EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

Communicated on 29 October 2020

Published on 16 November 2020

THIRD SECTION

Application no. 13232/18
TELEGRAM MESSENGER LLP and TELEGRAM MESSENGER INC.
against Russia
lodged on 14 March 2018 and 23 April 2019

STATEMENT OF FACTS

1. The applicant, Telegram Messenger Limited Liability Partnership (hereinafter, "Telegram Messenger LLP"), until 2 April 2019, was a company incorporated in the United Kingdom and having its registered address in London. On 2 April 2019 it was struck off the Companies House Register on the application of its members – Telegram Messenger Inc. and Telegraph Inc.

2. On 23 April 2019 Telegram Messenger Inc., a company incorporated on the British Virgin Islands and having its registered address there, notified the Court of its wish to pursue the proceedings before the Court in Telegram Messenger LLP's stead, and in its own name.

3. Both companies were/are represented before the Court by Mr D. Gaynutdinov, a lawyer authorised to practice in Russia.

A. The circumstances of the case

4. The facts of the case, as submitted by the applicants, may be summarised as follows.

1. Background information

5. Until May or June 2018 Telegram Messenger LLP owned and operated Telegram, a messaging application, which can be used free of charge on various devices such as mobile telephones, tablets or computers.

This application is used by millions of people in Russia and worldwide (see also "Other relevant information" below).

6. In early 2017 the Federal Telecom Supervision Service (Roskomnadzor) decided to list the applicant company as an "Internet communications organiser" (ICO) (*организатор распространения информации в сети Интернет*) in a special public register (see "Relevant domestic law and practice" below). Accordingly, Roskomnadzor invited Telegram LLP to provide certain information to it. In June 2017 the applicant company's CEO, Mr P. Durov, made a public statement taking note of the envisaged inclusion of the company into the register.

7. On 28 June 2017 Telegram Messenger LLP was listed as an ICO in the relevant register.

8. On 23 May 2018 Telegram Messenger LLP signed with Telegram Messenger Inc. an Intellectual Property Agreement Deed according to which the applicant company agreed to assign, transfer and convey to Telegram Messenger Inc. all of its rights, title and interest in and to the intellectual property owned by the applicant company including Telegram Messenger application. Shortly thereafter Telegram Messenger Inc. started to manage and to develop the messaging application.

2. A disclosure order

9. On 21 July 2017 Telegram Messenger LLP received a disclosure order dated 12 July 2017 and signed by Officer S. of the Federal Security Service ("FSB"). This disclosure order was issued under the FSB's Order No. 432 of 19 July 2016 (see "Relevant domestic law and practice" below). The disclosure order required the applicant company to disclose technical information which would facilitate "the decoding of communications since 12 July 2017 in respect of the Telegram users who were suspected of terrorism-related activities". The FSB listed six mobile telephone numbers associated with Telegram Messenger accounts and numbers of six court decisions issued on 10 July 2017.

10. The legal basis and the contents of those court decisions are not specified. In particular, it is not clear whether those court decisions concerned authorisation of interception of telephone communications on those telephone numbers or/and electronic communications, in particular in the Telegram Messenger, that might be associated with those telephone numbers.

11. The disclosure order required Telegram Messenger LLP to submit, *inter alia*, an IP address, a TCP/UDP port number and the "data relating to the (encryption) keys" (*ключевой материал*) which would be "necessary and sufficient" for decoding a communication. The information was to be sent, by 19 July 2017, to the FSB's email address at fsb@fsb.ru. A journalistic investigation carried out several months later disclosed that two

of the six mobile numbers referenced by the FSB belonged to two people suspected in relation to the explosions in St Petersburg metro in April 2017.

12. Telegram Messenger LLP refused to comply with the disclosure order, putting forward the importance of preserving the confidentiality of private communications and the freedom of expression on the part of the Telegram users.

