer for retail sale of medicines, including distance (online) sale, if the retail sale of those medicines is restricted or prohibited. Offers by unlicensed and unpermitted entities to sell medicines will also be blocked.

In addition to that, January 10, 2021, saw the entry into effect of amendments to Federal Law No. 272-FZ on Enforcement Actions Regarding Persons Involved in Violations of Fundamental Human Rights and Freedoms and the Rights and Freedoms of Russian

11 Federal Law No. 105-FZ of April 3, 2020, on Amendments to Article 15.1 of the Federal Law on Information, Information Technologies and Protection of Information and the Federal Law on the Circulation of Medicines.

Federation Citizens of December 28, 2012 ("**Law No. 272**"[12]). The amendments introduced a new ground for blocking information: a decision declaring the owner of an information resource involved in violations of fundamental human rights and freedoms, and the rights and freedoms of Russian Federation citizens (the "**Decision**").

The owner of an information resource is involved in these violations if it restricts users' dissemination of socially significant information in the Russian Federation, including media reports and materials. It is also involved if it sets other restrictions that violate Russian citizens' right to freely search for, receive, transmit, generate and disseminate information. The restriction of disseminating such information will fall under Law No. 272 if it is imposed, e.g., based on ethnicity, language, financial and employment situation, attitudes toward religion or due to foreign states' introduction of political or economic sanctions against the Russian Federation, Russian citizens or Russian legal entities. However, the criteria for determining what is "socially significant information" or "other restrictions" are not defined for the purposes of Law No. 272.

Thus, those issuing the Decision, namely the Prosecutor General of the Russian Federation and his deputies (in coordination with the Ministry of Foreign Affairs of Russia) have absolute discretion to assess these circumstances.

After it receives the Decision Roskomnadzor will include the details on the information resource on a special list and interact with the resource's owner. If the owner fails to correct the violation, then access to the resource will be restricted using the mechanisms provided to Roskomnadzor by the "sovereign Internet" law[13] (for more detail see section 1 of the Major Russian Legislation Changes for 2019). The access may be restricted fully or partially and Law No. 272 does not contain the factors affecting the extent of blocking.

Considering the "sanction" nature of Law No. 272, it can be supposed that the amendments to it will not affect the entire market, but primarily the media and information resources covering political and public activities. From the perspective of users (whether individuals or corporate users), the amendments adopted to guarantee rights to free search, access and dissemination of information may ultimately result in no longer having access to large volumes of information.

12 Federal Law No. 482-FZ of December 30, 2020 on Amendments to the Federal Law on Enforcement Actions Regarding Persons Involved in Violations of Fundamental Human Rights and Freedoms and the Rights and Freedoms of Russian Federation Citizens of December 30, 2020.

13 Federal Law No. 90-FZ of May 1, 2019, on Amendments to the Federal Law on Communications and the Federal Law on Information, Information Technologies and Protection of Information.

4.3. Multimillion-ruble administrative fines

The Administrative Code contains a new Article 13.41 which sets administrative fines in the millions of rubles for failure to remove prohibited information and failure to take steps to restrict access to that information where required to do so by law ("**Law No. 511**"[14]).

The administrative sanction is imposed on such entities involved in the information blocking process as hosting providers and other entities hosting an information resource, owners of sites and information resources. The following fines have been set:

- RUB 800,000 to RUB 4,000,000 (first offense)
- 1/20 the total revenue for the calendar year preceding the year or part of the year in which the offense was discovered, but not less than RUB 4,000,000 (repeat offense)

The fines are higher for cases of failure to remove certain categories of prohibited information, namely, information containing appeals to engage in extremist activities, materials with pornographic images of minors, information about narcotics and psychotropic substances. Failure to remove such information is subject to the following fines:

- RUB 3,000,000 to RUB 8,000,000 (first offense)
- From 1/10 to 1/5 the total revenue for the calendar year preceding the year or part of the year in which the offense was discovered, but not less than RUB 8,000,000 (repeat offense)

The explanatory note to Article 13.41 of the Administrative Code states that its provisions do not apply to the restriction of access to information the dissemination of which infringes copyright and related rights.

4.4. Development of laws on identification

Federal Law No. 479-FZ on Amendments to Certain Legislative Acts of the Russian Federation of December 29, 2020, amended a number of legislative acts related to the processes of remote identification and authentication of individuals by biometric data duly provided in advance and to take certain legal actions[15] (the "**Law No. 479**").

