Liniya Prava

Liniya Prava Law Firm
4 Shluzovaya naberezhnaya | Moscow 115114, Russia
Business Centre "Rosso Riva" | 5th Floor
Tel: +7 495 937-80-00 | Fax: +7 495 937-80-01
E-mail: moscow@lp.ru | web: www.lp.ru

RCLS 俄罗斯-中国法学会 Russia-China Law Society

13.10.2017 No. 6

RECENT UPDATES IN RUSSIAN LAW (3 QUARTER 2017)

Vadim Konyushkevich
Partner, Head of Foreign Investments practice Liniya Prava Law Firm
Vadim.Konyushkevich@lp.ru
http://lp.ru/en/

1. FOREIGN INVESTMENTS

1.1. Russia plans to strengthen control over foreign aircraft acquisition

The draft law expanding powers of the Government to control the acquisition of foreign aviation and shipbuilding production has been introduced in the State Duma[1]. It provides for the amendments to the Federal Law dated 18 July 2011 No. 223-FZ (**Law on procurement**) establishing the procurement rules for state corporations, companies and publicly-held enterprises (**state companies**). State companies shall coordinate with the Government Import Substitution Commission (**Commission**) purchase of goods, works and services defined by the Government within the implementation of investment projects with a value exceeding 10 billion rubles.

However, certain types of products, primarily, of aviation and shipbuilding industries are exempted from this rule on the basis of the cost and designated purpose criteria and, therefore, their acquisition does not require coordination with the Commission. According to the draft law, the Government by specific bylaws will determine the list of goods, works, services, rent (including freight and leasing) and the initial (maximum) price of the contract. If this price is exceeded, the purchaser will be obliged to obtain approval from the Commission to conclude such agreement.

At this stage the following ultimate values are proposed:

- for aircrafts - 1 billion RUB (approx. 17.2 mln USD);

- for shipbuilding products - 2 million RUB (approx. 34,500 USD);
- for drilling platforms - 100 million RUB (approx. 1.7 mln USD).

Besides, the draft law extends the force of the Law on procurement: earlier only state-owned companies were covered by specific procurement requirements within investment projects. Now the subsidiaries of state-owned companies shall also coordinate their transactions with the Commission.

In order to purchase products from a foreign supplier it will be necessary to obtain prior approval of the Commission in terms of operational characteristics of goods, as well as to justify the need for the procurement outside the Russian Federation.

In case the draft law is adopted, it will come into force at the beginning of 2018.

The Ministry of Transport also proposed measures aimed at stimulation of import substitution in the aviation industry. The Ministry is going to amend the Federal Aviation Regulations and establish the minimum quantity of domestic aircraft in the fleet.

New rules for coordination of transactions concerning foreign aircraft will affect most Russian air carriers, which will be obliged to coordinate almost all aircraft transactions with the Commission. On the one hand, the initiatives are aimed at development of domestic aviation and shipbuilding production. On the other hand, they will lead to certain difficulties for air carriers and limitation of access to the market of foreign suppliers.

[1] Draft Federal law No. 261318-7 "On amending Federal law "On procurement of goods, works, services by certain types of legal entities"

1.2. Recent case law on foreign investors' protection in Russia

On 12 July 2017 the Presidium of the Supreme Court issued the review of the case law related to protection of foreign investors (Review).

The most significant conclusions are listed below.

Legal regime of foreign investments

- Benefits granted to foreign investors cannot be abolished after long term on formal grounds and when public interest is not proved.

Implementation control of foreign investments

- Creating branches and representative offices of companies with foreign investments on the territories of closed administrative entities requires obtaining permission.

- If several foreign companies controlled by one foreign person acquire shares of a Russian joint stock company, such shares are consolidated for establishment of necessity to coordinate such transaction with the Federal Anti-Monopoly Service.

Taxes payments

- Tax incentives guaranteed to investors cannot be abolished until the end of the initially settled period, even if the legislator subsequently changed the provisions concerning their application.

- Double taxation treaties do not provide for the right to choose the jurisdiction where the tax is to be paid. Payment of tax on dividends in the state of the recipient of income does not exempt from payment of tax in the state which is the source of income on the basis of rates indicated on the respective treaty.