3. Prosecution for an administrative offence

(a) Pre-trial and trial proceedings

13. On 14 September 2017 a FSB officer compiled a report of an offence under Article 13.31 (2.1) of the Code of Administrative Offences ("CAO") against Telegram Messenger LLP. For unspecified reasons no representative of the applicant company was present during the compiling of the report.

14. The case file was then submitted to the justice of the peace of the 383rd Court District of the Meshchanskiy District of Moscow.

15. On 16 October 2017 the justice of the peace held a hearing. For unspecified reasons the applicant company was not represented at the hearing. Neither was any representative of the FSB present at it. The justice of the peace heard no oral representations but only examined the written material in the file.

16. By a judgment of 16 October 2017 the justice of the peace convicted Telegram Messenger LLP and imposed on it a fine of 800,000 Russian roubles (equivalent to 11,740 euros at the time).

(b) Appeal proceedings

17. Telegram Messenger LLP appealed to the Meshchanskiy District Court of Moscow arguing, *inter alia*, as follows:

(a) The disclosure order had been directed, in substance, at interception of telephone communications, which under Russian law required a judicial authorisation. No court order had been presented to the applicant company or at least to the court dealing with the CAO case. Therefore, it had not been possible to ascertain that the FSB's disclosure order pursued a legitimate aim and that the substantive and procedural requirements for restricting individual constitutional rights had been complied with. In such circumstances, the applicant company had been prevented from complying with the disclosure order, on account of its own professional duty to ensure confidentiality of the communications between the users of its Internet messenger service.

(b) The disclosure order was not narrowly tailored, in particular in that it did not allow compliance with it by way of submitting the contents of the relevant communications. Instead, it specifically required disclosure of such technical data, which might facilitate access to the communications of the Telegram users beyond the six mobile telephone numbers mentioned in the

disclosure order. In substance, the disclosure order actually required the applicant to design a mechanism for decoding communications. From a purely technical point of view it was impracticable to comply with the disclosure order since the traces of a communication would only be kept on the devices used for that communication. In substance, the disclosure order amounted to a request to design a so-called backdoor technical solution for access to the confidential data.

(c) The applicable domestic provisions defined jurisdiction with reference to the court in the area where the legal entity was situated meaning the municipality in Russia where it had its registration. However, the applicant company was never registered in Russia, being incorporated in the United Kingdom and operating in London.

18. At the hearing on 12 December 2017 the applicant company's lawyers lodged a number of motions:

- to require participation of a public prosecutor in the proceedings;
- to require attendance at an appeal hearing by a representative of the FSB, the authority that initiated the proceedings and compiled the offence record serving as a basis for prosecution and adverse evidence for establishing the pertinent facts as well as the defendant's guilt;
- to require production of the court decisions mentioned in the disclosure order of 12 July 2017;
- to admit into evidence and to examine a written statement prepared by Mr Shsch., apparently having expertise in the field of information technologies, as regards the technical impossibility to comply with the disclosure order in respect of six people without endangering the confidentiality of the other Telegram users;
- to hear Mr Shch.'s oral testimony at the court hearing;
- to require the attendance by Officer S. who signed the disclosure order of 12 July 2017, in particular with a view to interviewing him about the technical feasibility matter.

19. The appeal court dismissed the above motions as the case file already contained all the documents which were necessary for dealing with the merits of the charge against the applicant company.

20. By decision of 12 December 2017 the District Court upheld the trial judgment. As regards the points of appeal mentioned above, the appeal court stated as follows:

(a) the disclosure order to the defendant (the applicant company) had mentioned court decisions authorising restrictions in respect of telephone communications;

(b) referring to Articles 1.4 and 2.6 of the CAO and the Russian Supreme Court's Ruling No. 5 of 24 March 2005, the appeal court considered that the justice of the peace in Moscow had jurisdiction in so far as he was a court to which was assigned the place "where the prescribed

action should have been accomplished or an obligation should have been complied with".

21. It is unclear whether Telegram Messenger LLP paid the fine.

4. Further proceedings

(a) Judicial review of the FSB's Order No. 432

22. In December 2017 Telegram Messenger LLP instituted proceedings before the Supreme Court of Russia, challenging the FSB's Order No. 432. It appears that the Supreme Court upheld the legality of the Order.

