Computerrecht 2024/98

# Het EHRM acht een verplichting die er in de prakijk op neerkomt dat encryptietechnologie wordt verzwakt in strijd met artikel 8 EVRM.

EHRM 13-02-2024, ECLI:CE:ECHR:2024:0213JUD003369619, m.nt. O.L. van Daalen

| | |
|---|---|
| Instantie | Europees Hof voor de Rechten van de Mens |
| Datum | 13 februari 2024 |
| Magistraten | Pere Pastor Vilanova, President, Jolien Schukking, Yonko Grozev, Georgios A. Serghides, Peeter Roosma, Ioannis Ktistakis, Oddný Mjöll Arnardóttir |
| Zaaknummer | 33696/19 |
| Noot | O.L. van Daalen |
| JCDI | JCDI:ADS962903:1 |
| Vakgebied(en) | EU-recht (V) |
| Brondocumenten | ECLI:CE:ECHR:2024:0213JUD003369619, Uitspraak, Europees Hof voor de Rechten van de Mens, 13-02-2024 |
| Wetingang | (artikel 8 EVRM) |

**Essentie**

Het EHRM acht een verplichting die er in de prakijk op neerkomt dat encryptietechnologie wordt verzwakt in strijd met artikel 8 EVRM.

## Partij(en)

arrest in de zaak van Podchasov t. Rusland:

The European Court of Human Rights (Third Section), sitting as a Chamber composed of:

Pere Pastor Vilanova, President,

Jolien Schukking,

Yonko Grozev,

Georgios A. Serghides,

Peeter Roosma,

Ioannis Ktistakis,

Oddný Mjöll Arnardóttir, judges,

and Olga Chernishova, Deputy Section Registrar,

Having regard to:

the application (no. 33696/19) against the Russian Federation lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ('the Convention') by a Russian national, Mr Anton Valeryevich Podchasov ('the applicant'), on 18 June 2019;

the decision to give notice of the application to the Russian Government ('the Government');

the observations submitted by the Government and the observations in reply submitted by the applicant;

the comments submitted by the European Information Society Institute and Privacy International, which were granted leave to intervene by the President of the Section;

the decision of the President of the Section to appoint one of the sitting judges of the Court to act as an *ad hoc* judge, applying by analogy Rule 29 § 2 of the Rules of Court (see, for an explanation of the background, Kutayev v. Russia, no. 17912/15, §§ 5-8, 24 January 2023);

Having deliberated in private on 9 January 2024,

Delivers the following judgment, which was adopted on that date:

**Uitspraak**

**INTRODUCTION**

**1.**

The case concerns the statutory requirement for "Internet communication organisers" to store all communications data for a duration of one year and the contents 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 are encrypted.

**THE FACTS**

**2.**

The applicant was born in 1981 and lives in Barnaul. He was represented by Mr S. Darbinyan, a lawyer practising in Moscow.

**3.**

The Government were initially represented by Mr A. Fedorov, former Representative of the Russian Federation to the European Court of Human Rights, and later by his successor in that office, Mr M. Vinogradov.

**4.**

The facts of the case may be summarised as follows.

**5.**

The applicant is a user of 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. According to its official website, 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. The official site reads, in particular:

'All messages in secret chats use end-to-end encryption. This means only you and the recipient can read those messages - nobody else can decipher them, including us here at Telegram.'

**6.**

On 28 June 2017 Telegram Messenger LLP was listed as an 'Internet communications organiser' (организатор распространения информации в сети Интернет - hereinafter 'ICO') in a special public register. This entailed an obligation for Telegram to store all communications data for a duration of one year and the contents 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 (see paragraphs 17-25 below).

**7.**

On 12 July 2017 the Federal Security Service ('the FSB') required Telegram Messenger LLP to disclose technical information which would facilitate 'the decryption of communications since 12 July 2017 in respect of Telegram users who were suspected of terrorism-related activities'. The disclosure order referred to section 10.1(4.1) of the Information Act and Order no. 432 of 19 July 2016 (see paragraphs 20 and 24 below). It listed six mobile telephone numbers associated with Telegram Messenger accounts and referred to six court decisions delivered on 10 July 2017. It required Telegram Messenger LLP to submit, among other things, *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 decrypting a communication. The information was to be sent, by 19 July 2017, to the FSB's email address.