- Termination of the foreign shareholder's participation in a Russian company by the time the dividends are paid does not prevent application to such dividends of a reduced tax rate provided in the double taxation treaty, if the decision on their payment was taken before the termination of participation.

- The foreign shareholder, which contributed the necessary amount of investment into the share capital of a Russian company, does not lose the right to apply a reduced tax rate to dividends provided for by a double taxation treaty if it mergers with another foreign company.

- The amount of contribution into property of a Russian company by a foreign participant can be taken into account for the purposes of applying a reduced tax rate to dividends at source in Russia.

- Tax benefits provided for by international treaties are not granted in respect of cross-border transactions executed by its participants with the main purpose of receiving income solely or primarily by using the tax benefits (creating favorable tax conditions) in the absence of intention to carry out real economic activities.

- Absence of an apostille on the certificate of tax residency is not per se the basis for rejection in application of tax incentives under double taxation treaties, if there is a long-term practice between Russia and a foreign country which assumes mutual acceptance of such non-apostilled certificates and if the validity of the certificate can be confirmed by the tax authorities in the framework of mutual information exchange.

The generalization of practice by the Supreme Court has to promote uniform approach in judicial consideration of disputes involving foreign investors and increase the attractiveness of the Russian investment climate.

2. INTERNET AND TELECOM

2.1. Digital Technology Strategy In Russia

In July 28, 2017, the Russian Government approved a program called "Digital Economy of the Russian Federation". Among other things, the program defines the main aspects of legal regulation of digital technologies [1].

The program features a list of steps aimed at creating a new legal framework, information infrastructure, provision of information security and personnel training.

It is the basic document that defines the main development directions for short-term legal regulation of digital technologies and the economy.

Legal significance of digital data

- Remote identity proofing for effecting legally significant actions
- Legal status of electronic communication
- Legal significance of digital data and paper-based media

Big data

- Regulation of big data processing and access
- Legal status and conditions for big data commercialization
- Differentiation of access rights to big data and user data

Internet of Things and Robotics

- Use of robotics and artificial intelligence
- Machine-to-machine communication standards
- Identification of user Internet of Things

Information Security

- Requirements for the stability and security of communication networks and equipment at important infrastructure facilities
- Requirements for the use of domestic equipment at data processing infrastructure facilities
- Criminalization of illegal cyber actions

The program also makes provisions for harmonization of legislation within the framework of the EAEU in accordance with the specified approaches.

Based on the formulated tasks and established deadlines, it can be concluded that players in the IT market should prepare for the emergence of a new regulation in the near future.

[1] Executive Order No. 1632-r of the Government of the Russian Federation dated July 28, 2017

2.2. Latest initiatives on Internet regulation in Russia-2017

One may see an increase of attention and governmental control over IT sphere in Russia in recent years. A number of laws applicable to the Internet regulation were enacted, which gave a rise to various discussions in IT community and among ordinary users.

In July 2017, the Russian Government approved a program called "Digital Economy of the Russian Federation" aimed at creating a new legal framework, regulating the IT sphere including the national Internet segment, the creation of information infrastructure, ensuring cyber security, etc. Some of the adopted laws have not come into force yet. Besides, there are some initiatives under consideration and discussion that are worth paying attention to. Below we listed the most significant from our point of view new laws and initiatives in this area.

Adopted laws

1. Restriction on the use of anti-blocking services

Comes into force since 1 November 2017[1].

- Anti-blocking services including VPN based resources allowing to obtain access to the blocked Russian websites will be prohibited.
- The owners of such resources will be obliged to liaise with Roskomnadzor, which includes providing necessary information in response to the relevant request.
- The law establishes an exception for commercial use of VPN provided that such use is carried out by a limited number of users and is driven by the technical need.

2. Mandatory identification of instant messenger (IM) users

Comes into force since 1 January 2018[2].

- IM operator shall transmit messages of the users preliminarily identified by applying subscriber's number, based on a special identification agreement concluded between IM operator and communications provider.
- IM operators will be obliged to ensure the technical and legal capability of the identification.

3. Security of critical information infrastructure

Comes into force since 1 January 2018[3].