(b) The blocking of the messaging application in Russia

(i) Judicial proceedings

23. On 20 March 2018 Roskomnadzor ordered the applicant company to provide technical data allowing access to the encrypted messages of users. The applicant company replied that this was not feasible from the technological point of view.

24. On 10 April 2018 Roskomnadzor instituted proceedings before the Taganskiy District Court of Moscow seeking judicial authorisation for blocking access to the Telegram messaging application. On 11 April 2018 the court's registry informed the applicant's lawyer about the application.

25. The District Court ruled that the case be examined under the rules of the Code of Civil Procedure (CCP).

26. Having heard the representatives of Roskomnadzor and the FSB, by a judgment of 13 April 2018 the District Court ordered the blocking of the Telegram application in Russia. The court held as follows:

(a) Telegram Messenger LLP had been listed as an Internet communications organiser (ICO). It had then failed in its statutory obligation to comply with the disclosure order and had been fined. It had subsequently refused to provide the necessary data again.

(b) The argument about the impossibility to submit the decoding data was rejected because an ICO providing a possibility of coded communications was bound to comply with its statutory obligation to submit decoding data. In any event, the argument was not substantiated.

(c) The judgment was to be enforced immediately because its prolonged non-enforcement could result in "substantial violations of the constitutional rights relating to one's personal data and cause important damage to public and private interests".

27. On 18 April 2018 Telegram Messenger LLP lodged an ancillary appeal (*частная жалоба*) against the immediate enforcement of the judgment (as provided for by Article 212 § 3 of the CCP). This appeal was then attached to the case file as an "addition" to the main statement of appeal (see below).

28. On 11 May 2018 Telegram Messenger LLP lodged the main statement of appeal before the Moscow City Court against the judgment. The applicant company argued that the District Court's arbitrary decision to apply the CCP had deprived it of the adequate level of procedural protection, for instance as regards the burden of proof that would be on the administrative authority in the procedure under the Code of Administrative Procedure (CAP).

29. On 14 June 2018 the City Court examined the main appeal and the addition to it and upheld the judgment stating as follows:

(a) The ICO had been notified of the court hearing on 13 April 2018 and had designated several representatives; the unavailability of one representative did not constitute a valid ground for adjourning the hearing; thus the ICO had to bear the procedural consequences resulting from its absence from a hearing, namely as regards the submission of evidence or contesting adverse evidence; the first-instance court could thus determine the case on the basis of the evidence made available to it; the ICO provided the appeal court with no additional evidence which would confirm that it allegedly had had insufficient time to submit before the first-instance court;

(b) Russian law did not clearly prescribe that an application for blocking access to an information system or programme had to be examined under the CAP. In any event, the choice of procedure did not adversely affect the correct outcome of the case;

(c) The ICO's reference to the first-instance court's failure to take account of various protected interests and the negative effect resulting from blocking the messaging application was dismissed as unfounded. Such interests and effect could not absolve the ICO from its obligation to provide the decoding data and could not serve as a basis for absolving it from the responsibility for failing to do so. The ICO's reference to the confidentiality of communications was dismissed as unfounded because the decoding data was not classified in Russian law as a protected type of information relating to the secrecy of correspondence or communications. Thus, Russian law did not impose any special conditions or procedure for accessing it;

(d) The immediate enforcement of the blocking order was justified in that "the continuation of electronic communications without providing the decoding data could result in the dissemination of the information that could be used for committing unlawful actions, including actions of terrorist and extremist nature".

30. Telegram Messenger LLP applied for further (cassation) review of the lower courts' judgments. On 9 October 2018 and 25 January 2019 the City Court and the Supreme Court of Russia respectively rejected the cassation appeals. The Supreme Court referred to the provisions of the CAP.

