The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Blacklist of Sites Is Already a Reality

By The Moscow Times

November 27, 2012



On Nov. 1, 2012, the Russian Government's Resolution No. 1101 dated Oct. 26, 2012 came into force. It approved the rules for creating, compiling and maintaining the unified automated information system that contains details of domain names, website page indexes and network addresses allowing sites to be identified in the Internet that contain information which it is prohibited to distribute in Russia (The full title is the "Unified register of domain names, website page indexes in the Internet information and telecoms network, and network addresses allowing sites to be identified in the Internet information and telecoms network, that contain information forbidden to be distributed in Russia").

The resolution was adopted in pursuance of article 15.1 of Federal Law No. 149-FZ dated July 27, 2006 On information, information technologies and the protection of information (the Information Law). This provision came into being because legislation was reformed in the area of protecting children from information that damages their health and development.

Both the amendments to legislation and the resolution were the subject of heated debate among those who were to be regulated by them. Among those affected (along with particular

state authorities) are the owners of websites, website hosting services who ensure that sites are available via the Internet, and telecoms operators providing Internet access to their users.



Natalia Ivaschenko

Head of the Telecoms Group, PhD in Law
Pepeliaev Group

All those affected have, in one way or another, agreed that it is necessary to fight against unlawful content. Nonetheless, there are big question marks over whether the methods currently enshrined in legislation are actually effective.

We will attempt to assess whether the Unified Register (the so-called blacklist of sites) solves the problem of unlawful content being distributed.

The Unified Register's website at http://zapret-info.gov.ru/ contains a search system that allows a check to be made of whether an IP address or domain name is in the Register. On the same page, a message can be left about a resource containing forbidden information, and this will be checked out by the regulator Roscomnadzor before the resource is added to the Register. Users have been able to access this webpage since 1 November 2012, i.e. as soon as the amendments to legislation came into effect.

How do domain names, website page indexes and network addresses come to be included in the Register? Within 24 hours of the grounds for doing so occurring, they are included in the Register by Roscomnadzor (a private company that, along with Roscomnadzor, may also includes this information in the Register in the capacity of the operator of the Register, if such company is found to meet the criteria imposed by the Resolution). The grounds for an

entry to be made in the register are:

a court decision which has come into legal force that information distributed via the Internet is prohibited information;

a decision of a duly authorized body that information should be deemed prohibited (the Federal Narcotics Control Service for information relating to the circulation of narcotic substances; Rospotrebnadzor for information about ways to commit suicide as well as encouragement to commit suicide; and Roscomnadzor for information that may be classed as prohibited under the law).

A duly authorized body must take such a decision within 24 hours of the time when a communication directly reaches it, or when a request from Roscomnadzor (or the operator of the Register) reaches it. A 24-hour time limit from when a communication or contact is received also applies for Roscomnadzor to send a request to the duly authorized body.

The maximum timeframe for an entry to be made in the Register when it is confirmed that information is prohibited is 3 days from when contact is received from any person or body.

At the same time as information is included in the Register, the identity is determined of the website hosting service that allowed the site in question to be placed on the Internet, and a notice is sent to that party. It is important to be aware that the site owner must be notified not by Roscomnadzor but by the website hosting service. The site owner and/or the hosting service will be given 3 days to delete the prohibited information and/or restrict access to the site with unlawful content.

In addition, obligations are imposed on telecoms operators to monitor updates to the Register (such updates are made every day between 9.00 and 21.00), and to restrict access to sites included in the Register within 24 hours of the relevant update. It is noteworthy that neither site owners nor hosting services have such a monitoring obligation.

Telecoms operators have an automatic obligation to block access to a site if the owner and hosting service have not taken the appropriate steps and a network address that allows the site with prohibited information to be identified has been included in the Register.

This means that telecoms operators are the ultimate links in the chain of persons who are obliged to fight against unlawful content.

Interestingly, neither article 15.1 of the Law on Information nor the Resolution contains a reference to the method of blocking access to unlawful content. Therefore, as things stand, operators can only proceed on the basis of what technology makes possible for them. Not all Russian telecoms operators by a long way currently have the ability to use Deep Packet Inspection (DPI), i.e. technology for gathering statistical data that checks and filters network packets by their content. This technology means that information that does not comply with the criteria can be filtered on a deep level. However, it is rather costly, and in practice operators have the technical ability to block access, albeit to a resource as a whole rather than to defined content within the resource.

When the courts have heard cases relating to disputes between the prosecutor's office

and telecoms operators, they have assessed an argument from operators that it is technically possible to restrict access to specific pages of a site on DNS-servers only if access to the whole site is restricted, which contravenes current legislation, the constitutional freedom to distribute information and contravenes the rights of a broad spectrum of the telecoms operator's users of telematics services (Appeal Ruling of the Samara Region Court dated 4 October 2012 in case No. 33-9233/2012.). As a rule, the courts do not accept this argument: they believe that the telecoms operators must take steps to restrict access to the above websites by virtue of the law (for example, the Federal Law On protecting children from information that causes harm to their health and development).

Courts follow different approaches when they hear disputes regarding the method for restricting access when telecoms operators have the obligation to restrict access to an internet resource: in some cases, it is stated that the method by which the obligation is performed has no relevance in terms of resolving the dispute (Appeal Ruling of the Tyumen Region Court dated 5 September 2012 in case No. 33-3971/2012.), while in other cases an operator is obliged to restrict access to specific websites by adding rules for filtering IP addresses at the border router (Appeal Ruling of the Moscow City Court dated 10 July 2012 in case No. 11-10809.).

Whether there will be further developments on the issue of blocking access to prohibited information, only time will tell. Without a doubt, not all players on the market welcome the idea of blocking access to the resource as a whole rather than to particular content.

In conclusion, we should note that the Law on Information and the Resolution have set a procedure for excluding from the Register a domain name, a website page index and a network address that allows a site to be identified on the Internet. An obligation is imposed on Roscomnadzor (or on the operator of the Register) to exclude the relevant entry from the Register: (a) within three days of being contacted by a website owner, a hosting service or telecoms provider after measures have been taken to delete information distribution of which is prohibited in Russia; or (b) within three days of a court ruling coming into legal force that sets aside a previous decision of Roscomnadzor regarding an entry in the Register.

Despite there being insufficient regulation of the aspects described above and the potential for disputes to arise, there is no doubt that the creation of the register is a useful step in the fight against prohibited information.

Original url:
https://www.themoscowtimes.com/2012/11/27/blacklist-of-sites-is-already-a-reality-a19728