According to Law No. 479, biometric data may be collected and processed for identification and authentication using either the state information systems (the unified system of identification and authentication (**USIA**) or the unified biometric system (**UBS**), or other privately operated information systems. In the last case, there are additional requirements compliance with which will be monitored by an accreditation procedure (in particular, the taking of technical and organizational measures to ensure the security of personal data).

Law No. 479 empowers banks and other organizations, individual entrepreneurs and notaries to use USIA and UBS to identify people. So, it has become possible, among other things, to enter into communications services contracts using the streamlined procedure. According to the amendments made to the Federal Law on Communications,[16] starting June 1, 2021, such a contract may be concluded online using a simple e-signature (the key to which was obtained when requesting state or municipal services) using information from the USIA.

14 Federal Law No. 511-FZ of December 30, 2020, on Amendments to the Russian Federation Code of Administrative Offenses.
15 Federal Law No. 479-FZ on Amendments to Certain Legislative Acts of the Russian Federation of December 29, 2020.
16 Federal Law No. 533-FZ of December 30, 2020, on Amendments to the Federal Law on Communications.


nfidential Data
[Identify Person]

5. Concept for the development of legal regulation of artificial intelligence and robotics technologies

The Concept for the Development of Regulation of Relations in Artificial Intelligence and Robotics Technologies until 2024[17] (the "**Concept**") has been approved.

The Concept expands on the goals and objectives defined in the National Strategy for the Development of Artificial Intelligence for the Period until 2030[18] and is aimed at defining legal barriers and approaches to transforming the regulatory system, and at creating prerequisites for the fundamental regulation of new social relationships. This transformation must balance the interests of various stakeholders: humans, society, government and business.

In addition to approaches to transforming legal regulation, the Concept also sets goals, objectives and areas for regulating AI and robotics relations, regulatory principles and key issues. The Concept highlights industrywide and industry-specific regulatory objectives (for example, for such fields as healthcare, public administration, transportation, urban planning, finance and industry). The following are designated as industrywide regulatory tasks:

- Creating mechanisms for simplified implementation of products using AI and robotics technologies
- Solving liability issues
- Improving the circulation of data
- Developing insurance institutions
- Improving the protection of intellectual property rights

The Concept also notes the need for financial incentives for companies focusing on developing AI and robotics technologies. Among other things, public-private partnerships need to be developed in this area. Another effective tool for realizing the ideas enshrined in the Concept is the use of experimental legal regimes (generally known as **Regulatory sandbox**). For example, a five-year Regulatory sandbox to develop and implement AI technologies was set in Moscow from July 1, 2020[19], even before the Concept was adopted. To participate in the Regulatory sandbox an application needs to be submitted to the competent agency of Moscow to then be included in a special register.