31. It appears that Telegram Messenger Inc. was not involved in the above proceedings.

(ii) Enforcement of the blocking order

32. The judgment of 13 April 2018 was subject to immediate enforcement. It is unclear what specific measures were taken in that respect and what practical effects they have had in terms of normal accessibility of the messaging application in Russia, that is without having to make use of various "filter-bypassing services" (see also paragraph 42 below).[1]

B. Relevant domestic law and practice

1. Internet communications organisers and their statutory obligations

33. Section 10.1 of the Information Technologies Act (Federal Law No. 149-FZ of 27 July 2006) was introduced into the Act in 2014. It defines an "Internet communications organiser" (ICO) and lists its statutory obligations.

An ICO is a person or an entity that ensures the functioning of information systems and (or) programmes for electronic devices, with the aim of receiving, transmitting, delivering and (or) processing electronic communications on the Internet. An ICO must notify the competent federal authority about its activity.

In July 2016 sub-section 4.1 was added and read as follows:

> "4.1. Where additional coding is used in relation to receiving, transmitting, delivering and (or) processing of electronic communications of Internet users, an Internet communications organiser must submit, to the federal authority on information security, the information which is necessary for decoding ..."

34. The FSB Act (Federal Law No. 40-FZ of 3 April 1995) appoints the FSB as the federal authority in charge of the security and gives it a statutory competence to enact legal acts of general application in the areas of its competence.

35. FSB's Order No. 432 of 19 July 2016 was issued in pursuance of section 10.1 (4.1) of the Information Technologies Act and section 3 of the FSB Act. It specifies that its analytical unit was competent to require submission of information which is necessary for decoding electronic communications. A related disclosure order should specify the contents (the format) of the requested information and the address for dispatching such information.

36. Article 13.31 of the Code of Administrative Offences punishes offences constituted by the failure on the part of an Internet communications organiser to comply with its obligations. In July 2016 sub-section 2.1 was introduced into this Article. It reads as follows:

> "2.1. An Internet communications organiser's failure to comply with its obligation to submit, to the federal authority on information security, the information which is

[1] see, for instance, Application no. 4945/20 pending before the Court.

necessary for decoding incoming, outgoing, arriving and (or) processed electronic communications, is punishable by an administrative fine ..."

2. Restrictions of access to an information system or programme

37. Section 15.4(2) of the Information Technologies Act provided at the time that a final court order could restrict access to the relevant information system or programme, in the event of the ICO's failure to comply with its obligations under section 10.1, until the ICO's compliance complied with such obligations.

3. Other relevant provisions and jurisprudence

38. Pursuant to Article 2 § 4 of the CAP and Article 1 § 4 of the CCP, in the absence of a specific procedural rule applicable to the matter arising in the ongoing administrative proceedings a court should apply a rule applicable to similar matters or, as last resort, the principles of justice.

39. Article 212 of the CCP provides that a court may grant a claimant's request for immediate enforcement of the court's decision where there are exceptional circumstances indicating that the delay in its enforcement may result in a significant damage to the judgment creditor or in the impossibility to enforce that judgment. A court order on immediate enforcement of a judgment is amenable to review by way of an ancillary appeal (*частная жалоба*), which does not suspend the enforcement of the order.

40. In Ruling no. 5 of 24 March 2005 the Plenary Supreme Court of Russia indicated that a CAO case had to be examined by a court competent for the area "where the offence was committed". Where an offence consisted of an inaction, that would be the court in the area where the corresponding action should have been accomplished or an obligation should have been complied. Where the inaction was related to non-compliance with a statutory or otherwise prescribed obligation or duty, it was necessary to take into account a person's registered place of residence, an official's station of duty or a legal entity's place of business (*место нахождения юридического лица*), which could be determined with reference to Article 54 of the Civil Code (that is the municipality where the legal entity was registered in the Russian Federation; a legal entity is registered where its permanent executive body is situated or, if no such executive body exists, where its officer or another authorised person is situated (*находится*)).

