Mandates of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; and the Special Rapporteur on the right to privacy

REFERENCE:
AL RUS 7/2018

15 May 2018

Excellency,

We have the honour to address you in our capacities as Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; and Special Rapporteur on the right to privacy, pursuant to Human Rights Council resolutions 34/18 and 28/16.

In this connection, we would like to bring to the attention of your Excellency's Government information we have received concerning the Court decision on 13 April 2018 to allow Russia's federal media regulator, Roskomnadzor, to block Telegram over the latter's failure to grant the Russia Security Services their users' encryption keys.

Telegram is a global instant-messenger service, launched in 2013 in Russia. It is registered as both an English LLP and an American LLC.

According to the information received:

The legal authority to block websites is derived from the 2006 Federal Law "On Information, Information Technologies and the Protection of Information", and supplemented by the 2012 Federal Law 139-FZ "On Introducing Amendments to the Law on the Protection of Children from Information Harmful their Health and Development". The Government agencies mandated to authorize blocking and the permitted grounds for blocking have been expanded since 2012, through Federal Law 139-FZ; Federal Law 135-FZ; Law 149-FZ; and Federal Law FZ-398.

Article 15 of Federal Law 139-FZ established a blacklist, administered by the federal media regulator of the Russian Federation, Roskomnadzor. The content of websites added to the list is prohibited, and all internet service providers based in Russia are obliged to immediately block access to it. Roskomnadzor is empowered to block websites at the request of multiple government agencies without judicial oversight. In October 2015, the Federal Tax Administration was authorized to add sites to the blacklist without a court order.

Roskomnadzor is also responsible for blocking content included in the Federal List of extremist Materials established by Federal Law 114-FZ.

In June 2017, Roskomnadzor requested Telegram management to comply with Russian legislation or face blocking of its messenger application in Russia. Telegram agreed to register the service in Russia, but refused to abide by "laws incompatible with Telegram privacy policy".

In July 2017, Telegram received requests from the FSB (Federal Security Service of the Russian Federation) to provide information for decoding messages of six users of its app, which it said enabled terrorists to communicate with a high level of encryption. According to the FSB, Telegram was used by the suicide bomber and plotter of the terrorist attack in St. Petersburg's metro on 3 April 2017, which killed 15 persons and injured at least 45 others. In September 2017, law enforcement authorities initiated administrative action against Telegram due its refusal to comply with the request.

The Meshchansky District Court of Moscow fined the company 800,000 Russian Rubles (approximately 13,000 United State Dollars), for the refusal to provide the FSB with the information required to decrypt the messages of several users. Telegram has argued that it is technically impossible to transfer encryption keys. Telegram was found guilty of failure to store and furnish information on users and their messages to law enforcement agencies.

In December 2017, Telegram Messenger LLP filed a lawsuit in the Supreme Court of Russia seeking to cancel the FSB decree establishing the procedure for the provision of information on the decoding of user data. The lawsuit was dismissed on 19 March 2018, and the company was ordered to comply with the with the FSB order within 15 days. On 22 March 2018, Telegram filed an application to the European Court of Human Rights against the fine.

In early April 2018, the Presidential Council for Human Rights called on Roskomnadzor to refrain from blocking Telegram messenger and asked the FSB to find other ways of legal access to the messages of users that allegedly would endanger national security.

On 13 April 2018, the Tagansky District Court of Moscow issued a decision allowing Roskomnadzor to block access to Telegram messenger for the whole Russian Federation. The decision came into force immediately and Telegram started to be blocked as of 13 April 2018.

The court tasked Roskomnadzor with "putting a stop to sending and receiving messages" in Telegram until the messenger fulfils its obligations by providing deciphering keys.