**8.**

Telegram Messenger LLP refused to comply with the disclosure order, arguing that it was technically impossible to execute it without creating a backdoor that would weaken the encryption mechanism for all users. It explained, in particular, that the six users mentioned in the disclosure order had switched on the 'secret chat' feature and therefore used end-to-end encryption. The company was fined by the Meshchanskiy District Court of Moscow on 12 December 2017. Subsequently, by a judgment of 13 April 2018, the Taganskiy District Court of Moscow ordered the blocking of the Telegram application in Russia. Both judgments were upheld on appeal.

**9.**

On 12 March 2018 the applicant together with thirty-four other persons challenged the disclosure order before

a court. The plaintiffs argued that the provision of encryption keys as required by the FSB would enable the decryption of the communications of all 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 pointed to the broad scope of section 10.1 of the Information Act (see paragraphs 16-23 below) as the legal basis for the interference and a lack of guarantees against the potentially unjustified disclosure of their personal information.

**10.**

On 22 March 2018 the Meshchanskiy District Court rejected the complaint as inadmissible, finding that the challenged disclosure order did not affect the plaintiffs' rights. The inadmissibility decision did not contain any further reasoning.

**11.**

On 22 May 2018 the Moscow City Court upheld the inadmissibility decision on appeal.

**12.**

On 10 September 2018 a judge of the Moscow City Court refused to refer a cassation appeal lodged by the applicant to the Plenary Moscow City Court for examination, finding no significant violations of substantive or procedural law which had influenced the outcome of the proceedings.

**13.**

A further cassation appeal by the applicant was rejected on 16 January 2019 by the Supreme Court of the Russian Federation.

**14.**

The Telegram Messenger application is still available and functioning in Russia.

## RELEVANT LEGAL FRAMEWORK

**15.**

For a summary of the domestic provisions on secret surveillance of communications, including the relevant provisions of the Code of Criminal Procedure and of the Operational-Search Activities Act, see Roman Zakharov v. Russia ([GC], no. 47143/06, §§ 15-138, ECHR 2015).

**16.**

Section 10.1 of Federal Law no. 149-FZ of 27 July 2006 on Information, Information Technologies and Protection of Information ('the Information Act') was introduced into that Act in 2014. It defines an ICO and lists its statutory obligations.

**17.**

An ICO is defined as 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 (section 10.1(1) of the Information Act).

**18.**

In July 2016 the following obligations of an ICO were introduced.

**19.**

An ICO must store on Russian soil all communications data generated by Internet users for a duration of one year and the contents of all communications for a duration of six months. This obligation concerns voice, textual, visual, sound, video or other electronic communications sent, received, transmitted or processed by Internet users (section 10.1(3)).

**20.**

An ICO must submit the information mentioned in section 10.1(3) to law-enforcement authorities or security services in the circumstances specified by law (section 10.1(3.1)). It must also submit any information necessary to decrypt electronic communications if they are encrypted (section 10.1(4.1)).

**21.**

Equipment installed by an ICO must meet the technical requirements set out by the government and enable law-enforcement authorities and security services to carry out their tasks (section 10.1(4)).

**22.**

In the context of the provision of instant messaging services, an ICO must, in addition to the requirements above, identify the users of such messaging services by their mobile telephone numbers (section 10.1(4.2)(1)).

**23.**

The scope of the information which must be stored pursuant to section 10.1(3), the location and conditions of storage, the procedures for providing the information to the law-enforcement authorities and security services and the procedures for the supervision of ICOs must be established by the Russian government (section 10.1(6)).

**24.**

Order no. 432 of 19 July 2016 of the FSB provides that an ICO must submit any information necessary to decrypt electronic communications within ten days after a request by a competent security services unit. The request must specify the contents (the format) of the requested information and the postal or electronic destination address (paragraphs 3-6).

**25.**

Order no. 743 of 31 July 2014 of the Russian government, as amended on 18 January 2018, provides that an ICO must grant security services remote access to its information system in order to enable them to receive the information mentioned in section 10.1(3) and (4.1) of the Information Act (paragraph 8).

**26.**

Order no. 571 of 29 October 2018 of the Ministry of Digital Development and Communications provides that an ICO must install equipment which is capable of, among other things, searching, processing and delivering to the control centre of the FSB - at the request of that control centre or automatically - the following data: the identity of registered users; the receiving, sending, delivering or processing of voice, textual, visual, sound, video or other electronic communications by Internet users; the contents of voice, textual, visual, sound, video or other electronic communications; and the information necessary to decrypt electronic communications if they are encrypted (paragraph 4). The control centre of the security services must have round-the-clock remote access to the equipment and be capable of administering it (paragraph 14).

