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

Press Release
issued by the Registrar of the Court

ECHR 382 (2015)
04.12.2015

Arbitrary and abusive secret surveillance of mobile telephone communications in Russia

In today's **Grand Chamber** judgment[1] in the case of **Roman Zakharov v. Russia** (application no. 47143/06) the European Court of Human Rights held, unanimously, that there had been:

a violation of Article 8 (right to respect for private life and correspondence) of the European Convention on Human Rights.

The case concerned the system of secret interception of mobile telephone communications in Russia. The applicant, an editor-in-chief of a publishing company, complained in particular that mobile network operators in Russia were required by law to install equipment enabling law-enforcement agencies to carry out operational-search activities and that, without sufficient safeguards under Russian law, this permitted blanket interception of communications.

The Court found that Mr Zakharov was entitled to claim to be a victim of a violation of the European Convention, even though he was unable to allege that he had been the subject of a concrete measure of surveillance. Given the lack of remedies available at national level, as well as the secret nature of the surveillance measures and the fact that they affected all users of mobile telephone communications, the Court considered it justified to have examined the relevant legislation not from the point of view of a specific instance of surveillance of which Mr Zakharov had been the victim, but in the abstract. Furthermore, the Court considered that Mr Zakharov did not have to prove that he was even at risk of having his communications intercepted. Indeed, given that the domestic system did not provide an effective remedy to the person who suspected that he or she was subject to secret surveillance, the very existence of the contested legislation amounted in itself to an interference with Mr Zakharov's rights under Article 8.

The Court noted that interception of communications pursued the legitimate aims of the protection of national security and public safety, the prevention of crime and the protection of the economic well-being of the country. However, in view of the risk that a system of secret surveillance set up to protect national security might undermine or even destroy democracy under the cloak of defending it, the Court had to be satisfied that there were adequate and effective guarantees against abuse.

The Court concluded that the Russian legal provisions governing interception of communications did not provide for adequate and effective guarantees against arbitrariness and the risk of abuse which was inherent in any system of secret surveillance, and which was particularly high in a system such as in Russia where the secret services and the police had direct access, by technical means, to all mobile telephone communications.

In particular, the Court found shortcomings in the legal framework in the following areas: the circumstances in which public authorities in Russia are empowered to resort to secret surveillance measures; the duration of such measures, notably the circumstances in which they should be discontinued; the procedures for authorising interception as well as for storing and destroying the intercepted data; the supervision of the interception. Moreover, the effectiveness of the remedies available to challenge interception of communications was undermined by the fact that they were available only to persons who were able to submit proof of interception and that obtaining such

1. Grand Chamber judgments are final (Article 44 of the Convention).
All final judgments are transmitted to the Committee of Ministers of the Council of Europe for supervision of their execution. Further information about the execution process can be found here: www.coe.int/t/dghl/monitoring/execution.

proof was impossible in the absence of any notification system or possibility of access to information about interception.

Principal facts

The applicant, Roman Zakharov, is a Russian national who was born in 1977 and lives in St Petersburg. He is the editor-in-chief of a publishing company and subscribed to the services of several mobile network operators.

In December 2003 Mr Zakharov brought judicial proceedings against three mobile network operators, the Ministry of Communications, and the Department of the Federal Security Service for St Petersburg and the Leningrad Region, complaining about interference with his right to privacy of his telephone communications. He maintained that, under the relevant national law – namely, the Operational-Search Activities Act of 1995 (the OSSA), the Code of Criminal Procedure of 2001 (the CCrP) and, more specifically, Order no. 70 issued by the Ministry of Communications which requires telecommunications networks to install equipment enabling law-enforcement agencies to carry out operational-search activities – the mobile operators had permitted unrestricted interception of all telephone communications by the security services without prior judicial authorisation. He asked the district court in charge to issue an injunction to remove the equipment installed under Order no. 70, and to ensure that access to telecommunications was given to authorised persons only.

The Russian courts rejected Mr Zakharov's claim. In a judgment upheld in April 2006, the district court found, in particular, that he had failed to prove that his telephone conversations had been intercepted or that the mobile operators had transmitted protected information to unauthorised persons. Installation of the equipment to which he referred did not in itself infringe the privacy of his communications.

Complaints, procedure and composition of the Court

Relying on Article 8 (right to respect for private life and correspondence) of the European Convention, Mr Zakharov complained about the system of covert interception of mobile telephone communications in Russia. He argued in particular that the relevant national law permitted the security services to intercept, through technical means, any person's communications without obtaining prior judicial authorisation, alleging that such legislation permitted blanket interception of communications. He further relied on Article 13 (right to an effective remedy), complaining that he had no effective legal remedy at national level to challenge that legislation.