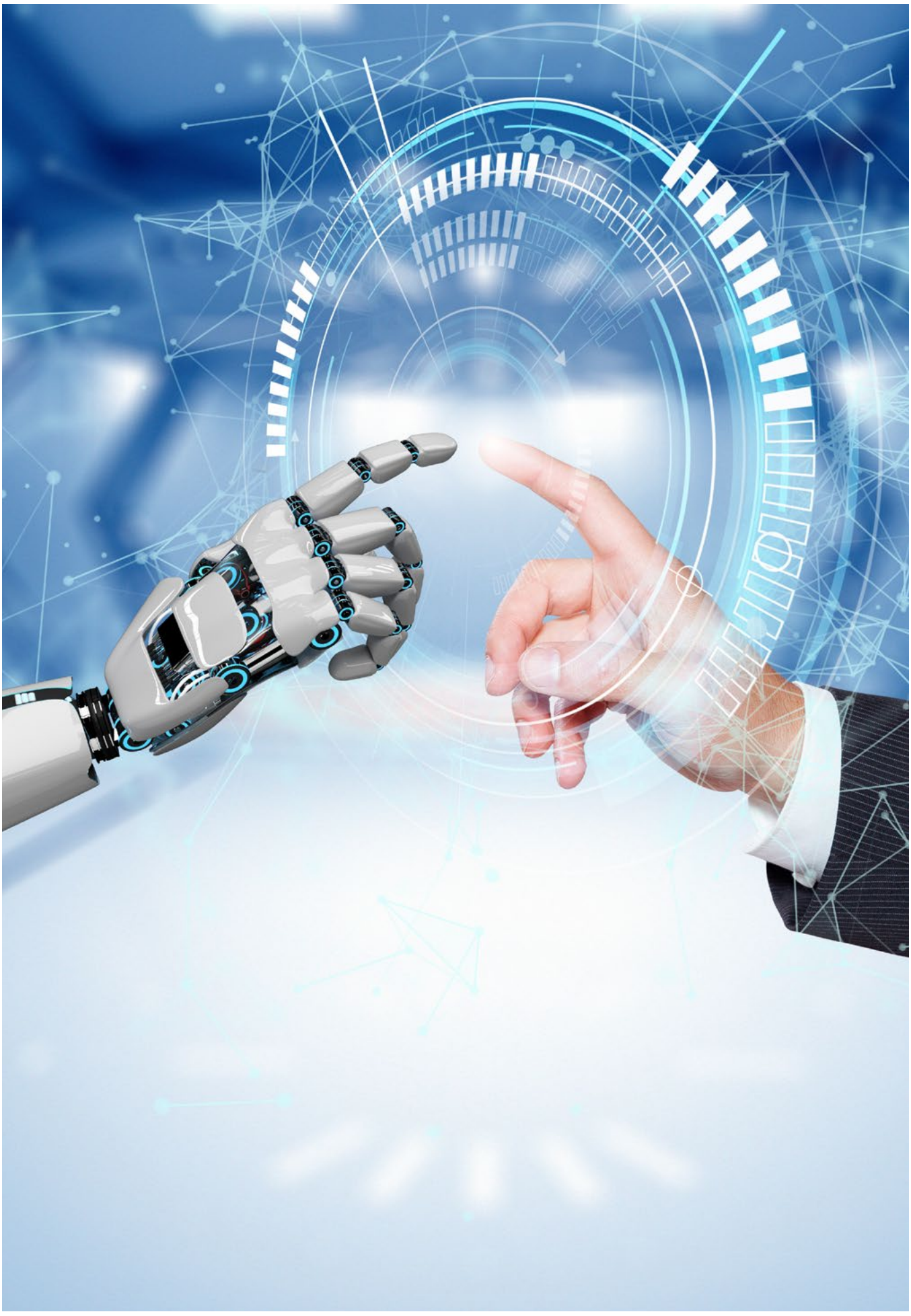
The Federal Law that introduced the Regulatory sandbox in Moscow outlines the goals, objectives and principles for setting them but does not set special requirements for the development, creation, rollout and implementation of AI technologies, how and under what conditions personal data will be processed, or the specifics of tracking the results of using artificial intelligence. The Government of Moscow was delegated to determine all of that. It adopted the relevant regulations in December 2020. You can learn more about Regulatory sandboxes in other areas in section 6 of this document.

In conclusion, it should also be noted that the establishment of the sandbox is possible both in relation to federal legislation and at the level of the constituent entity of the Russian Federation (on the subject of jurisdiction of the constituent entity of the Russian Federation).

17 RF Government Order No. 2129-r of August 19, 2020 on Approval of the Concept for the Development of Regulation of Relations in Artificial Intelligence and Robotics Technologies until 2024 of August 19, 2020.

18 Order of the President of Russia No. 490 of October 10, 2019, on the Development of Artificial Intelligence in the Russian Federation of October 10, 2019.

19 Federal Law No. 123-FZ of April 24, 2020, on the Conduct of an Experiment to Establish Special Regulation to Create the Necessary Conditions for the Development and Implementation of Artificial Intelligence Technologies in Moscow, a Constituent Entity of the Russian Federation and Federal City, and Amending Articles 6 and 10 of the Federal Law on Personal Data.



6. Experiments with laws for digital innovation

January 28, 2021, saw the enactment of the Federal Law on Experimental Legal Regimes in Digital Innovations in the Russian Federation[20] ("**Law No. 258**"). It creates a legal basis for establishing experimental legal regimes (generally known as **Regulatory sandbox**) in various areas. A large number of statutory acts detailing its provisions were adopted in addition to Law No. 258.

