European Court of Human Rights: Podchasov v. Russia and Škoberne v. Slovenia

IRIS 2024-3:1/20

Dirk Voorhoof
Human Rights Centre, Ghent University and Legal Human Academy

A judgment of 13 February 2024 in the case of *Podchasov v. Russia* deals with the right to privacy as protected under Article 8 of the European Convention on Human Rights (ECHR) in relation to the retention of communications data and content by Internet service providers, the protection of encrypted messages and access by law-enforcement authorities and security services to such data and content. The judgment in *Podchasov v. Russia* is highly relevant for all member states of the ECHR, also in relation to the earlier case law of the European Court of Human Rights (ECtHR) on deploying bulk or secret surveillance (see *Big Brother Watch and Others v. the United Kingdom*, IRIS 2021-7:1/20). Another judgment of the ECtHR issued just two days later, on 15 February 2024, in the case of *Škoberne v. Slovenia*, also deals with the issue of retention of communications data in light of the right to privacy. In both cases the ECtHR found a violation of Article 8 ECHR. This contribution focusses on the Russian case, highlighting the users' rights to privacy and freedom of expression.

The applicant in the Russian case is Anton Valeryevich Podchasov. He is a user of Telegram, a messaging application used by millions of people in Russia and worldwide. Telegram does not have end-to-end (client-client) encryption by default, but instead uses a custom-built server-client encryption scheme in its default "cloud chats". It is, however, possible to switch to end-to-end encryption by activating the "secret chat" feature. In June 2017, Telegram Messenger LLP was listed as an "Internet communications organiser" (ICO) in a special public register, based on section 10 of the Federal Law on Information, Information Technologies and Protection of Information (Information Act), introduced in 2014. This entailed an obligation for Telegram to store all communications data for a duration of one year and the content of all communications for a duration of six months, and to submit those data to law-enforcement authorities or security services in circumstances specified by law, together with information necessary to decrypt electronic messages if they were encrypted. Podchasov and 34 other persons challenged before a court a disclosure order by the Federal Security Service (FSB) requiring Telegram to disclose technical information which would facilitate the decryption of communications in respect of Telegram users who were suspected of terrorism-related activities. The plaintiffs argued that the provision of encryption keys as required by the FSB would enable the decryption of the communications of all Telegram users. It would therefore breach their right

to respect for their private life and for the privacy of their communications. After receiving the encryption keys, the FSB would have the technical capability to access all communications without the judicial authorisation required under Russian law. They also argued that the Russian law lacked guarantees against the potentially unjustified disclosure of their personal information. After a district court and the Moscow City Court rejected the complaints as inadmissible and after the refusal of two requests for cassation appeal, Podchasov lodged an application with the ECtHR, relying on Article 8 ECHR.

The ECtHR found that although there was no evidence that the authorities had accessed Podchasov's data stored by Telegram, he did have a claim that he was the victim of an interference with his rights under Article 8 ECHR. It was indeed impossible for an individual or a legal person to know for certain whether their data had been accessed. The ECtHR noticed furthermore that in the present case, personal data were stored for the purposes of allowing the competent national authorities the opportunity to conduct targeted secret surveillance of Internet communications. The issues relating to the storage of personal data and to secret surveillance are therefore closely linked in the present case. The crucial question in the light of Article 8 ECHR is whether the domestic law contained adequate and effective safeguards and guarantees to meet the requirements of "quality of law" and "necessity in a democratic society", in order to justify the interference with Podchasov's right to privacy. The ECtHR reiterated that confidentiality of communications is an essential element of the right to respect for private life and correspondence, as enshrined in Article 8 ECHR. Users of telecommunications and Internet services therefore must have a guarantee that their own privacy and freedom of expression will be respected. This guarantee however cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others.

With regard the obligation for ICOs to retain communications data and content, the ECtHR was struck by the extremely broad formulated duty provided by the contested legislation and it found that the interference with the right to privacy was exceptionally wide-ranging and serious. Precisely because of the seriousness of the interference, the ECtHR examined with particular attention whether the domestic law provided adequate and sufficient safeguards against abuse relating to access by law-enforcement authorities to the Internet communications and related communications data stored by ICOs pursuant to the Information Act. It observed that the manner in which access to the stored data is organised in Russia, gave the security services technical means to access stored Internet communications and communications data without obtaining prior judicial authorisation. The ECtHR found that such a system, which enables the secret services to directly access the Internet communications of each and every citizen without being required to show an interception authorisation to the

communications service provider, or to anyone else, was particularly prone to abuse. The ECtHR found that the domestic law did not at all provide for adequate and sufficient safeguards against such abuses.

As regards the requirement to submit to the security services information necessary to decrypt electronic communications if they are encrypted, the ECtHR observed that international bodies have argued that encryption provides strong technical safeguards against unlawful access to the content of communications and has therefore been widely used as a means of protecting the right to respect for private life and for the privacy of correspondence online. In the digital age, technical solutions for securing and protecting the privacy of electronic communications, including measures for encryption, contribute to ensuring the enjoyment of other fundamental rights, such as freedom of expression. Encryption, moreover, appears to help citizens and businesses to defend themselves against abuses of information technologies, such as hacking, identity and personal data theft, fraud and the improper disclosure of confidential information. The ECtHR gave due consideration to this approach in assessing the measures at issue which may weaken encryption. It appeared that in order to enable decryption of communications protected by end-to-end encryption, such as communications through Telegram's "secret chats", it would be necessary to weaken encryption for all users. These measures allegedly cannot be limited to specific individuals and would affect everyone indiscriminately, including individuals who pose no threat to a legitimate government interest. Weakening encryption by creating back doors would apparently make it technically possible to perform routine, general and indiscriminate surveillance of personal electronic communications. Back doors may also be exploited by criminal networks and would seriously compromise the security of all users' electronic communications. The ECtHR furthermore took note of the dangers of restricting encryption described by many experts in the field, and it found that the requirement to decrypt encrypted communications, as applied to end-to-end encrypted communications, cannot be regarded as necessary in a democratic society.

As the legislation at issue permitted the public authorities to have access, on a generalised basis and without sufficient safeguards, to the content of electronic communications, it impaired the very essence of the right to respect for private life under Article 8 ECHR. The Russian authorities have therefore overstepped any acceptable margin of appreciation in this regard. Unanimously the ECtHR concluded that there had been a violation of Article 8 ECHR.

Judgment by the European Court of Human Rights, Third Section, in the case of Podchasov v. Russia, Application No. 33696/19, 13 February 2024

https://hudoc.echr.coe.int/eng?i=001-230854

Judgment by the European Court of Human Rights, First Section, in the case of Škoberne v. Slovenia, Application No. 19920/20, 15 February 2024

https://hudoc.echr.coe.int/eng?i=001-230885