Critical information infrastructure objects (CIIO) are identified as information and process control systems, including the defense industry, transport, communications, and the financial sector.

The main areas of regulation include:

- requirements of ensuring CIIO security;
- preventing illegal access to CIIO information;
- interacting with the state system of detection, prevention and mitigation of computer attacks consequences on the Russian information resources.

4. Obligations of communication providers and operators provided for in the counterterrorism legislation

Comes into force since 1 July 2018[4].

Communication providers and operators will be obliged to store text messages, voice information, images, sounds, video, and other messages of communication services users for up to 6 months from the end of their reception, transmission, delivery and (or) processing. At the same time, the order, specific terms and the volume of storage has not been established by the Russian Government yet.

Legal initiatives

1. The defense of the Russian Internet segment

The draft law has passed public discussion[5].The Ministry of Communication has prepared the draft law aimed at increasing degree of protection of the Russian Internet segment from foreign

interference. The draft law provides, in particular, the connection of the subscribers of Internet access services only via traffic exchange points included in the special state register. The share of foreign participation in companies owning such points on the territory of the Russian Federation is proposed to be limited to 20%.

2. Obligation of social network operators to delete illegal information

The draft law is under consideration by the State Duma[6]. The draft law obliging social network operators to delete illegal information, including the information intended to promote war and incite hatred, inaccurate information and the information that defames any person or that person's reputation, has been introduced into the State Duma.

3. Control over displaying links to the prohibited websites by search engines

The draft order is undergoing public discussion[7]. The Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) has developed a draft order providing for the control over the abidance of the search engine operators, distributing advertisements, by the obligation to limit displaying links to websites, the access to which is limited or prohibited in the Russian Federation.

4. Transfer of users' data to law enforcement agencies

The draft order is undergoing public discussion[8]. The Ministry of Communications and Mass Media of the Russian Federation (Minkomsvyaz) has published a draft order obliging operators to use equipment ensuring the storage of the internet users' information. The list of the data to be fixed by means of such equipment includes users' personal data, information about accounts, IP addresses, information about effected payments as well as data exchanged by a user with other users in social networks. Such information will be provided to law enforcement agencies during investigation operations.

Preliminary conclusions

As evidenced by the laws and initiatives discussed above, the government is intending to lay down the rules of the game in the sphere, where there was no to little detailed legal regulation until recently. It is anticipated that in the next few years the legislation in new spheres of IT economy, regulating conditions for circulation and commercialization of Big Data, introduction of legal status of user data, standardization of IoT, etc. will be introduced. At the same time, it is already clear that as a result of most of these legislative measures market participants will incur considerable costs associated with changing their business models and fulfilling obligations placed on them (e.g. the obligation to store information). The expert community repeatedly pointed out that a number of initiatives needed to be polished both in terms of compliance with the effective legislation and in terms of business burden-sharing. Provided that a considerable part of the adopted laws and pending draft laws contains just references to important regulation issues

(which are yet to be developed), its influence on IT sector could be finally assessed only after adoption of the relevant regulatory framework.

[1] Federal law dated 29 July 2017 No. 276-FZ "On amending Federal law "On information, information technologies and data protection".

[2] Federal law dated 29 July 2017 No. 241- FZ "On amending Articles 10.1 and 15.4 of the Federal law "On information, information technologies and data protection".

[3] Federal law dated 26 July 2017 No. 187-FZ "On the security of the critical information infrastructure of the Russian Federation".

[4] Federal law dated 6 July 2016 No. 374-FZ "On amending Federal law "On the counteraction of terrorism" and certain legislative acts of the Russian Federation with regard to establishing additional measures designed to counteract terrorism and promote public security".

[5] Draft law "On amending Federal law "On communications".

[6] Draft law No. 223849-7 "On amending Article 10.1 of the Federal Law "On information, information technologies and data protection".

[7] Draft order of Roskomnadzor "On adoption of a procedure for controlling termination on the territory of the Russian Federation of provision of information about information resources, information and telecommunication networks access to which is limited on the territory of the Russian Federation, by search engine operators, disseminating advertisements in the Internet attracting attention of customers, residing in Russia".

