European Human Rights Advocacy Centre

Submissions under Rule 9(2) of the Committee of Ministers' rules for the supervision of the execution of judgments and of the terms of friendly settlements

Judgment in *Roman Zakharov v. Russia* (App. No. 47143/06, 4 December 2015)

1. These submissions have been lodged by the European Human Rights Advocacy Centre (EHRAC), Memorial and Citizens' Watch (St Petersburg) to provide information on legislative developments relevant to the implementation of the Grand Chamber judgment of the European Court of Human Rights in *Roman Zakharov v. Russia*,[1] in preparation for the meeting of the Committee of Ministers on 18-20 September 2018, when this case is listed to be examined.

2. The case involved a claim by Mr Zakharov, an editor and chairman of the St Petersburg branch of the Glasnost Defence Foundation, a media freedom NGO, against the blanket interception of telephone communications by law enforcement agencies, under the System of Operative Investigative Measures (SORM). On 4 December 2015, the Grand Chamber of the ECtHR unanimously found Russia in violation of Article 8 of the Convention. It found that Russian legislation did not 'provide for adequate and effective guarantees against arbitrariness and the risk of abuse which is inherent in any system of secret surveillance, and which is particularly high in a system where the secret services and the police have direct access, by technical means, to all mobile telephone communications'.[2]

The Russian Government's Action Plan of 3 August 2018

3. The latest Russian action plan (3 August 2018) fails to mention the enactment of the Yarovaya laws (which are discussed below), and does not refer to any legislative or judicial developments which address the specific weaknesses and failures in the legal framework which were identified by the European Court (in paras. 243-305 of the judgment). The action plan also appears to seek to argue that legislative instruments and judicial decisions dating from before the Court's judgment in some way remedy the problems identified in the Court's judgment. Some statistics are provided as regards the prosecutor's oversight, but no references are cited.

[1] *Zakharov v. Russia*, App. No. 47143/06 (Grand Chamber Judgment) (4 December 2015). EHRAC and Memorial acted as Roman Zakharov's legal representatives in this case. See also: Communication from the Russian Federation in the case of Roman Zakharov against Russian Federation (23 August 2017) Doc no DH-DD(2017)875, [III.1]; Communication from the Russian Federation in the case of Roman Zakharov against Russian Federation (23 August 2017) Doc. No. DH-DD(2017)875, [III.2]; Committee of Ministers, Notes on the Agenda on H46-25 *Roman Zakharov v. Russian Federation* (7 December 2017) Reference doc no DH-DD(2017)875.
[2] Ibid [302].

Relevant legislative developments

4. Despite the Court's findings, Russia has not taken any steps to amend SORM regulations.[3] Three SORM systems exist requiring service providers to collect, analyse and store transmitted data. SORM-1 relates to telephone data and SORM-2 to Internet traffic. SORM-3 relates to all media, providing for their long-term storage.[4] The *Zakharov* case related to SORM-1 and SORM-2 (SORM-3 being issued in 2014 after Mr. Zakharov had lodged his complaint at the ECtHR).[5] There is no indication that changes to the orders for any of these SORMs has been introduced.

5. Furthermore, the Russian authorities have adopted a range of other measures which, it is submitted, seriously undermine Article 8 protections as well as the judgment's findings regarding the collection and retention of user data and the weak oversight regarding their interception. These are described below.

6. Federal Laws 374-FZ and 375-FZ of 2016 (together known as the 'Yarovaya law') are important in relation to *Zakharov* because they impose new obligations which in effect require service providers to use SORMs with new capabilities to meet them.[6] In essence, the Yarovaya law requires service providers to retain voice data, texts and images for six months, make them available to the security services, if required, and retain metadata such as the time, location and sender of messages, for up to three years.[7] They must disclose communications and metadata, if requested by government authorities, without the authorities having to obtain a court order.[8] Telecommunications service providers face a maximum fine of approximately $15,000 for the failure to comply.

