

Ilya Goryachev Senior Lawyer
 goryachev@gorodissky.ru
 Gorodissky and Partners, Moscow

Russia introduces new rules on VPNs and anonymisers

Many users and businesses utilise anonymising technologies, such as virtual private networks ('VPNs'), in order to increase privacy and security on their systems, but in Russia, from 1 November 2017, new rules aimed at establishing greater control over the use of VPNs, other anonymisers and technology that redirects Russian internet traffic through foreign servers will enter into force. These new rules introduced via Federal Law No. 276-FZ (the 'Amending Law'), which introduces amendments to Federal Law No.149-FZ on Information, Information Technologies and the Protection of Information. Ilya Goryachev, Senior Lawyer at Gorodissky and Partners, assesses the specifics and implications of the Amending Law, and considers what prompted the Russian Government to introduce the amendments that grant new powers to Russia's IT, mass media and telecommunications regulator Roskomnadzor.

What are the reasons for the rules?

On the whole, the Amending Law may be treated as part of the ongoing trend to regulate the online flow of information in Russia. With the level of restriction varies, trends exist in various jurisdictions, and Russia is no exception.

But specifically, the Amending Law may also be viewed as part of the initiative to ensure that administrative and court decisions relating to blocking specific categories of websites are enforced. In Russia, various websites may be blocked due to reasons such as child pornography, the promotion of suicide, extremist content, IP rights infringement, personal data violations, etc.

The Amending Law does not ban the use of VPNs and anonymisers for legitimate purposes that do not involve access to such blocked websites, so in this regard, the Amending Law restrictions do not apply to VPN and other related technologies when utilised by businesses for legitimate needs (e.g. to establish access to corporate databases for employees, etc.).

The Amending Law bans the use of such technologies to obtain access to blocked websites, and encourages

the owners of anonymiser/VPN/ internet traffic direction technologies to cooperate with Roskomnadzor in preventing access to such websites.

At the stage when the draft Amending Law was being considered, after it was submitted to Parliament, there was an Explanatory Note on the draft, which highlighted the official reasons behind the necessity of the law. Namely, these included:

- The possibility of finding links to blocked websites through search engine results;
- The possibility of using technologies that allow users to obtain access to blocked informational resources;
- Operators of search engines are not obliged to terminate the delivery of search results to blocked websites;
- In order to obtain access to websites blocked in Russia, there are technologies used to direct the traffic of Russian internet users via foreign servers, anonymous proxy servers, VPNs, etc.;
- No ban currently exists that prevents the use of technologies which facilitate access to blocked websites in Russia. However, access to some websites, which allowed

'bypass blocking,' was restricted under Russian court decisions;

- Technologies that direct Russian internet users via foreign servers, anonymous proxy servers, and VPNs are legal, and;
- Despite the vast range of possibilities for using such technologies for legitimate needs, they are nevertheless used for accessing blocked resources.

The purpose of the measures under the Amending Law according to the Explanatory Note was determined to be 'for the purpose of increasing efficiency of restricting access to the information sources, access to which is legitimately blocked in Russia, with account of possibilities of legitimate use of technologies, used to "bypass blockings."'

Therefore, from the Explanatory Note, it is clear that the purpose of the Amending Law was not to eliminate technologies that redirect Russian internet users via foreign servers, anonymous proxy servers, and VPNs as such, but rather to eliminate the conditions under which such technologies may be used to obtain access to blocked websites in Russia.

What is the essence of the new rules?

The Amending Law introduces Article 15.8 to Federal Law No. 149-FZ on Information, Information Technologies and the Protection of Information.