[8] Draft order of the Ministry of Communications "On adoption of requirements to equipment and hardware and software used by the organizers of dissemination of information in the Internet in information systems operated by them, ensuring performance of particular actions during search operations, including storage system".

3. BANKING, FINANCE AND FINTECH

3.1. The Bank of Russia confirms its harsh position towards cryptocurrency

The Bank of Russia on 4 September 2017 published the announcement confirming its legal position regarding cryptocurrency, initially stated in 2014.

The Bank of Russia pointed out the following characteristics of cryptocurrency:

- the absence of legal framework;

- the absence of governmental guarantees;
- anonymous nature.

The Bank of Russia pays attention to the risk of involvement of cryptocurrency transactions participants in money laundering and terrorism financing activity.

The press release also designates particular risks of cryptocurrency exchange operations and attraction of investments through ICO (Initial Coin Offering):

- financial risks due to exchange rate fluctuations;
- technological risks of issuance and circulation of cryptocurrency;
- risks of recording rights to cryptocurrency.

According to the Bank of Russia, the abovementioned risks may result in financial losses of individuals as financial services consumers as well as the impossibility of their rights protection.

Therefore, the Bank of Russia considers the admission of cryptocurrency and any similar financial instruments to on-exchange trading as well as clearing and settlement infrastructure of the Russian Federation as premature.

At the same time, many jurisdictions provided for the regulation of cryptocurrency and transactions therewith, including ICO. For instance, the U.S. applies the existing securities laws to ICO, *de facto* providing ICO with the same status as IPO. The similar position was expressed by the Monetary Authority of Singapore.

In its recently published report the People's Bank of China assumed conservative approach indicating that ICO is illegal, therefore the Bank demanded immediate termination of all related fundraising activity.

Despite the fact that the announcement of the Bank of Russia is not a regulatory legal act and, consequently, is not mandatory, it demonstrates, though, the government's cautious attitude towards cryptocurrency.

We believe that the state authorities will take this position into account till the adoption of the law which is expected to regulate cryptocurrency and the terms of its circulation.

3.2. Securities regulations may apply to initial coin offering (ICO) in USA

On 25 July 2017 the United States Securities and Exchange Commission (SEC) published a report on investigation of the case on initial coin offering (ICO) of The DAO, a decentralized autonomous organization, containing several significant conclusions.

SEC noted that depending on the facts and circumstances, the securities laws including Securities Exchange Act of 1933 and Securities Exchange Act of 1934 may apply to cryptocurrency transactions.

Each offer and sale of securities in the U.S. must comply with the federal laws regardless of technology of placement and method of payment. In The DAO case SEC concluded that the tokens issued through ICO are deemed as securities.

According to the U.S. legislation, a "security" includes "an investment contract", which is an investment of money in a common enterprise with a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others. The DAO tokens were qualified as such investment contract.

In the context of The DAO case it is important to highlight the following conclusions made by SEC:

- "contribution" or "investment" is not limited to transfer of cash, since the tokens were purchased with ETH cryptocurrency;
- reference to investors' potential profits in promo-materials is sufficient for determining the aim of the investment;
- investors' profits derived from the managerial efforts of third parties, as the investors had no influence on decisions on company's funds disposal;
- decentralized autonomous organization (even not registered as a legal entity) may be recognized as a securities issuer.

In case tokens (other "digital assets") are considered as securities, an issuer is obliged either to obtain a relevant legal status or operate pursuant to the exemptions provided by the law.

SEC also issued a special bulletin for potential ICO participants. According to it, investors should pay their attention to the following:

- project's business-plan and white paper;
- anticipated expenditures of raised funds;
- rights provided by a virtual coin or token.

Therefore, recognition of tokens as securities will depend on the facts of particular case, as well as on discretion of SEC. Herewith, the broad wording of security's (investment contract) attributes applied to The DAO tokens are common for most tokens being issued by ICO.

It seems that the SEC approach will facilitate application of securities laws to majority of the U.S. based ICOs. Which is likely to result in increase of costs and decrease of market activity. In this situation jurisdictions having the regulatory framework (e.g., Japan) or finishing its establishment (e.g., Singapore, Switzerland) could become more attractive for organizing new ICOs.