**27.**

Government Decree no. 1526 of 23 September 2020 provides that an ICO must provide the law-enforcement authorities and security services with communications data within thirty days of a request, or within three days in urgent situations (paragraphs 8 and 9). The request must include specific information identifiers that will be used as search criteria, such as a telephone number, an email address, the information found in the communication protocol's header or other identifiers (paragraph 7).

**International material**

**United Nations**

**28.**

The Report on the right to privacy in the digital age by the Office of the United Nations High Commissioner for Human Rights, published on 4 August 2022 (A/HRC/51/17), reads as follows, in so far as relevant (footnotes omitted):

**‘B. Restrictions on encryption**

…

2 1. Encryption is a key enabler of privacy and security online and is essential for safeguarding rights, including the rights to freedom of opinion and expression, freedom of association and peaceful assembly, security, health and non-discrimination. Encryption ensures that people can share information freely, without fear that their information may become known to others, be they State authorities or cybercriminals. Encryption is essential if people are to feel secure in freely exchanging information with others on a range of experiences, thoughts and identities, including sensitive health or financial information, knowledge about gender identities and sexual orientation, artistic expression and information in connection with minority status. In environments of prevalent censorship, encryption enables individuals to maintain a space for holding, expressing and exchanging opinions with others. In specific instances, journalists and human rights defenders cannot do their work without the protection of robust encryption, shielding their sources and sheltering them from the powerful actors under investigation. Encryption provides women, who face particular threats of surveillance, harassment and violence online, an important level of protection against involuntary disclosure of information. In armed conflicts, encrypted messaging is indispensable to ensuring secure communication among civilians. It is notable that in the two months after the beginning of the armed conflict in Ukraine on 24 February 2022, the number of downloads in Ukraine of the encrypted messaging app Signal went up by over 1,000 per cent compared with preceding months.

…

2 3. In spite of its benefits, Governments sometimes restrict the use of encryption, for example for the protection of national security and combating crime, in particular to detect child sexual abuse material. Restrictions include bans on encrypted communications and criminalization for offering or using encryption tools or mandatory registration and licensing of encryption tools. Similarly, in some instances, encryption providers have been required to ensure that law enforcement or other government agencies have access to all communications upon request, which can effectively amount to a blanket restriction of encryption that could require, or at least encourage, the creation of some sort of back door (a built-in path to bypass encryption, allowing for covert access to data in plain text). Another form of interference with encryption is the requirement that key escrow systems be created and maintained, and all private keys needed to decrypt data be handed over to the Government or a designated third party. The imposition of traceability requirements, according to which providers need to be able to trace any message back to its supposed originator, could also require the weakening of encryption standards. Recently, various States have started imposing or considering general monitoring obligations for providers of digital communications, including those offering encrypted communications services. Such duties could effectively force those providers to abandon strong end-to-end encryption or to identify highly problematic workarounds (see paras. 27-28 below).

2 4. There is no doubt that widely used encryption capabilities, capabilities that the public has demanded as a response to mass surveillance and cybercrime, create a dilemma for Governments seeking to protect populations, in particular their most vulnerable members, against serious crime and security threats. However, as pointed out by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, regulation of encryption risks undermining human rights. Governments seeking to limit encryption have often failed to show that the restrictions they would impose are necessary to meet a particular legitimate interest, given the availability of various other tools and approaches that provide the information needed for specific law enforcement or other legitimate purposes. Such alternative measures include improved, better-resourced traditional policing, undercover operations, metadata analysis and strengthened international police cooperation.

2 5. Moreover, the impact of most encryption restrictions on the right to privacy and associated rights are disproportionate, often affecting not only the targeted individuals but the general population. Outright bans by Governments, or the criminalization of encryption in particular,

cannot be justified as they would prevent all users within their jurisdictions from having a secure way to communicate. Key escrow systems have significant vulnerabilities, since they depend on the integrity of the storage facility and expose stored keys to cyberattacks. Moreover, mandated back doors in encryption tools create liabilities that go far beyond their usefulness with regard to specific users identified as crime suspects or security threats. They jeopardize the privacy and security of all users and expose them to unlawful interference, not only by States, but also by non-State actors, including criminal networks. Licensing and registration requirements have similar disproportionate effects as they require that encryption software contain exploitable weaknesses. Such adverse effects are not necessarily limited to the jurisdiction imposing the restriction; rather it is likely that back doors, once established in the jurisdiction of one State, will become part of the software used in other parts of the world.