We express concern at the court decision of 13 April to block Telegram across the Russian Federation, as this appears to represent an undue restriction on the right to freedom of expression, including access to information in the country. While governments enjoy a clear legitimate interest when it comes to public order and national security, the blocking must also satisfy the criteria of necessity and proportionality under article 19(3) of the International Covenant on Civil and Political Rights (ICCPR), ratified by the Russian Federation on 16 October 1973. In the case of the decision to block Telegram across Russia, it is not clear how this far-reaching measure can be deemed

necessary and proportionate for the protection of national security. Furthermore, we express concern about the underlying basis for blocking Telegram- the denial to grant the FSB the encryption keys of their users- and we would like to highlight that encryption allows for zones of privacy that enables all sorts of expression. Secure communications are fundamental to the exercise of freedom of opinion and expression in the digital age, permitting the maintenance of opinions without interference and securing the right to seek, receive and impart information and ideas.

In connection with the above alleged facts and concerns, please refer to the **Annex on Reference to international human rights law** attached to this letter which cites international human rights instruments and standards relevant to these allegations.

As it is our responsibility, under the mandates provided to us by the Human Rights Council, to seek to clarify all cases brought to our attention, we would ~~therefore~~ be grateful for your observations on the following matters:

1. Please provide any additional information and/or comment(s) you may have on the above-mentioned allegations.

2. Please provide information about how the decision to block Telegram is considered necessary and proportionate under articles 17 and 19 (3) of the ICCPR.

3. Please provide more information about the court decision of 13 April 2018

We would appreciate receiving a response within 60 days. Your Excellency's Government's response will be made available in a report to be presented to the Human Rights Council for its consideration.

While awaiting a reply, we urge that all necessary interim measures be taken to halt the alleged violations and prevent their re-occurrence and in the event that the investigations support or suggest the allegations to be correct, to ensure the accountability of any person(s) responsible for the alleged violations.

Please accept, Excellency, the assurances of our highest consideration.

David Kaye
Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

Joseph Cannataci
Special Rapporteur on the right to privacy

Annex
Reference to international human rights law

In connection with above alleged facts and concerns, we would like to draw your attention to articles 17 and 19 of the International Covenant on Civil and Political Rights (ICCPR), ratified by the Russian Federation ratified on 16 October 1973.

Article 19 guarantees the right to freedom of opinion and expression. Freedom of opinion is absolute, and no interference, limitation or restriction is allowed. Any restriction on the right to freedom of expression must be consistent with article 19(3) of the ICCPR, and thus be provided by law, be necessary in a democratic society and serve a legitimate government interest, namely for respect of the rights or reputations of others; for the protection of national security or of public order (*ordre public*); or of public health or morals.

While governments enjoy a clear legitimate interest when it comes to public order and national security, the blocking must also satisfy the criteria of necessity and proportionality under article 19(3).

The Human Rights Committee has stated that when a "State party invokes a legitimate ground for restriction of freedom of expression, it must demonstrate in specific and individualized fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat." (General Comment No. 34, para. 35.) In the case of the decision to block Telegram across Russia, it is not clear how this far-reaching measure can be deemed necessary and proportionate for the protection of national security.

Furthermore, Article 17(1) of the ICCPR provides for the rights of individuals to be protected, inter alia, against arbitrary or unlawful interference with their privacy and correspondence and provides that everyone has the right to the protection of the law against such interference. In this connection, Articles 17 and 19 of the ICCPR are closely connected, as the right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression (see A/HRC/23/40 and A/HRC/29/32).

With respect to the underlying basis for blocking Telegram- the denial to grant the FSB the encryption keys of their users- we would like to highlight to your Excellency's Government that encryption allows for zones of privacy that enables all sorts of expression. As highlighted by the Special Rapporteur on freedom of expression, secure communications are fundamental to the exercise of freedom of opinion and expression in the digital age, permitting the maintenance of opinions without interference and securing the right to seek, receive and impart information and ideas (A/HRC/29/32).

