Генеральная прокуратура Российской Федерации

УПОЛНОМОЧЕННЫЙ РОССИЙСКОЙ ФЕДЕРАЦИИ ПРИ ЕВРОПЕЙСКОМ СУДЕ ПО ПРАВАМ ЧЕЛОВЕКА

General Prosecutor's Office
of the Russian Federation

**Representative
of the Russian Federation
at the European Court of Human Rights**

Office du Procureur Général
de la Fédération de Russie

**Représentant
de la Fédération de Russie auprès de
la Cour Européenne des Droits de l'Homme**

Bolshaya Dmitrovka str., 15A, build. 1, Moscow, 125993

e-mail: [redacted]

18 January 2022 № Исорг-90/3-359-22/466

**EUROPEAN COURT
OF HUMAN RIGHTS**

**COMMENTARIES ON THIRD PARTY OBSERVATIONS
re application no. 33696/19
"Podchasov v. Russia"**

1. Regarding the allegations of the third party that the provision of encryption keys to the Federal Security Service of the Russian Federation (hereinafter referred to as the "FSB of Russia") provides for real or potential access to the messages of all users without their knowledge, which means that the overall security of users is at risk, since at any time any conversation can potentially be decrypted, which is, in the opinion of the third party, an indiscriminate measure, the authorities of the Russian Federation hereby report as follows.

2. By Order of 19 July 2016 no. 432 "On Approval of the Procedure for the Submission by the Organizers of the Dissemination of Information in the Information and Telecommunications Network "Internet" to the Federal Security Service of the Russian Federation of Information Necessary for Decoding Received, Transmitted, Delivered and/or Processed Electronic Messages of Users of the Information and Telecommunications Network "Internet", the FSB of Russia has imposed on the internet service providers (hereinafter referred to as the "ISP") the general obligation to provide encryption keys, while this Order does not contain the requirement to transfer the decryption keys for all traffic to the special services. Moreover, the authorities of the Russian Federation note that the obligation of the ISP to provide such information is possible only upon request, in which the requested information is specified.

3. Thus, contrary to the arguments of the third party about the possibility of decoding the messages of all users on the request of the FSB of Russia contested

by the applicant of 12 July 2017, addressed to Telegram Messenger LLP, the security authorities requested the information necessary to decode the messages of users of Telegram Messenger for 6 phone numbers (which is also indicated in the judgment in the case of an administrative offense of the Meshchansky District Court of Moscow of 16 October 2017). In addition, according to the specified request, these persons were suspected of involvement in terrorist activities, which is a particularly serious crime under Russian law. Moreover, the number of the judicial order was indicated in the request of the FSB of Russia, i.e. the conduct of this operational search event was authorized by the court.

4. While the Court recognises that intelligence services may legitimately exist in a democratic society, it reiterates that powers of secret surveillance of citizens are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions (see "Klass and Others v. Germany", no. 5029/71, § 42, of 6 September 1978; and "Rotaru v. Romania" [GC], § 47). Such interference must be supported by relevant and sufficient reasons and must be proportionate to the legitimate aim or aims pursued. In this connection, the Court considers that the national authorities enjoy a margin of appreciation, the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved. In the instant case, the interest of the respondent State in protecting its national security and combating terrorism must be balanced against the seriousness of the interference with the respective applicants' right to respect for private life (see "Segerstedt-Wiberg and Others v. Sweden", § 88).

5. The authorities of the Russian Federation claim that the alleged interference in connection with the existence of the contested legislation was "necessary in a democratic society" and pursued a "pressing social need" for national security purposes. To do this, security agencies need tools for timely and effective detection of threats arising in the digital space. Undoubtedly, one of such tools is the interception of information. Many of these threats come from international networks of hostile actors with access to increasingly sophisticated technology enabling them to communicate undetected. Access to such technology also permits hostile State and non-State actors to disrupt digital infrastructure and even the proper functioning of democratic processes through the use of cyberattacks, a serious threat to national security which by definition exists only in the digital domain and as such can only be detected and investigated there (see "Big Brother Watch and Others v. the United Kingdom" [GC], no. 58170/13, no. 62322/14 and no. 24960/15, of 25 May 2021, § 323).

6. Thus, the allegations of the third party about the violation by Order of the FSB of Russia of 19 July 2016 no. 432 of the privacy of users of the Telegram Messenger and freedom of expression, as well as about the full access of security agencies to the correspondence of users are ill-founded.