2 6. … Since the content of messages, once encrypted, cannot be accessed by anyone except the sender and the recipient, any general monitoring obligation would force service providers to either abandon transport encryption or seek access to messages before they are encrypted …'

**Council of Europe**

**29.**

Appendix to Recommendation by the Committee of Ministers of the Council of Europe on the protection of human rights with regard to social networking services (CM/Rec(2012)4, adopted on 4 April 2012) reads as follows:

'1 5. In co-operation with the private sector and civil society, member States, in addition to the measures stated in section I of this appendix, should take appropriate measures to ensure that users' right to private life is protected, in particular by engaging with social networking providers to carry out the following actions:

…

- ensure that the most appropriate security measures are applied to protect personal data against unlawful access by third parties. This should include measures for the end-to-end encryption of communication between the user and the social networking services website …'

**30.**

The Council of Europe Parliamentary Assembly Resolution 2045 (2015) on mass surveillance, adopted on 21 April 2015, reads as follows, in so far as relevant:

'5. The Assembly is deeply worried about threats to Internet security by the practices of certain intelligence agencies, disclosed in the Snowden files, of seeking out systematically, using and even creating 'back doors' and other weaknesses in security standards and implementation that could easily be exploited by terrorists and cyberterrorists or other criminals.

6. It is also worried about the collection of massive amounts of personal data by private businesses and the risk that these data may be accessed and used for unlawful purposes by State or non-State actors. …

8. … High-technology surveillance tools are already in use in a number of authoritarian regimes and are used to track down opponents and to suppress freedom of information and expression.

In this regard, the Assembly is deeply concerned about recent legislative changes in the Russian Federation which offer opportunities for enhanced mass surveillance through social networks and Internet services.

9. In several countries, a massive ‘surveillance-industrial complex’ has evolved, fostered by the culture of secrecy surrounding surveillance operations, their highly technical nature and the fact that both the seriousness of alleged threats and the need for specific counter-measures and their costs and benefits are difficult to assess for political and budgetary decision makers without relying on input from the interested groups themselves. There is a risk that these powerful structures could escape democratic control and accountability and threaten the free and open nature of our societies …

1 1. The Assembly recognises the need for effective, targeted surveillance of suspected terrorists and other organised criminal groups. Such targeted surveillance can be an effective tool for law enforcement and crime prevention. At the same time, it notes that, according to independent reviews carried out in the United States, mass surveillance does not appear to have contributed to the prevention of terrorist attacks, contrary to earlier assertions made by senior intelligence officials. Instead, resources that might prevent attacks are diverted to mass surveillance, leaving potentially dangerous persons free to act …

1 9. The Assembly therefore urges the Council of Europe member and observer States to:

1 9. 1 ensure that their national laws only allow for the collection and analysis of personal data (including so-called metadata) with the consent of the person concerned or following a court order granted on the basis of reasonable suspicion of the target being involved in criminal activity; unlawful data collection and processing should be penalised in the same way as the violation of the traditional confidentiality of correspondence; the creation of ‘back doors’ or any other techniques to weaken or circumvent security measures or exploit their existing weaknesses should be strictly prohibited; all institutions and businesses holding personal data should be required to apply the most effective security measures available;

1 9. 2 ensure, in order to enforce such a legal framework, that their intelligence services are subject to adequate judicial and/or parliamentary control mechanisms …

1 9. 5 promote the further development of user-friendly (automatic) data protection techniques capable of countering mass surveillance and any other threats to Internet security, including those posed by non-State actors …’

**European Union**

**31.**

The judgment given by the Court of Justice of the European Union (CJEU) on 8 April 2014 in the joined cases of Digital Rights Ireland and Seitinger and Others (C-293/12 and C-594/12, EU:C:2014:238) declared the Data Retention Directive 2006/24/EC invalid. The Directive laid down an obligation on the providers of publicly available electronic communication services or of public communications networks to retain all traffic and location data for periods from six months to two years, in order to ensure that the data were available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each member State in its national law. For a summary of that judgment and further developments in the case-law of the CJEU, see Big Brother Watch and Others v. the United Kingdom [GC], nos. 58170/13 and 2 others, §§ 209-41, 25 May 2021.