41. In Russia the law-enforcement authorities are not required under domestic law to show the judicial authorisation to the communications service provider before obtaining access to a person's communications, except in connection with the monitoring of communications-related data under the Code of Criminal Procedure. Pursuant to Orders issued by the Ministry of Communications, in particular the addendums to Order No. 70

of 20 April 1999, communications service providers must install equipment giving the law-enforcement authorities direct access to all mobile telephone communications of all users. The communications service providers also have an obligation under the Russian Government's Order no. 538 of 27 August 2005 to create databases storing information about all subscribers, and the services provided to them, for three years; the secret services have direct remote access to those databases. The law-enforcement authorities thus have direct access to all mobile telephone communications and related communications data (see *Roman Zakharov v. Russia* [GC], no. 47143/06, § 269, ECHR 2015).

C. Other relevant information

42. The Telegram Messenger provides for a possibility to have so-called "secret chats" all messages in which have end-to-end encryption. This means only the sender and the recipient can read those messages; nobody else can decipher them, including the applicant company. This means that all data (including media and files) sent and received via Telegram cannot be deciphered when intercepted by a user's Internet service provider network administrator or other third parties. All secret chats in Telegram are device-specific and are not part of the Telegram cloud. This means a user can only access messages in a secret chat, he is a part of, from his or her own device of origin. When a secret chat is created, the participating devices exchange encryption keys using the so-called Diffie-Hellman key exchange. After the secure end-to-end connection has been established, there is a picture being generated that visualises the encryption key for the users' chat. As regards electronic communications outside the scope of "secret chats", it appears that they are not subject to end-to-end encryption.

43. It appears that on 16 April 2018 a deputy Prosecutor General requested Roskomnadzor to block access to particular information channels on the platform of the Telegram messenger on the grounds that they contained "texts and videos promoting or justifying the activities of the Islamic State of Iraq and the Levant, Jabhat al-Nusra, Jabhat Fatah al-Sham, Ahrar al-Sham and other illegal armed formations in the Syrian Arab Republic". He also requested Roskomnadzor to block particular "filter-bypassing services" which enabled users to access such content, and any future "mirrors" or copies of that content. Within one week of those decisions, Roskomnadzor blocked access to approximately 20,000,000 IP addresses, including those of major cloud services such as Google, Amazon Web Services, DigitalOcean, Microsoft and Hetzner, which were allegedly used for circumventing the blocking measures.[2]

[2] see, for instance, Application no. 48932/19 pending before the Court.

COMPLAINTS

44. Telegram Messenger LLP complained under Article 10 of the Convention that its conviction and the fine imposed for its refusal to facilitate the FSB's access to confidential private information had amounted to an interference with its freedom to impart information regardless of frontiers as protected by Article 10 of the Convention. The applicant company argued that this interference had not been "prescribed by law" and had not been "necessary in a democratic society" in pursuance of any legitimate aim (for instance, relating to national security), in particular because:

(a) Section 10.1 of the Information Technologies Act did not contain a precise and exhaustive list of conditions circumscribing the federal authority's disclosure order and the resulting access to confidential communications between users of an Internet service;

(b) FSB's Order No. 432 did not set a procedure with adequate safeguards for preventing the disclosure of the confidential information of the users, who were not targeted by a disclosure order, and did not set any time-limit for complying with a disclosure order. The absence of a time-limit should have prevented the finding the applicant company was liable for non-compliance with the disclosure order;

(c) The disclosure order required an unlimited access to the communications of six users while no court orders authorising such access and setting safeguards for transmitting the information had been produced. Neither the Information Technologies Act nor Order no. 432 contained a requirement of a prior judicial authorisation of the access to confidential electronic communication before ordering an ICO to disclose the information which is necessary for decoding such communications;

(d) Compliance with the disclosure order exposed the applicant and its employees to criminal liability for a breach of the privacy of communications in the absence of a relevant court decision;

(e) The applicable primary and secondary legislation, the disclosure order itself or the court decisions in the CAO case contain no assessment aimed at striking a balance between the aim of fighting terrorism and ensuring public safety, on one hand, and the Internet service users' right to respect for their private lives and freedom of expression as well as the applicant company's freedom to impart information, on the other.