The application was lodged with the European Court of Human Rights on 20 October 2006. On 11 March 2014 the Chamber to which the case had been allocated relinquished jurisdiction in favour of the Grand Chamber[2]. A Grand Chamber hearing was held on the case on 24 September 2014.

Judgment was given by the Grand Chamber of 17 judges, composed as follows:

Dean **Spielmann** (Luxembourg), *President*,
Josep **Casadevall** (Andorra),
Guido **Raimondi** (Italy),
Ineta **Ziemele** (Latvia),
Mark **Villiger** (Liechtenstein),
Luis **López Guerra** (Spain),
Khanlar **Hajiyev** (Azerbaijan),

[2] Under Article 30 of the European Convention on Human Rights, "Where a case pending before a Chamber raises a serious question affecting the interpretation of the Convention or the Protocols thereto, or where the resolution of a question before the Chamber might have a result inconsistent with a judgment previously delivered by the Court, the Chamber may, at any time before it has rendered its judgment, relinquish jurisdiction in favour of the Grand Chamber, unless one of the parties to the case objects."

Angelika **Nußberger** (Germany),
Julia **Laffranque** (Estonia),
Linos-Alexandre **Sicilianos** (Greece),
Erik **Møse** (Norway),
André **Potocki** (France),
Paul **Lemmens** (Belgium),
Helena **Jäderblom** (Sweden),
Faris **Vehabović** (Bosnia and Herzegovina),
Ksenija **Turković** (Croatia),
Dmitry **Dedov** (Russia),

and also Lawrence **Early**, *Jurisconsult.*

Decision of the Court

Article 8 (right to private life and correspondence)

The Court found that Mr Zakharov was entitled to claim to be a victim of a violation of the European Convention, even though he was unable to allege that he had been the subject of a concrete measure of surveillance. Given the secret nature of the surveillance measures provided for by the legislation, their broad scope (affecting all users of mobile telephone communications) and the lack of effective means to challenge them at national level (see point 6 below), the Court considered that it was justified to examine the relevant legislation not from the point of view of a specific instance of surveillance, but in the abstract. Furthermore, the Court considered that Mr Zakharov did not have to prove that he was even at risk of having his communications intercepted. Indeed, given that the domestic system did not afford an effective remedy to the person who suspected that he or she was subjected to secret surveillance, the very existence of the contested legislation amounted in itself to an interference with Mr Zakharov's rights under Article 8.

It was not in dispute between the parties that interception of mobile telephone communications had had a basis in Russian law, namely the OSAA, the CCrP, the Communications Act and Orders issued by the Ministry of Communications (in particular Order no. 70), and pursued the legitimate aims of the protection of national security and public safety, the prevention of crime and the protection of the economic well-being of the country.

However, the Court concluded that the Russian legal provisions governing interception of communications did not provide for adequate and effective guarantees against arbitrariness and the risk of abuse.

In particular, the Court found shortcomings in the legal framework in the following areas:

1. **The circumstances in which public authorities are empowered to resort to secret surveillance measures**

   Notably, Russian legislation lacks clarity concerning some of the categories of people liable to have their telephones tapped, namely a person who may have information about an offence or information relevant to a criminal case or those involved in activities endangering Russia's national, military, economic or ecological security. For example, as concerns the latter category, the OSAA leaves the authorities an almost unlimited degree of discretion in determining which events or acts constitute such a threat and whether that threat is serious enough to justify secret surveillance;

2. **The duration of secret surveillance measures**

   Notably the provisions on the circumstances in which secret surveillance measures must be discontinued do not provide sufficient guarantees against arbitrary interference.

Regrettably, the requirement to discontinue interception when no longer necessary is only mentioned in the CCrP and not in the OSAA. This means in practice that interception of communications in criminal proceedings have more safeguards than interceptions in connection with activities endangering Russia's national, military, economic or ecological security;

3. **The procedures for destroying and storing intercepted data**

In particular, the domestic law permits automatic storage for six months of clearly irrelevant data in cases where the person concerned has not been charged with a criminal offence and, in cases where the person has been charged with a criminal offence, it is not sufficiently clear as to the circumstances in which the intercepted material will be stored and destroyed after the end of a trial;

4. **The procedures for authorising interception**

The authorisation procedures are not capable of ensuring that secret surveillance measures are ordered only when necessary.

Most notably, Russian courts do not verify whether there is a reasonable suspicion against the person for whom interception has been requested or examine whether the interception is necessary and justified. Thus, interception requests are often not accompanied by any supporting materials, judges never request the interception agency to submit such materials and a mere reference to the existence of information about a criminal offence or activities endangering national, military, economic or ecological security is considered to be sufficient for the interception to be authorised.