**32.**

The CJEU also held, in its judgment of 6 October 2015 in the case of *Maximillian Schrems v. Data Protection Commissioner* (C-362/14, EU:C:2015:650), as follows:

> ‘9 4. In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter …’

**33.**

A Joint Statement by Europol and the European Union Agency for Cybersecurity (ENISA) of 20 May 2016 on lawful criminal investigation that respects 21st Century data protection reads:

‘Intercepting an encrypted communication or breaking into a digital service might be considered as proportional with respect to an individual suspect, but breaking the cryptographic mechanisms might cause collateral damage. The focus should be on getting access to the communication or information; not on breaking the protection mechanism. The good news is that the information needs to be unencrypted at some point to be useful to the criminals. This creates opportunities for alternatives such as undercover operations, infiltration into criminal groups, and getting access to the communication devices beyond the point of encryption, for instance by means of live forensics on seized devices or by lawful interception on those devices while still used by suspects. Moreover, forensic methods that make use of physical fingerprints of devices might not help to intercept the communication content itself, but might provide other important clues for the investigator. Even so, there are cases in which there are no such alternatives and access to the concealed content can only be gained by a form of decryption.

While no practical encryption mechanism is perfect in its design and implementation, decryption appears to be less and less feasible for law enforcement purposes. This has led to proposals to introduce mandatory backdoors or key escrow to weaken encryption. While this would give investigators lawful access in the event of serious crimes or terrorist threats, it would also increase the attack surface for malicious abuse, which, consequently, would have much wider implications for society. Moreover, criminals can easily circumvent such weakened mechanisms and make use of the existing knowledge on cryptography to develop (or buy) their own solutions without backdoors or key escrow …

Solutions that intentionally weaken technical protection mechanisms to support law enforcement will intrinsically weaken the protection against criminals as well, which makes an easy solution impossible …

When circumvention is not possible yet access to encrypted information is imperative for security and justice, then feasible solutions to decryption without weakening the protective mechanisms must be offered, both in legislation and through continuous technical evolution. For the latter, the fostering of close cooperation with industry partners, as well as the research community with expertise in crypto-analyses for the breaking of encryption where lawfully indicated, is strongly advised. We are convinced that a solution that strikes a sensible and workable balance between individual rights and protection of EU citizen's security interests can be found. In this respect, the deployment of European R&D instruments may drive this collaboration while at the same time EU Agencies can work closely together in establishing best practices.’

**34.**

On 28 July 2022 the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) adopted Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse. It provides as follows (footnotes omitted):

**‘Executive summary**

… measures permitting the public authorities to have access on a generalised basis to the content of a communication in order to detect solicitation of children are more likely to affect the essence of the rights guaranteed in Articles 7 and 8 of the Charter …

The EDPB and EDPS also express doubts regarding the efficiency of blocking measures and consider that requiring providers of internet services to decrypt online communications in order to block those concerning CSAM [child sexual abuse material] would be disproportionate.

Furthermore, the EDPB and EDPS point out that encryption technologies contribute in a fundamental way to the respect for private life and confidentiality of communications, freedom of expression as well as to innovation and the growth of the digital economy, which relies on the high level of trust and confidence that such technologies provide. Recital 26 of the Proposal places not only the choice of detection technologies, but also of the technical measures to protect confidentiality of communications, such as encryption, under a caveat that this technological choice must meet the requirements of the proposed Regulation, i.e., it must enable detection. This supports the notion gained from Articles 8(3) and 10(2) of the Proposal that a provider cannot refuse execution of a detection order based on technical impossibility. The EDPB and EDPS consider that there should be a better balance between the societal need to have secure and private communication channels and to fight their abuse. It should be clearly stated in the Proposal that nothing in the proposed Regulation should be interpreted as prohibiting or weakening encryption …

4.10. Impact on encryption

96. European data protection authorities have consistently advocated for the widespread availability of strong encryption tools and against any type of backdoors. This is because encryption is important to ensure the enjoyment of all human rights offline and online. Moreover, encryption technologies contribute in a fundamental way both to the respect for private life and confidentiality of communications …

97. In the context of interpersonal communications, end-to-end encryption ('E2EE') is a crucial tool for ensuring the confidentiality of electronic communications, as it provides strong technical safeguards against access to the content of the communications by anyone other than the sender and the recipient(s), including by the provider. Preventing or discouraging in any way the use of E2EE, imposing on service providers an obligation to process electronic communication data for purposes other than providing their services, or imposing on them an obligation to proactively forward electronic communications to third parties would entail the risk that providers offer less encrypted services in order to better comply with the obligations, thus weakening the role of encryption in general and undermining the respect for the fundamental rights of European citizens. It should be noted that while E2EE is one of the most commonly used security measures in the context of electronic communications, other technical solutions (e.g., the use of other cryptographic schemes) might be or become equally important to secure and protect the confidentiality of digital communications. Thus, their use should not be prevented or discouraged too.