Regulatory sandbox makes it possible to not apply certain provisions of regulations which are specified in the program of the sandbox, that hinder the development of digital innovations, and to set special rules for its participants in a certain territory (generally). The regulations will not apply for up to three years and this period may be extended for one year by the Russian Government. Although Regulatory sandbox is established by the Russian Government or the Central Bank adopting the program, if the program of sandbox is to cancel and/or change the effect of the provisions of any federal law, then the federal law needs to be amended first. At the end of the testing period and once the participants' performance is evaluated, a decision is made whether the legislative acts need to be amended permanently.

The law lists eight areas where Regulatory sandbox may be established: (1) medical and pharmaceutical activities; (2) the creation and operation of vehicles and provision of transportation services; (3) agriculture; (4) financial market; (5) distance (online) selling; (6) real estate design, construction, repair and operation; (7) provision of state and municipal services and government oversight; and (8) industrial manufacturing. The Russian Government may extend this list of areas.

The state and (in some cases) local government authorities initiate an ELR. Unsolicited proposals may also be made by legal entities and individual entrepreneurs.

20 Federal Law No. 258-FZ on Experimental Legal Regimes in Digital Innovations in the Russian Federation of July 31, 2020.

The digital innovations tested by participants must be new or substantially improved products, processes or methods based on technologies listed by the Russian Government and the Central Bank (only on the financial market). The Russian Government and the Central Bank have already approved lists that include more than 60 such technologies, e.g., artificial intelligence, blockchain, robotics, quantum technologies, VR/AR and IOT.

The Regulatory sandbox must pursue socially useful objectives such as developing competition, creating new types and forms of economic activity, improving legislation, and raising investment in the digital economy. Some areas cannot be subject to special regulation within the Regulatory sandbox. These include areas of regulation associated with a high risk of harming the interests of the individual, society and the state, including the security of critical information infrastructure, and the introduction into circulation of goods, work and services whose circulation is restricted or prohibited. The Russian Government may decide to end the sandbox in progress, before it is slated to end, if unforeseen risks causing human rights violations, harming health or property, prejudicing the interests of the state, compromising state defense and/or security and that cannot be corrected by the the sandbox subjects are discovered.

The Regulatory sandbox participants have special responsibilities. These include maintaining a register of counterparties, informing people who express an interest in dealing with the participant of the terms of the sandbox, and following the statutory procedure to review complaints of rights violations in connection with implementing the Regulatory sandbox.

It is important to stress that, although general regulations are limited within the Regulatory sandbox, the sandbox participants are not exempt from civil liability for harm to life, health or property caused by their lawful actions.

In conclusion, it should also be noted that the Regulatory sandbox can be set up at the level of federal and regional law (of the Russian Federation constituent entity) within the powers of the government authorities in the constituent entity's areas of jurisdiction.

7. Changes in intellectual property

7.1. Commercialization of intellectual property created under a state (or municipal) contract

Federal Law No. 456-FZ was adopted in December 2020 and amended part four of the Russian Federation Civil Code[21] ("**Law No. 456**"). Law No. 456 is intended primarily to unify the regulation of rights to various results of intellectual activity ("**IP**") created in performing a state or municipal contract.

A new provision was added to part four of the Civil Code. Article 1240.1 sets a general rule that the contractor holds the exclusive right to IP created in performing a state or municipal contract. The exceptions are when:

a. The IP is directly related to defense and security.

b. The IP is needed to provide public services or perform public functions.

c. The contractor has not taken the actions needed to have its exclusive right to the IP recognized within 12 months of when the work was accepted.

d. The IP was created under a contract made to fulfill the Russian Federation's international commitments.

The Russian Federation, its constituent entity or a municipality holds the exclusive right to the IP in the above cases and in other cases stipulated by law. The rights holder is responsible for starting to use the IP in practical activity or assigning the exclusive right to other interested parties within two years of when the right arises. The Russian Government determines the conditions and procedure for fulfilling this responsibility, the consequences for failing to fulfill it and how it may be terminated.

There is special regulation for certain types of IP.

The amendments that were adopted should promote the commercial use of intellectual properties funded by the state or municipal budget. They should also eliminate situations where rights holders do not use the items.