7. Most of the provisions in Federal Law 374-FZ (which amends counter-terrorism laws), and the entirety of Federal Law 375-FZ (which amends the Criminal Code and Code of Criminal Procedure), came into force on 20 July 2016. For Federal Law 374-FZ, the provisions requiring

[3] Anastasia Kornya, 'Telegram будет судиться с Россией в Страсбурге' *Vedomosti* (21 March 2018), www.vedomosti.ru/politics/articles/2018/03/21/754508-telegram-strasburge, accessed 3 August 2018.
[4] James Lewis, 'Reference Note on Russian Communications Surveillance' (18 April 2014) Center for Strategic & International Studies, www.csis.org/analysis/reference-note-russian-communications-surveillance, accessed 3 August 2018; Andrei Soldatov and Irina Borogan, 'Russia's Surveillance State' *World Policy Journal* (2013), https://worldpolicy.org/2013/09/12/russias-surveillance-state/, accessed 3 August 2018.
[5] See *Zakharov* (n 1) [115]-[138] for the orders of the Ministry of Communications and Mass Media relevant to SORM-1 and SORM-2; SORM-3 is contained in Order no 83 of 2014, issued 18 April 2014, entered into force 29 July 2014, http://minsvyaz.ru/ru/documents/4249/, accessed 3 August 2018.
[6] Svetlana Yastrebova, 'Первые системы СОРМ готовы для исполнения закона Яровой' *Vedomosti* (16 March 2018), www.vedomosti.ru/technology/articles/2018/03/16/753935-sorm-yarovoi, accessed 3 August 2018.
[7] Daniel Garrie and Irene Bykhovsky, 'Privacy and Data Protection in Russia' (2017), Journal of Law and Cyber Warfare 235, 247-248.
[8] Human Rights Watch, 'Russia: 'Big Brother' Law Harms Security, Rights' (12 July 2016), www.hrw.org/news/2016/07/12/russia-big-brother-law-harms-security-rights, accessed 3 August 2018.

the retention of client voice data for six months entered into force on 1 July 2018, and those on the retention on all remaining electronic correspondence for three months will enter into force on 1 October 2018.[9] As of late-June 2018, many service providers reported that they were struggling to meet the July deadline.[10]

8. In addition to the Yarovaya law, Federal Law no 242-FZ[11] (known as the 'New Data Protection Law') came into force on 1 September 2015. It amended the Personal Data Protection Act in two key ways. First, it introduced an obligation on service providers to collect, store and process personal information. Second, it created a mechanism whereby the Federal Service for Oversight of Communications, Information Technology and Mass Media (*Roskomnadzor*) could block service providers for the failure to meet their obligations.[12] Some commentators have argued that this mechanism represents a significant measure, due to the severe reputational consequences of non-compliance.[13]

9. The New Data Protection Law requires that personal data must be stored in data centres within Russia, and implicitly prohibits storage outside its borders,[14] whereas previously, such information could be stored anywhere.[15] This represents the latest step following the introduction of two previous sets of measures, in 2013 and 2014, which were intended to localise data storage.[16] One significant effect of the law is that it increases the Russian authorities' control over online activities, including by increasing the power of law enforcement to access information and to control public access to it.[17]

---

[9] Federal Law 374-FZ on Certain Amendments to Laws on Additional Measures on Counter-Terrorism and Safety, adopted 29 June 2016, with certain provisions entered into force 20 July 2016 and 1 July 2018, and entering into force 1 October 2018, http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102404066, accessed 3 August 2018; Federal Law 375-FZ on Amendments to the Criminal Code and Code of Criminal Procedure under the Additional Measures on Counter-Terrorism and Safety, adopted 20 June 2016, entered into force 20 July 2016, http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102404067, accessed 3 August 2018; Andrei Kuzmin, 'Под закон Яровой подпадают все облачные сервисы и интернет-магазины' *RusBase* (11 July 2016), https://rb.ru/opinion/yarovaya-pack/, accessed 3 August 2018; 'Russia's "anti-terrorism" telecoms law is ready for action and it reportedly won't cost companies all they feared' *Meduza* (6 March 2018), https://meduza.io/en/news/2018/03/06/russia-s-anti-terrorism-telecoms-law-is-ready-for-action-and-it-reportedly-won-t-cost-companies-all-they-feared, accessed 3 August 2018.