98. The deployment of tools for the interception and analysis of interpersonal electronic communications is fundamentally at odds with E2EE, as the latter aims to technically guarantee that a communication remains confidential between the sender and the receiver …

100. The impact of degrading or discouraging the use of E2EE, which may result from the Proposal needs to be assessed properly. Each of the techniques for circumventing the privacy preserving nature of E2EE presented in the Impact Assessment Report that accompanied the Proposal would introduce security loopholes. For example, client-side scanning would likely lead to substantial, untargeted access and processing of unencrypted content on end user's devices … At the same time, server-side scanning, is also fundamentally incompatible with the E2EE paradigm, since the communication channel, encrypted peer-to-peer, would need to be broken, thus leading to the bulk processing of personal data on the servers of the providers.

101. While the Proposal states that it 'leaves to the provider concerned the choice of the

0 technologies to be operated to comply effectively with detection orders and should not be
1. understood as encouraging or discouraging the use of any given technology', the structural incompatibility of some detection orders with E2EE becomes in effect a strong disincentive to use E2EE. The inability to access and use services using E2EE (which constitute the current state of the art in terms of technical guarantee of confidentiality) could have a chilling effect on freedom of expression and the legitimate private use of electronic communication services …'

## THE LAW

### preliminary issues

**35.**

The applicant's complaints concern the continuous storage of Internet communications and related communications data by ICOs, the authorities' potential access to these data and the ICOs' obligation to decrypt them if they are encrypted, pursuant to the Information Act and its regulations on implementation. The Court will examine the Convention compliance of the contested law on the date of its examination of the admissibility of the applicant's complaints (see Big Brother Watch and Others v. the United Kingdom [GC], nos. 58170/13 and 2 others, §§ 268-70, 25 May 2021). The Court decides that it has jurisdiction to examine the present application in so far as the facts giving rise to the alleged violations of the Convention occurred prior to 16 September 2022 - the date on which the Russian Federation ceased to be a party to the Convention (see Fedotova and Others v. Russia [GC], nos. 40792/10 and 2 others, §§ 68-73, 17 January 2023; Pivkina and Others v. Russia (dec.), no. 2134/23 and 6 others, § 61, 6 June 2023; and N.F. and Others v. Russia, nos. 3537/15 and 8 others, § 30, 12 September 2023).

### ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

**36.**

The applicant complained about the statutory requirement for ICOs to store the content of all Internet communications and related communications data, and to submit those data to law-enforcement authorities or security services at their request together with information necessary to decrypt electronic messages if they were encrypted. He relied on Article 8 of the Convention, which reads as follows:

'1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

#### Admissibility

37.
The Court notes that this complaint is neither manifestly ill-founded nor inadmissible on any other grounds listed in Article 35 of the Convention. It must therefore be declared admissible.

**Merits**

Submissions by the parties
(a) The applicant

38.
The applicant submitted that the statutory requirement for ICOs to store the contents of all online communications, coupled with the requirement to provide encryption keys at the request of law-enforcement authorities, amounted to an interference with the applicant's right to respect for his private life and correspondence. Moreover, it was technically impossible to provide the authorities with encryption keys associated with specific users of the Telegram messenger application. Any disclosure of encryption keys therefore affected the privacy of the correspondence of all Telegram users.