Article 1370 of the Civil Code was amended for the same purpose. Those amendments entitle the employee (the author of the work for hire invention, utility model or industrial design) to request that the employee be assigned the patent royalty-free if the employer decides to terminate the patent prematurely. The employee may file a lawsuit if the employer refuses or avoids making the assignment.

21 Federal Law No. 456-FZ on Amendments to Parts Two and Four of the Russian Federation Civil Code and Repeal of Legislative Acts (certain provisions of legislative acts) of the Russian Federation of December 22, 2020.

Law No. 456 becomes effective on January 1, 2022. The Russian Government still has to determine other details.

7.2. New rules for remunerating works for hire

New Rules for Paying Remuneration for Works for Hire that are Inventions, Utility Models or Industrial Designs[22] (the "**Rules**") went into effect on January 1, 2021.

The main difference between the new Rules and the old regulation is an increase in payments for using an invention, utility model or industrial design. Now instead of one average salary the employer must pay the employee three average salaries for use of an invention, and two average salaries for use of a utility model or industrial design for the last 12 calendar months. The amounts paid for creating IP remain unchanged.

As before, these Rules do not apply to cases where the employer and employee have made an agreement on the amount, conditions and procedure for paying remuneration.

The Rules will remain in effect until January 1, 2027.

7.3. Eurasian patent for an industrial design

In November 2020 Russia ratified the Protocol on the Protection of Industrial Designs to the September 9, 1994, Eurasian Patent Convention[23] (the "**Protocol**").

The Protocol was developed in 2019 by the Eurasian Patent Office together with member states of the Eurasian Patent Convention (EPC) to create a regional system for protecting industrial designs based on a single Eurasian patent.

The procedure established by the Protocol makes it possible to get legal protection for an industrial design throughout the member states by filing a single application with the Eurasian Patent Office (directly or through the national office). Upon registration, the Eurasian patent is effective in all member states. The duration is five years, which may be extended but may not exceed 25 years from the filing date.

The main advantage of this procedure is that it reduces the administrative and financial burden on applicants. This should also generally encourage the development of industrial designs in EPC member states.

22 Russian Federation Government Resolution No. 1848 on Approval of the Rules for Paying Remuneration for Works for Hire that are Inventions, Utility Models or Industrial Designs of November 16, 2020.

23 Federal Law No. 377-FZ of November 23, 2020 on Ratification of the Protocol on the Protection of Industrial Designs to the September 9, 1994, Eurasian Patent Convention.

8. Changes in consumer laws

Last year there were a number of new developments in consumer protection legislation that could be very important for e-commerce and the sale of IT devices.

First, Russian Federation Government Resolution No. 2463 of December 31, 2020,[24] entered into effect on January 1, 2021. Among other things, it set new rules for distance (online) selling of products.

The general rules and approaches regulating distance selling remain the same. However, there are a number of changes. For example, possible ways of identifying customers have been provided for. The new distance selling rules are much less broad than those that were previously instituted by the old RF Government Resolution No. 612 of September 27, 2007.[25] Thus, distance selling is mainly regulated by the Russian Federation Law on Consumer Protection and the general rules for retail sale and purchase.

Second, a law on mandatory preinstallation of Russian (or Eurasian) software on certain types of devices was adopted. Technically, the amendments were made to Article 4 of the RF Law on Consumer Protection. That article addresses the quality of goods, work and services. The key rules for preinstallation are set forth in RF Government Resolution No. 1867 of November 18, 2020[26] (the **"Resolution"**).

According to the Resolution, Russian software must be preinstalled on smartphones and tablets, computer devices and Smart TVs.

The Resolution specifies the types of devices and programs that must be installed on those devices. For example, for smartphones it is search engines, navigators, antivirus and some other programs.

The Resolution also contains criteria for Russian software for preinstallation purposes. These criteria are largely in line with the requirements for software allowed for state and municipal procurement.[27] However, there are a number of additional requirements (for example, technical requirements and those having to do with the software's popularity and social value).

Russian Federation Government Order No. 3704-r of December 31, 2020,[28] already specified the list of software to be preinstalled. For example, the list includes some Yandex apps (such as Maps and Disk), the ICQ messenger, the VKontakte social network app, many audiovisual service apps and TV channels.

The requirement to sell devices with preinstalled Russian programs becomes effective on April 1, 2021, just as the Order containing the Russian software list.

The third new development is that product and service aggregators are now responsible for enabling acceptance of the Mir card for cashless payments.

