NEW LEGISLATION REGULATING CYBER SECURITY AND THE INTERNET IN RUSSIA

This summer Russia has passed three new cyber-security and Internet laws:

(1) Federal Law No. 187-FZ "On the Security of the Russian Federation's Critical Data Infrastructure", which introduces requirements for infrastructure security (the "**CDI Law**");

(2) Federal Law No. 276-FZ "On Amendments to the Federal Law "On Data, Information Technologies and Data Security", which regulates the technologies that can be used to access restricted websites in Russia (the "**VPN Law**"), and

(3) Federal Law No. 241-FZ "On Amendments to Articles 10.1 and 15.4 of the Federal Law "On Data, Information Technologies and Data Security", which introduces specific regulations for instant messaging service providers (the "**IM Law**").

This briefing provides an overview of these laws.

Key issues

CDI Law

- The CDI Law introduces specific security regulations for CDI Facilities in important sectors of the Russian economy;
- Owners will be obligated to evaluate how important their CDI Facilities are and, if required, to have them put on a government register;
- Owners of Important CDI Facilities have to comply with additional security requirements and cooperate with governmental agencies in preventing and investigating cyber-incidents.

VPN Law

- VPN solutions providers have to cooperate with the government and block users' access to websites that may not be accessed from Russia.

IM Law

- The anonymous use of IM is being prohibited;
- IM Providers will have to identify IM users by their mobile numbers.

CDI LAW

The main purpose of the CDI Law is to ensure that Russia's critical data infrastructure[1] is secure and stable in the face of cyber attacks[2]. The CDI Law will come into force on 1 January 2018; the implementing regulations have yet to be adopted by the Russian executive authorities. However, when the regulatory framework is fully in place, it will have an impact upon the majority of market participants.

1 The CDI Law defines "**critical data infrastructure**" as "*critical data infrastructure facilities and telecommunications networks used for the interaction of such facilities*".

2 The CDI Law defines "**cyber-attack**" as "a *targeted attack, through software and/or firmware applications, on critical data infrastructure facilities or the telecommunications networks used for the interaction of such facilities, intended to make them malfunction or stop working and/or to create a threat to the security of the data processed by the data facilities*".

The CDI Law imposes certain obligations upon Russian entities and (or) individual entrepreneurs ("**CDI Operators**") that own, lease or have other legal rights to critical data infrastructure facilities[3] operating in one of the following areas: (i) healthcare, (ii) science, (iii) transport, (vi) communications, (v) energy, (vi) banking and other sectors of financial markets, (vii) oil & gas, (viii) nuclear, (xi) defence, (x) rocket and space, (xi) mining, (xii) metals and (xiii) chemical industry ("**CDI Facilities**").

Each CDI Operator is obligated, among other things, to:

- inform the federal agency (the "**Agency**")[4] and the Central Bank of the Russian Federation (if the CDI Operator operates in banking or other sectors of financial markets) immediately of any "cyber-incident"[5];
- cooperate with the Agency with respect to (1) the detection, prevention or remedying of cyber-attacks and (2) determination of the causes and circumstances of cyber-incidents.

In addition to the above, the CDI Law provides that each CDI Operator is under an obligation to evaluate the "importance" of the CDI Facilities that it owns, leases or has other legal rights to in order to determine whether the CDI Facility should be classed as what is called an "important critical data infrastructure facility" ("**Important CDI Facility**"), and, if so, which level of importance needs to be assigned to it. The Russian Government has yet to adopt specific rules for these evaluations[6] but the evaluative criteria will relate to:

- social importance: possible damage to people's lives and health or possible malfunctions or stoppages in life-supporting infrastructure facilities, the transport infrastructure or telecommunications networks or the unavailability of public services in excess of the maximum period permitted;
- political importance: possible damage to the interests of the Russian Federation in matters relating to its foreign or domestic policy;
- economic importance: potential direct or indirect damage to CDI Operators and (or) the budgets of the Russian Federation;
- ecological importance: impact on the environment; and
- importance for national defence and law and order.

The CDI Operator must within 10 days following completion of the evaluation, submit the results to the federal agency for security of the critical data infrastructure of the Russian Federation (the "**Security Agency**")[7]. The Security Agency independently reviews the evaluation and, if it finds that the CDI Facility is an Important CDI Facility, it will put it on the register of important critical data infrastructure facilities that the Security Agency keeps (the "**Register**").

Once an Important CDI Facility is on the Register, the CDI Operator will have additional obligations under the CDI Law. These include:

---

3 Critical data infrastructure facilities include the (1) data systems, (2) data and telecommunications networks, and (3) automated control systems of CDI Operators.

4 The federal agency responsible for ensuring the functioning of the state system for identifying, preventing and remedying cyber-attacks on the Russian Federation's data resources. The competent authority is yet to be appointed.

5 The CDI Law defines "**cyber-incident**" as "*malfunction or stoppage of a critical data infrastructure facility or telecommunications network used for the interaction of such facilities, and/or a breach of the security of the data processed by such facilities, including as a result of a cyber-attack*".