45. Telegram Messenger LLP also complained that the blocking of the messenger from 16 April to 14 June 2018, without a final court order, violated section 15.4(2) of the Information Technologies Act, was not based on any compelling reasons and was disproportionate.

46. Referring to Article 13 of the Convention, Telegram Messenger LLP complained that the courts had not assessed whether the blocking order and its immediate enforcement were "necessary in a democratic society",

including whether they were proportionate to any legitimate aim being pursued.

47. Telegram Messenger LLP complained that Article 6 of the Convention had been violated:

(a) in the CAO proceedings on account of (i) the requirement of objective impartiality because of the lack of a prosecuting party in the CAO cases; (ii) the jurisdiction of the trial court ("established by law");

(b) in the blocking proceedings on account of (i) the allegedly unlawful decision to examine the application for blocking Telegram messaging application under the rules of the Code of Civil Procedure rather than the Code of Administrative Procedure; (ii) the insufficient time to prepare its defence prior to the first-instance hearing, no access to the statement of claim and related documents prior to the hearing, inability to make arrangements for the lawyer's presence at it.

48. In April 2019 Telegram Messenger Inc. maintained the above complaints and expressed its intention to pursue them following Telegram Messenger LLP's dissolution on the latter's behalf and in its own name.

QUESTIONS TO THE PARTIES

1.1. Did the "interferences" in the present case (the fine imposed for Telegram Messenger LLP's refusal to disclose technical data which would facilitate the State's access to the confidential private information of Telegram application users; the blocking order and its immediate enforcement) relate to the applicant company's (companies') freedom of expression as protected by Article 10 § 1 of the Convention (compare *Magyar Kétfarkú Kutya Párt v. Hungary* [GC], no. 201/17, §§ 87-92, 20 January 2020; *Ahmet Yıldırım v. Turkey*, no. 3111/10, § 50, ECHR 2012; and *Neij and Sunde Kolmisoppi v. Sweden* (dec.), no. 40397/12, 19 February 2013)?

1.2. Were the interferences "prescribed by law"?

1.3. Did the interferences pursue a legitimate aim within the meaning of Article 10 § 2 of the Convention?

1.4. Were the interferences "necessary in a democratic society"?

2. Was there a violation of Article 13 in conjunction with Article 10 of the Convention in respect of the judicial authorisation for blocking Telegram Messenger (compare *Lashmankin and Others v. Russia*, nos. 57818/09 and 14 others, § 356, 7 February 2017; *Ivashchenko v. Russia*, no. 61064/10, §§ 88-92, 13 February 2018; *Kablis v. Russia*, nos. 48310/16 and 59663/17, §§ 64-72, 30 April 2019; and *Elvira Dmitriyeva v. Russia,* nos. 60921/17 and 7202/18, §§ 57-65, 30 April 2019) and the immediate enforcement of the blocking order?

3.1. As to the justice of the peace's judgment of 16 October 2017 as upheld on appeal on 12 December 2017, was there a violation of Article 6 of the Convention (under its criminal limb) in those proceedings on account of (i) the requirement of objective impartiality because of the lack of a prosecuting party (see *Karelin v. Russia*, no. 926/08, §§ 69-84, 20 September 2016); (ii) the jurisdiction of the trial court ("established by law")?

3.2. As to the judgment of 13 April 2018 by the Taganskiy District Court as upheld on further review, was there a violation of Article 6 of the Convention (under its civil limb) in the blocking proceedings on account of (i) the decision to examine the case under the Code of Civil Procedure

rather than the Code of Administrative Procedure; (ii) the insufficient time to prepare the ICO's defence prior to the first-instance hearing, no access to the statement of claim and related documents prior to the hearing, and the ICO lawyer's absence from it?

4. The respondent Government are requested to submit copies of the court decisions mentioned in the disclosure order of 12 July 2017; and the Supreme Court's decisions taken on judicial review in respect of the FSB's Order No. 432.