As for sellers (providers), this responsibility affects aggregators whose revenue for the preceding calendar year was RUB 40 million or more.

However, this threshold will drop to RUB 20 million in revenue for the preceding calendar year starting July 1, 2021. There will be a transitional period between March 1 and June 30, 2021, when the revenue threshold will be RUB 30 million.

24 Russian Federation Government Resolution No. 2463 on Approval of the Rules for Selling Goods under a Retail Sale and Purchase Agreement, the List of Durable Goods for Which the Customer Cannot Request to be Provided Free of Charge with a Similar Product for the Period of Repair or Replacement and the List of Proper-Quality Nonfood Products that Cannot Be Exchanged, and Amendments to Certain Acts of the Government of the Russian Federation of December 31, 2020.

25 Russian Federation Government Resolution No. 612 on Approval of the Rules for Distance Sale of Goods of September 27, 2007.

26 Russian Federation Government Resolution No. 1867 on the List of Certain Types of Technically Complex Products with Preinstalled Russian Computer Software, the Procedure for Making and Keeping the List of Russian Computer Software Which Must Be Preinstalled on Certain Types of Technically Complex Products and the Procedure for Preinstalling Them of November 18, 2020.

27 Unified Register of Russian Software and Databases kept by the Ministry of Communications of Russia (https://reestr.digital.gov.ru/).

28 Russian Federation Government Order No. 3704-r on Approval of the List of Russian Computer Software Which Must Be Preinstalled on Certain Types of Technically Complex Products of December 31, 2020.

9. Changes in inspection rules

2020 saw a number of changes to how the competent communications, IT and telecommunications authorities conduct inspections. We have prepared a list of the key changes.

Preventing violations of mandatory advertising requirements

Since January 1, 2021, it has been possible to arrange for and conduct measures to prevent violations of the mandatory requirements set by Federal Law No. 38-FZ on Advertising of March 13, 2006, other federal laws and regulations on advertising.[29]

FAS administrative regulations on unscheduled inspections updated

The updated regulations contain an exhaustive list of documents and information that may be requested during an inspection (around 20 items).[30] Among the items that may be requested during an inspection are copies of the advertisement, information about the scope of the advertising campaign, about equipment and software used to disseminate advertising on telecommunications networks, and copies of standard contracts (e.g., sale and purchase, loan and other contracts).[31] A provision was added to the Decree whereby, during an inspection, information and documents may be requested from the government authorities, local government authorities and organizations under their jurisdictions as part of liaising with other agencies.[32]

An indicator of the risk of violation of requirements for the conduct of unscheduled inspections when Roskomnadzor performs supervision of communications has been established

According to a Ministry of Communications of Russia Decree[33] (the "**Decree**"), an unscheduled inspection may be based on information in the media or on the Internet that the telecommunications network is being used to provide paid communication services, services to connect telecommunications networks, and services for the transmission of traffic in the telecommunications network in the event that the telecommunication network is not commissioned.

On-site inspections of telecommunications equipment

The Decree clarifies the cases and procedure for conducting an on-site inspection within the procedure of giving telecommunications equipment made-in-Russia status.[34] An on-site inspection may be conducted because (1) the applicant has failed to submit documents in allowed cases (for example, if the documents contain a trade secret) or (2) there is a need to do additional examination of the documents if there are discrepancies or inconsistency with information in the Ministry of Industry and Trade of Russia order.[35] At the end of the inspection a decision is made on whether the telecommunications equipment does or doesn't meet the requirements.

29 Clause 2(e) of RF Government Resolution No. 1838 on Approval of the Regulations on State Supervision in Advertising of November 16, 2020.
30 FAS Russia Decree No. 1203/20 on Approval of the Administrative Regulations of the Federal Antimonopoly Service for State Supervision of Advertising by Doing Unscheduled Inspections of Compliance with Russian Federation Laws on Advertising of December 9, 2020.
31 Clause 1.12 of FAS Russia Decree No. 1203/20 of December 9, 2020.
32 Clause 1.13 of FAS Russia Decree No. 1203/20 of December 9, 2020.
33 Ministry of Communications of Russia Decree No. 451 on Approval of the Risk Indicator of Violation of Mandatory Requirements Used to Determine the Need to Conduct Unscheduled Inspections when the Federal Service for Supervision of Communications, Information Technologies and Mass Media and its Regional Offices Perform State Federal Supervision of Communications of September 9, 2020.
34 Clause 14 of Ministry of Industry and Trade of Russia Decree No. 2351 on Approval of the Procedure for the Conduct of an On-Site Inspection for the Examination of the Applicant's Telecommunications Equipment of July 22, 2020.
35 Clauses 34, 44 and 51 of RF Government Resolution No. 878 of July 10, 2019 (as amended on July 25, 2020).