[10] 'Russia's "Big Brother" Law Enters Into Force' *The Moscow Times* (Moscow: 1 July 2018), https://themoscowtimes.com/news/russias-big-brother-law-enters-into-force-62066, accessed 3 August 2018.

[11] Federal Law 242-F on Amendments to Certain Legislative Acts of the Russian Federation for Clarification of Personal Data Processing in Information and Telecommunication Networks, adopted 21 July 2014, entered into force 1 September 2015, http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102355893, accessed 3 August 2018.

[12] Human Rights Watch (n 11).

[13] Garrie and Bykhovsky (n 8) 242, 245; Sergey Medvedev, 'Data Protection in Russian Federation: overview' (May 2016), https://uk.practicallaw.thomsonreuters.com/2-502-2227?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1, accessed 24 July 2018.

[14] ibid Medvedev.

[15] Alexander Savelyev, 'Russia's New Personal Data Localization Regulations: A Step Forward Or A Self-Imposed Sanction?' (2016) 32 Computer Law & Security Review 128, 129, as cited in Daniel Garrie and Irene Bykhovsky, 'Privacy and Data Protection in Russia' (2017) Journal of Law and Cyber Warfare 235, 242, 245.

[16] Alexander Savelyev, 'Russia's new personal data localization regulations: A step forward or a self-imposed sanction?' (2016) Computer Law & Security Review 128, 129.

[17] ibid 141.

10. Since the New Data Protection Law came into force, authorities in Russia have blocked or threatened to block certain service providers. For example, in 2016 a Moscow court blocked the career networking site LinkedIn for failing to store personal data locally.[18] *Roskomnadzor* has stated that it may block Facebook if it does not localise its data storage by the end of 2018.[19]

11. Furthermore, Federal Law 241-FZ has been enacted, requiring messaging service providers to identify users and transmit user messages to the authorities when required to do so. Known as the Messaging Services Law, it came into force in January 2018. Service providers must identify users by mobile phone number, store user identification information within Russia, restrict the dissemination of information which is prohibited in Russia, and transmit messages at the request of the Russian authorities.[20] The law further enhances the powers of the Federal Security Bureau (FSB), to which service providers may be required to hand over user information.[21]

12. Since its entry into force, the Messaging Services Law has been the subject of several lawsuits. In December 2015, Telegram, a messaging application popular in the former-Soviet Union and the Middle East, challenged the FSB's right to request such information. However, the Supreme Court dismissed their claim in March 2018.[22] Telegram also challenged *Roskomnadzor*'s decision to block it, which it has taken to the European Court of Human Rights after its case was rejected by the Moscow City Court.[23] Conversely, Roskomnadzor took legal action against Telegram in April 2018 for refusing to give the FSB access to user messages.[24]

---

[18] Garrie and Bykhovsky (n 8) 246; Shaun Walker, 'Russia blocks access to LinkedIn over foreign-held data' *The Guardian* (Moscow: 17 November 2016), www.theguardian.com/world/2016/nov/17/russia-blocks-access-to-linkedin-over-foreign-held-data, accessed 3 August 2018.

[19] Leonid Bershidsky, 'Silicon Valley Giants Face a Test in Russia' *Bloomberg* (18 April 2018), www.bloomberg.com/view/articles/2018-04-18/amazon-google-and-facebook-all-face-pressure-in-russia, accessed 3 August 2018; 'Роскомнадзор проверит Facebook до конца 2018 года' *Izvestiya* (18 April 2018), https://iz.ru/733482/2018-04-18/roskomnadzor-proverit-facebook-do-kontca-2018-goda, accessed 3 August 2018.

[20] Sergey Medvedev and Ilya Goryachev, 'Russia further regulates instant messaging services providers' (2017) Gorodissky & Partners, www.gorodissky.com/publications/articles/russia-further-regulates-instant-messaging-services-providers/, accessed 3 August 2018.