Furthermore, the OSAA does not contain any requirements concerning the content either of the request for interception or of the interception authorisation, meaning that courts sometimes grant interception authorisations which do not mention a specific person or telephone number to be tapped, but authorise interception of all telephone communications in the area where a criminal offence has allegedly been committed, and on occasions without mentioning the duration of the authorised interception. Furthermore, the non-judicial urgent procedure provided by the OSAA (under which it is possible to intercept communications without prior judicial authorisation for up to 48 hours) lacks sufficient safeguards to ensure that it is used sparingly and only in duly justified cases.

Moreover, a system, such as the Russian one, which allows the secret services and the police to intercept directly the communications of each and every citizen without having to show an interception authorisation to the communications service provider, or to anyone else, is particularly prone to abuse. This system results in particular in the secret services and the police having the technical means to circumvent the authorisation procedure and intercept communications without obtaining prior judicial authorisation. The need for safeguards against arbitrariness and abuse appears therefore to be particularly great in this area;

5. **The supervision of interception**

As it is currently organised, supervision of interception does not comply with the requirements under the European Convention that supervisory bodies be independent, open to public scrutiny and vested with sufficient powers and competence to exercise effective and continuous control. Firstly, it is impossible for the supervising authority in Russia to discover interception carried out without proper judicial authorisation as Order no. 70 prohibits the logging or recording of such interception. Secondly, supervision of interception carried out on the basis of proper judicial authorisations is entrusted to the President, Parliament and the Government, who are given no indication under Russian law as to how they may supervise interception, as well as the competent prosecutors, whose

manner of appointment and blending of functions, with the same prosecutor's office giving approval to requests for interceptions and then supervising their implementation, may raise doubts as to their independence. Thirdly, the prosecutors' powers and competences are limited: notably, information about the security services' undercover agents and their tactics, methods and means remain outside their scope of supervision. Fourthly, supervision by prosecutors is not open to public scrutiny: their semi-annual reports on operational-search measures are not published or otherwise accessible to the public. Lastly, the effectiveness of supervision by prosecutors in practice is open to doubt, Mr Zakharov having submitted documents illustrating prosecutors' inability to obtain access to classified materials on interception and the Government not having submitted any inspection reports or decisions by prosecutors ordering the taking of measures to stop or remedy a detected breach in law;

6. **Notification of interception of communications and remedies available**

Any effectiveness of the remedies available to challenge interception of communications is undermined by the fact that they are available only to persons who are able to submit proof of interception. Given that a person whose communications have been intercepted in Russia is not notified at any point and does not have an adequate possibility to request and obtain information about interceptions, unless that information becomes known to him as a result of its use in evidence in eventual criminal proceedings, that burden of proof is virtually impossible to satisfy.

The Court noted that those shortcomings in the legal framework appear to have had an impact on the actual operation of the system of secret surveillance which exists in Russia. The Court was not convinced by the Government's argument that all interceptions in Russia were performed lawfully on the basis of a proper judicial authorisation. The examples submitted by Mr Zakharov in the domestic proceedings[3] and in the proceedings before the European Court of Human Rights[4] indicated the existence of arbitrary and abusive surveillance practices, which were apparently due to the inadequate safeguards provided by law.

In view of those shortcomings, the Court found that Russian law did not meet the "quality of law" requirement and was incapable of keeping the interception of communications to what was "necessary in a democratic society". There had accordingly been a violation of Article 8 of the Convention.

Other articles

Given the findings under Article 8, in particular with regard to the notification of interception of communications and available remedies, the Court held that it was not necessary to examine Mr Zakharov's complaint under Article 13 separately.

Article 41 (just satisfaction)

The Court held, by 16 votes to one, that the finding of a violation constituted in itself sufficient just satisfaction for any non-pecuniary damage sustained by Mr Zakharov. It further held that Russia was to pay Mr Zakharov 40,000 euros (EUR) in respect of costs and expenses.

[3] In the domestic proceedings Mr Zakharov referred in particular to two judicial orders, which retrospectively authorised the interception of a number of people's telephone communications, and which, in his opinion, went to prove that the mobile network operators and law-enforcement agencies routinely resorted to unauthorised interception.

[4] In order to prove that law-enforcement officials unlawfully intercepted telephone communications without prior judicial authorisation and disclosed the records, Mr Zakharov submitted to the European Court printouts from the Internet of the transcripts of politicians' private telephone conversations and news articles reporting on the fact that anyone could buy the transcript of a private telephone conversation from the police.

Separate opinions

Judge Ziemele expressed a dissenting opinion and Judge Dedov expressed a concurring opinion which are annexed to the judgment.

The judgment is available in English and French.

Press contacts
echrpress@echr.coe.int | tel.: +33 3 90 21 42 08

Tracey Turner-Tretz (tel: + 33 3 88 41 35 30)
Nina Salomon (tel: + 33 3 90 21 49 79)
Denis Lambert (tel: + 33 3 90 21 41 09)
Inci Ertekin (tel: + 33 3 90 21 55 30)