At the same time, as noted by the Special Rapporteur on freedom of expression in his the same report:

"13. The "dark" side of encryption and anonymity is a reflection of the fact that wrongdoing offline takes place online as well. Law enforcement and counter-terrorism officials express concern that terrorists and ordinary criminals use encryption and anonymity to hide their activities, making it difficult for Government to prevent and conduct investigations into terrorism, the illegal drug trade, organized crime and child pornography, among other government objectives. Harassment and cyberbullying may rely on anonymity as a cowardly mask for discrimination, particularly against members of vulnerable groups. At the same time, however, law enforcement often uses the same tools to ensure their own operational security in undercover operations, while members of vulnerable groups may use the tools to ensure their privacy in the face of harassment. Moreover, Governments have at their disposal a broad set of alternative tools, such as wiretapping, geo-location and tracking, data-mining, traditional physical surveillance and many others, which strengthen contemporary law enforcement and counter-terrorism." (AHRC/29/32).

Moreover, "[l]egislation must stipulate that State surveillance of communications must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority. Safeguards must be articulated in law relating to the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by the national law" (see A/HRC/23/40, para. 81). In addition to the normal rules that apply to surveillance, "a higher burden should be imposed in the context of journalists and others gathering and disseminating information" and in particular measures to "circumvent the confidentiality of sources of journalists, such as secret surveillance or metadata analysis, must be authorized by judicial authorities according to clear and narrow legal rules" (see A/70/361, paras. 24 and 62 respectively).

In addition, States are bound by the same duties and obligations under the ICCPR when they require or request corporate actors (both domestically and abroad) to participate in or cooperate with their surveillance activities (see A/HRC/23/40, para. 51). In particular, "States must not require or otherwise pressure the private sector to take steps that unnecessarily or disproportionately interfere with freedom of expression, whether through laws, policies, or extra-legal means." Further, "[a]ny demands, requests and other measures to take down digital content or access customer information must be based on validly enacted law, subject to external and independent oversight, and demonstrate [necessity and proportionality]" (A/HRC/32/38, para. 85).

In the context of mandatory third party data retention, the Special Rapporteur on freedom of expression has stated that "[t]he provision of communications data by the private sector to States should be sufficiently regulated to ensure that individuals' human rights are prioritized at all times. Access to communications data held by domestic corporate actors should only be sought in circumstances where other available less invasive techniques have been exhausted" (A/HRC/23/40, para. 85).

We should also note that Human Rights Council Resolution 32/13, adopted recently, "[c]alls upon all States to address security concerns on the Internet in accordance with their international human rights obligations to ensure protection of freedom of expression, freedom of association, privacy and other human rights online, including through national democratic, transparent institutions, based on the rule of law, in a way that ensures freedom and security on the Internet." The Special Rapporteur on freedom of expression has also concluded that States may only adopt those restrictions on encryption and anonymity, key security tools for individuals online, that "meet the requirements of legality, necessity, proportionality and legitimacy in objective." (A/HRC/29/32, para 57). States should "avoid all measures that weaken the security that individuals may enjoy online, such as backdoors, weak encryption standards and key escrows." On the other hand, regulations compelling targeted decryption may be permissible provided that they result from "transparent and publicly accessible laws applied solely on a targeted, case-by-case basis to individuals and subject to judicial warrant and the protection of due process rights of individuals" (A/HRC/29/32, para. 60).

The Special Rapporteur on the right to privacy has also consistently supported encryption as an "effective technical safeguard" that can, among other technical solutions, contribute to the protection of the right to privacy (A/HRC/31/64, para 50). He has made recommendations in favor of the incorporation of encryption capabilities to software applications and hardware devices through "privacy by design" (ibid) and welcomed court decisions rejecting the breaking of encryption as "disproportionate, privacy-intrusive measures" (A/HRC/31/64, para 58).

Lastly, we would like to refer to Human Rights Council resolution 24/5 which "reminds States of their obligation to respect and fully protect the rights of all individuals to assemble peacefully and associate freely, online as well as offline, including in the context of elections, and including persons espousing minority or dissenting views or beliefs, human rights defenders, trade unionists and others, including migrants, seeking to exercise or to promote these rights, and to take all necessary measures to ensure that any restrictions on the free exercise of the rights to freedom of peaceful assembly and of association are in accordance with their obligations under international human rights law."