Russia: Reject "Sovereign" Internet Bill

International Partnership for Human Rights (IPHR), together with 9 human rights, media and Internet freedom organisations, calls on Russian President Vladmir Putin, not to sign the so-called "Sovereign Internet Bill" as it will lead to further limitations of already restricted Internet and media freedoms in the country.

The bill (No. 608767-7) amends the laws "On Communications" and "On Information, Information Technologies and Information Protection" and states its aim as enabling the Russian Internet to operate independently from the World Wide Web in the event of an emergency or foreign threat. On 16 April 2019, the Russian State Duma approved the bill in the third reading amid widespread domestic criticism, protests and *online campaigning* around the country, and on 22 April, the Federation Council, the upper house of the Russian parliament, approved it. If signed by President Vladimir Putin, the bill would enter into force on 1 November 2019.

The bill creates a system that gives the authorities the capacity to block access to parts of the Internet in Russia, potentially ranging from cutting access to particular Internet Service Providers (ISPs) through to cutting all access to the Internet throughout Russia.

The bill gives control over Internet network routing to the state regulator for Telecommunications, Information Technologies and Mass Communications, Roskomnadzor. It provides that the Internet Service Providers (ISPs) should connect with other ISPs, or "peer," at Internet exchange points (IXes) approved by the authorities, and that these IXes should not allow unapproved ISPs to peer. The bill would also create a centralised system of devices capable of blocking Internet traffic. The bill requires ISPs to install the devices, which the government would provide free of charge, in their networks.

Under this system, Roskomnadzor would monitor threats to Russia's Internet access and transmit instructions to ISPs through the special devices about countering these threats. Cross-border Internet traffic would be kept under close state control. The draft does not specify what the range of instructions would be, but they could potentially include partially or fully blocking traffic both between Russia and the rest of the World Wide Web, and within Russia. Nor does the draft explain how the new equipment will work, or what specifically it will do. It is clear, however, that blocking would result from direct interaction between the government and the ISP and that it will be extrajudicial and nontransparent. The public would not know what has been blocked and why.

The bill states that the new measures will be activated in the event of a 'security threat'. The draft does not define security threats, and instead gives the government full discretion to decide what would constitute a security threat and what range of measures would be activated using the new system to address a threat.

The bill also states that Russian ISPs remain obligated to filter and block content in accordance with existing Russian law.

Further, the bill creates a national domain name system (DNS)— a system that acts as the address-book for the Internet by allowing anyone to look up the address of the server(s) hosting the URL of a website they are looking for. The bill would require Internet providers to start using the national DNS from 1 January 2021. Forcing ISP's to use the national system will give Russian authorities the ability to manipulate the results provided to the ISP outside the ISP's knowledge and control. Authorities will be able to answer any user's request for a website address with either a fake address or no address

at all. This not only allows them to conduct fine-grained censorship but will also let the national DNS to redirect users to government-controlled servers in response to any DNS requests instead of to a website's authentic servers.

These proposals are very broad, overly vague, and vest in the government unlimited and opaque discretion to define threats. They carry serious risks to the security and safety of commercial and private users and undermine the rights to freedom of expression, access to information and media freedom.

The bill contravenes standards on freedom of expression and privacy protected by the International Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR), to which Russia is a party. Both treaties allow states to limit freedoms to protect national security but impose clear criteria for such limitations to be valid. The UN Special Rapporteur on freedom of expression, commenting on the ICCPR, has reiterated that these limits should be *"provided by law, which is clear and accessible to everyone,"* and be predictable and transparent.

IPHR and other undersigned organisations are extremely concerned that the changes introduced in the bill threaten human rights and freedoms in Russia. Open, secure and reliable connectivity is essential for human rights online, including the rights to freedom of expression, information, assembly, privacy and media freedom. The bill could pose a threat to the Internet's rights-enabling features if access to the World Wide Web is wholly or partially cut off, or if arbitrary blocking and filtering of content is carried out. It would facilitate state surveillance and curb anonymity online. It also risks severely isolating people in Russia from the rest of the world, limiting access to information and constraining attempts at collective action and public protest. The Bill's negative impact on the freedom of expression will also affect the rights of journalists and media to work freely.

The adoption of the bill should be seen in the context of other Russian legislation that severely undermines protection of freedom of expression and privacy online and fails to meet international human rights standards. These include:

- The 2016 'Yarovaya Law,' which requires all communications providers and Internet operators to store metadata about their users' communications activities, to disclose decryption keys at the security services' request, and to use only encryption methods approved by the Russian government. It was adopted to allegedly counter 'extremism' but in practice, it creates a backdoor for Russia's security agents to access Internet users' data, traffic, and communications.

- In 2017, Federal Law 327-FZ made amendments to the 'Lugovoi Law' (Federal Law FZ-398, 2013) that gave the General Prosecutor or his/her deputies a right to block access to any online resource of a foreign or international NGOs designated 'undesirable'; and, to 'information providing methods to access' the resources enumerated in the 'Lugovoi Law', i.e. including hyper-links to old announcements on public rallies not approved by local authorities.

- *The recent March 2019 bills* mandate blocking and penalizing websites that publish what authorities deem to be "fake news" and "insult" to authorities, state symbols, and what the legislation vaguely describes as Russian "society."

The President of the Russian Federation should reject the bill. The Russian Government should also review other Internet related legislation, abolish the above listed laws and bring its legal framework to full compliance with international freedom of expression standards.

1. ARTICLE 19
2. Civil Rights Defenders
3. Committee to Protect Journalists
4. Human Rights Watch
5. International Federation for Human Rights (FIDH)
6. International Media Support
7. International Partnership for Human Rights
8. Norwegian Helsinki Committee
9. PEN International
10. Reporters without Borders