10. Clarification of regulation regarding the Yarovaya law

Two Russian Government resolutions entered into force on January 1, 2021. They clarify the legal regulation implementing the so-called Yarovaya law. Both acts affect the activities of organizers of the dissemination of information on the Internet (the "**Organizer**").

10.1. Rules for providing information about receipt and transmission of electronic messages to the competent government authorities

Russian Federation Government Resolution No. 1526 of September 23, 2020 ("**Resolution No. 1526**"),[36] similarly to the repealed RF Government Resolution No. 759 of July 31, 2014, outlines (1) the list of information about receipt, transmission, delivery and/or processing of voice information, written text, images, sounds, video or other electronic messages; (2) the list of information about users; (3) where and how information is stored; (4) how and when to provide information to the competent government authorities (conducting investigative activities or ensuring the security of the Russian Federation). The document limits the time Organizers can take to respond to requests from the competent authorities: a response to standard requests must be made within 30 days, and a response to standard requests marked "urgent" must be made within three business days of when the request is received.

10.2. Notifying Roskomnadzor of the commencement of activity to receive, transmit, deliver and/or process electronic messages

There is now a procedure for an Organizer to notify Roskomnadzor of the commencement of activity to support the functioning of information systems and/or computer programs that are intended for and/or used to receive, transmit, deliver and/or process Internet users' (the "**Notification**")[37] electronic messages.

The Organizer may file the notification on its own or the notification must be sent within 10 business days of receiving the request from Roskomnadzor. If the Organizer is a Russian citizen, a Russian legal entity or individual entrepreneur, identification and authentication procedures in the Unified System of Identification and Authentication must first be completed before submitting the Notification to Roskomnadzor.

After sending the Notification, the Organizer must notify Roskomnadzor of (1) change of information in the Notification; (2) ceasing activity to support the functioning of the information resource; (3) transfer of the rights to the information resource to another person. The regulator enters all of the information received in the Register of Organizers of the Dissemination of Information.

36 Russian Federation Government Resolution No. 1526 on the Rules for the Storage by Organizers of the Dissemination of Information on the Internet Information and Telecommunications Network of Information about the Receipt, Transmission, Delivery and/or Processing of Voice Information, Written Text, Images, Sounds, Video or other Electronic Messages of Users of the Internet Information and Telecommunications Network and Information about those Users and Providing it to the Competent Government Authorities Conducting Investigative Activities or Ensuring the Security of the Russian Federation of September 23, 2020.

37 Russian Federation Government Resolution No. 1824 on Approval of the Rules for Organizers of the Dissemination of Information on the Internet Information and Telecommunications Network to Notify the Federal Service for Supervision of Communications, Information Technologies and Mass Media of the Commencement of Activity to Support the Functioning of Information Systems and/or Computer Programs that are Intended and/or Used to Receive, Transmit, Deliver and/or Process Internet Users' Electronic Messages, and the Keeping of the Register of Those Organizers of November 12, 2020.

Contacts

Victor Naumov
St. Petersburg Managing Partner,
Head of the Russia IP, IT and
Telecommunications practice
and Co-Head of Europe Internet
& Tech Regulatory
T: + 7 812 325 84 44
victor.naumov@dentons.com

ABOUT DENTONS

Dentons is the world's largest law firm, connecting talent to the world's challenges and opportunities in more than 75 countries. Dentons' legal and business solutions benefit from deep roots in our communities and award-winning advancements in client service, including Nextlaw, Dentons' innovation and strategic advisory services. Dentons' polycentric and purpose-driven approach, commitment to inclusion and diversity, and world-class talent challenge the status quo to advance client and community interests in the New Dynamic.

dentons.com

CSBrand-53176-IP-IT-Decade-Top-EN-04 — 24/03/2021