[21] Damir Gainutdinov and Pavel Chikov, 'Internet Freedom 2017: Creeping Criminalisation' (2017) AGORA 21.

[22] Nikita Shiryayev, 'Russian Supreme Court upholds FSB decree on decoding messages' *Russian Legal Information Agency* (20 March 2018), www.rapsinews.com/judicial_news/20180320/282257394.html, accessed 3 August 2018.

[23] 'Telegram turns to ECHR over messenger blocking in Russia' *Russian Legal Information Agency* (18 June 2018), www.rapsinews.com/judicial_news/20180618/283026435.html, accessed 3 August 2018.

[24] 'Russia files lawsuit to block Telegram' *Reuters* (6 April 2018), www.reuters.com/article/us-russia-telegram/russia-files-lawsuit-to-block-telegram-messaging-app-idUSKCN1HD143, accessed 3 August 2018.

13. There are indications that the Russian legislature is taking further steps to explore monitoring social media. In 2018, the Russian Duma opened tenders for expert reports studying the regulation of social networks by other states. The report, the tender stated, was required due to the 'growth in social networks' which has 'raised the question of the need to legally regulate the relationships in social networks'. The focus of the research would be popular networks such as *Odnoklassniki*, *VKontakte*, Facebook, Twitter, Instagram, Youtube, Habrahabr and Badoo.[25]

Conclusion

14. It is submitted that the Russian authorities have clearly not taken the requisite steps to address the substance of the 2015 Grand Chamber judgment in *Roman Zakharov*. Rather than bringing the SORM systems into compliance with Article 8 of the Convention, it has enacted legislation which continues and extends the practice of the indiscriminate, arbitrary and unchecked interception, collection and storage of sensitive personal data.

15. The Committee of Ministers is accordingly requested to stipulate that the Russian Government should take the necessary measures to ensure that domestic legislation is amended so as to comply with the Grand Chamber judgment in *Roman Zakharov v. Russia*.

16. In particular, the Committee of Ministers is requested to require the following:

(i) the Government should undertake to overhaul the SORM hardware, so that there is a 'second key': the officer in charge of the surveillance should be required to produce the court order to the service provider;

(ii) the Government should undertake to remedy the specific legislative shortcomings identified by the Grand Chamber, including (but not limited to) setting out the following:

(a) an obligation to specify in all cases the person who is the target of the interception and the relevant device and/or telephone number (para. 265 of the judgment);

(b) an obligation to specify the nature of the offences which may give rise to an interception order (paras. 243-244) and to specify the category of persons who may be the target of surveillance who "may have information about a criminal offence" (but who are not a suspect or an accused) (para. 245);

[25] Roskomsvoboda, 'Госдума заказала исследование заграничного опыта регулирования соцсетей' (30 July 2018), https://roskomsvoboda.org/40698/, accessed 3 August 2018; Procurement item no 0173100009618000097, issued 27 July 2018, retrieved from the Unified Information System on Procurement, http://zakupki.gov.ru/epz/order/notice/ok44/view/documents.html?regNumber=0173100009618000097, accessed 3 August 2018.

(c) an obligation to set out a detailed and specific list of events or activities considered to endanger Russia's national, military, economic or ecological security (paras. 246-248 and 266);

(d) an obligation to set out safeguards for interceptions conducted outside the framework of criminal proceedings (paras. 251-253);

(e) an obligation to destroy immediately any data not required for the purposes of a criminal investigation (para. 255);

(f) an obligation to notify the target of the interception after the termination of the surveillance measure (where it can be carried out without jeopardising the purpose of the restriction) (para. 287).

(iii) the Government should be required to explain how it will ensure that the courts exercise a full, Article 8-compliant review of applications for interception and how it will ensure the legality of interceptions carried out both within and outside the framework of criminal proceedings (paras. 262-263, 272-285, 286-301). This will require a root and branch reform of administrative justice in the Russian Federation.

6 September 2018