6 The draft of the regulation is available at http://regulation.gov.ru/projects#npa=73423.

7 The competent authority is yet to be appointed.

- complying with security regulations for Important CDI Facilities (the "**Security Regulations**")[8];
- complying with orders from the Security Agency to rectify violations of the Security Regulations;
- responding to cyber-incidents in accordance with the procedures adopted by the Agency and taking steps to remedy cyber-attacks on Important CDI Facilities; and
- providing unrestricted access to Important CDI Facilities for audits conducted by the Security Agency.

CDI Operators' compliance with requirements under the CDI Law will be monitored by the Security Agency through scheduled and unscheduled audits. Scheduled audits will take place every three years. Unscheduled audits will be carried out in the circumstances specified in the CDI Law (for example, in the event of a cyber-incident with negative consequences for an Important CDI Facility).

CDI Operators' officers may be criminally prosecuted for violations of (1) the operating rules for facilities for storing, processing and transferring data within the critical data infrastructure, CDI Facilities or telecommunications networks or (2) the rules for accessing such data, CDI Facilities or telecommunications networks, if the violation has resulted in damage to the critical data infrastructure. There is no specific administrative liability for such violations but the Russian Administrative Offences Code includes a general clause imposing administrative liability for violations of data security requirements, which envisages fines for officers and Russian companies.

VPN LAW

The VPN Law will take effect on 1 November 2017. Federal Law No. 149-FZ "On Data, Information Technologies and Data Security" restricts access to certain data resources and data and telecommunications networks in Russia ("**restricted websites**"). Under the VPN Law, the owners of data and telecommunications networks and data resources that can be used to access restricted websites ("**VPN technology**") are prohibited from providing users of VPN technology ("**users**") with support to access restricted websites. The use of VPN technology is not prohibited but the VPN Law imposes certain obligations on (1) the owners of VPN technology ("**owners**"), (2) hosting providers and other persons providing for the distribution of VPN technology on the Internet ("**hosting providers**") and (3) the operators of internet search-engines that publish advertisements for customers in Russia ("**search-engine operators**").

The Federal Agency for Communications, Information Technology and Mass Media ("**Roskomnadzor**") is responsible for monitoring compliance with the VPN Law. To this end, it will maintain a federal state database of data resources and data and telecommunications networks access to which is restricted in Russia (the "**Database**").

The owners will be obligated to join the Database no later than 30 days from receipt of a request from Roskomnadzor[9]. Roskomnadzor can identify an owner by itself or through a request to the hosting provider. Upon a request from Roskomnadzor, the hosting provider has an obligation to (1) disclose the details of the owner or (2) notify the owner that it must disclose its details on its Internet website. Search-engine operators also must join the Database. Once the owners or search-engine operators are in the Database, they must block users' access to restricted websites within 3 days.

---

8 The Security Regulations have yet to be developed by the Security Agency. Security requirements will differ according to the category of importance assigned to the Important CDI Facility in question.

9 The draft of the regulation setting down the procedure for joining the Database is available at http://regulation.gov.ru/projects#npa=71495.

If the owner fails to, among other things, (1) join the Database within the required period or (2) block users' access to restricted websites, Roskomnadzor will block access to the web-sites through which the VPN technology is distributed to users until the violations are rectified.

It is also important to note that the requirements of the VPN Law do not apply to the use of VPN technology where (1) the users are predetermined by the owner and (2) the VPN technology is used in order to support users' businesses.

IM LAW

From 1 January 2018, the anonymous use of instant messaging ("**IM**") will be prohibited and IM service providers ("**IM Providers**") will have certain obligations under the IM Law.

The main obligation of IM Providers will be to identify IM users by their mobile numbers. For this purpose, IM Providers must enter into an agreement with mobile operators allowing IM users to be identified. Russian IM Providers are allowed to identify IM users without any assistance from mobile operators. IM Providers must store data relating to the identification of IM users' mobile numbers in the Russia Federation only.

IM Providers are also obligated to:

- upon receiving a request from the relevant Russian authority, block the messages of the relevant IM user that contain information (i) the distribution of which is prohibited in Russia or (ii) which is distributed in violation of provisions of Russian law;
- provide IM users with the technical ability to reject messages from other IM users;
- ensure the privacy of IM messages;
- allow messaging at the request of the Russian authorities under Russian law; and
- block messages sent to IM users in the cases stipulated by and in accordance with the procedures set down by Russian law.

If IM Providers fail to perform their obligations under the IM Law, their IM applications may be blocked by a Russian court.

CONTACTS

Alexander Anichkin
Partner

T +7 495258 5089
E Alexander.Anichkin
@cliffordchance.com

Evgeny Soloviev
Counsel

T +7 495 725 6420
E Evgeny.Soloviev
@cliffordchance.com

Ekaterina Makarova
Senior Associate

T +7 495 725 6435
E Ekaterina.Makarova
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, Ul. Gasheka 6, 125047 Moscow, Russia