The new requirements are as follows:

- Owners of IT networks and information resources (websites, information systems, software, herein referred to as 'Technologies') through which access to the blocked information resources in Russia is permitted are forbidden from providing the possibility to use the technologies to obtain access to the blocked websites;
- Roskomnadzor, in order to prevent the use of the Technologies to obtain access to the blocked information resources in Russia, is entitled to:

- (i) Keep a register of the blocked information resources and networks (the 'Register');
- (ii) Cooperate with criminal investigation authorities to obtain information on the Technologies that could grant access to the blocked websites;
- (iii) Send a request to the internet service provider, or another person providing an internet service, that ensures the provision of information about the owner of the Technologies, or that informs the owner of the Technologies of the necessity to publish such information on their website; and
- (iv) File a request to the owner of the Technologies to connect to the Register within three business days after Roskomnadzor obtains the information on the owner as per the request above;

- Within 30 business days of the above request, the owner of the Technologies is obliged to connect to the Register. At Roskomnadzor's request, such a connection shall also be required by the search engine operator, disseminating advertising to Russian users;
- Within three business days since access to the Register is granted, the owner of the Technologies is obliged to ensure that those Technologies are not used to obtain access to the blocked sites. The owner of the Technologies is also obliged to comply with Roskomnadzor's requirements on using the information in the Register;

- In case the owner of the Technologies does not connect to the Register and does not comply with the above obligations, Roskomnadzor has the power to restrict access to the Technologies (by ensuring the internet service providers restrict access). The owner of the Technologies may seek renewed access, if the owner of the technologies complied with the obligations and notified Roskomnadzor; and
- The Amending Law also provides obligations for search engine providers.

Various by-laws necessary for the Amending Law to operate are expected.

Exceptions to the Amending Law

It is also of importance that the Amending Law states those cases where the restrictions do not apply, namely:

- To the operators of state information systems, state authorities and local government authorities; and
- Cases where the Technologies are used on condition that users of such Technologies are determined in advance by the owner, and the use of the Technologies takes place for technological purposes that require active use of the Technologies by users. That exception covers the use of the Technologies for legitimate purposes by businesses (herein referred to as 'Corporate Technologies').

Potential implications

Companies who use the Technologies will need to cooperate with Roskomnadzor.

Even with the Amending Law excluding Corporate Technologies, there is a potential risk that companies will be engaged in using both the Technologies that may be used by everyone (e.g. a VPN application available from a mobile store) and the Corporate Technologies.

Such cooperation with Roskomnadzor is particularly important for those IT companies that provide corporate VPNs and other similar solutions to businesses in order to avoid negative commercial consequences.

Non-compliance with the Amending Law requirements may result in the termination of access to the contracted

VPN services. In this regard, businesses that use corporate VPN services also need to exercise caution in selecting the VPN service provider. The relevant provisions dealing with the risk of the specific Technologies being forbidden may be introduced in service agreements with IT solution providers.

Furthermore, the practice of enforcing the Amending Law may also lead to increased attention by the regulator to the websites and other resources that may contain the information regarding the use of the Technologies.

As noted above, businesses that utilise Corporate Technologies are exempted from the Amending Law. However, the wording of the Amending Law in this regard is general. In practice, there may be difficulties in distinguishing between the Technologies and Corporate Technologies.

As a guideline, it is advisable that companies stick to the wording of the Amending Law, which names two conditions under which the Corporate Technologies are exempted: i) if a pre-determined list of users is provided; and ii) where the Technologies are only used for technological purposes. In this regard, to be on the safe side and as part of a proactive approach, the following recommendations may be followed:

- Businesses need to have an official list of employees that have access to the Corporate Technologies. Such a list may serve as evidence that 'users of such Technologies are determined in advance by the owner;' and
- Internal employment policies need to have a provision forbidding employees from using the Corporate Technologies to gain access to the web resources blocked under the Russian legislation. That may serve as evidence that 'use of the Technologies takes place for technological purposes to ensure activity of the person that uses the Technologies.'

In conclusion, the Amending Law does not ban the use of the Technologies for business, corporate and other legitimate uses. It shall rather serve as a necessary tool to ensure that access to banned websites (including those involved in the infringement of IP rights) is legitimately restricted.