39.
The applicant further argued that the domestic law provisions requiring the storage of the contents of all online communications and the provision of encryption keys to the law-enforcement authorities were not foreseeable in their application and did not contain effective guarantees against arbitrariness. In particular, the domestic authorities did not need judicial authorisation to request encryption keys. Although the disclosure order of 12 July 2017 had mentioned that there had been judicial authorisations in respect of the six telephone numbers concerned, the judicial authorisations had never been shown to the Telegram Messenger company, to the domestic courts examining the company's or the applicant's cases or to the public.
(b) The Government

40.
The Government submitted that there had been no interference with the applicant's rights. The applicant had failed to demonstrate that there was a ‘reasonable likelihood’ that the security services had compiled and retained information concerning his private life. As regards Telegram encryption keys, Order no. 432 (see paragraph 24 above) did not contain a requirement to provide encryption keys to decrypt all traffic. Encryption keys were to be provided upon a request for specific data. The request for encryption keys of 12 July 2017 contested by the applicant had concerned communications involving six telephone numbers belonging to suspected terrorists and judicial authorisation had been obtained. The applicant's allegations that the security services had access to the communications of all users were therefore unsubstantiated.

41.
In the alternative, the Government submitted that the alleged interference had a basis in domestic law. The domestic legal provisions were accessible and foreseeable in their effects. Any interception of communications had to be authorised by a court. Interception of communications could only be conducted following the receipt of information that a criminal offence had been committed, was being committed or was being plotted; about persons conspiring to commit, or committing, or having committed a criminal offence; or about events or activities endangering the national, military, economic or ecological security of the Russian Federation. Only offences of medium severity, serious offences and especially serious offences might give rise to an interception order and only persons suspected of such offences or who might have information about such offences could be subject to interception measures. Records of intercepted communications had to be stored under conditions excluding any risk of their being listened to or copied by unauthorised persons (the Government cited domestic legal provisions summarised in *Roman Zakharov v. Russia*, [GC], no. 47143/06, §§ 31-33 and 51, ECHR 2015). The procedures to be followed for examining, using, storing and destroying the data obtained set out in the domestic law contained the necessary safeguards against abuses of power.

42.
The Government further argued that the provision of encryption keys to the FSB did not mean that the information necessary to decrypt encrypted electronic communications would become available to its entire staff. The heads of relevant services were responsible for making sure that their staff acted within the bounds established by the requirements of their duties. In any event, the FSB staff were bound by the duty of discretion in respect of information about private life that became known to them in the performance of their duties. Encryption keys served to decrypt communications in respect of which a judicial interception authorisation had been obtained.

43.
Lastly, the Government submitted that the interference was ‘necessary in a democratic society’ to achieve the legitimate aim of combating terrorism. For example, in April 2017 a terrorist attack had occurred in St Petersburg. Subsequently, in December 2017, another attack had been prevented. In both cases, the attacks had been coordinated from abroad through secret chats via Telegram.
(c) Third parties
(i) European Information Society Institute (EISI)

44.
EISI explained that end-to-end encryption was a mathematics-based tool which worked as follows: with the help of a ‘public’ key, any message (‘plaintext’) was translated into a seemingly random combination of letters, numbers or symbols (‘ciphertext’). Only the senders and receivers could see the plaintext, whereas outsiders could only see the ciphertext. The message in ciphertext could not be translated back into plaintext without the ‘private’ key, which was kept securely on the receiver's device. The conversion into plaintext took place directly on the receiver's device. End-to-end encryption ensured that the operator of the messaging service never had access to either the private key or the original plaintext message at any point, preventing any access to the exchanged content.

45.
EISI further argued that the FSB's disclosure order to Telegram amounted to a ‘backdoor order’ which indiscriminately affected all users of Telegram. Compliance with that order would essentially mean that Telegram would have to centrally store ‘private’ keys, that is, it would be unable to legally provide end-to-end encrypted services to its users.

46.
EISI submitted that encryption used by messaging services was a self-defence mechanism against surveillance. It played a vital role in ensuring the integrity and security of messages during transmission. It offered essential protection to vulnerable individuals, such as journalists, opposition leaders or victims of cyber abuse. There was therefore a strong connection between encryption and human rights, particularly Articles 8 and 10 of the Convention. Introducing backdoors in encrypted communications would weaken that defence mechanism and pose security risks.

47.
EISI argued against the necessity and proportionality of requiring backdoor access to all encrypted messages because it compromised the privacy of all users for the sake of a small number of suspects. It made all users vulnerable to unauthorised State surveillance, cybercriminal activities and other malicious actors. Even if these risks did not materialise, the knowledge of such threats created a chilling effect, making authors, researchers, journalists and opposition activists hesitant to speak up or communicate with their sources. EISI also submitted that less intrusive targeted alternatives to combat crime and protect national security existed, such as, among other things, using live forensics on seized devices, guessing or obtaining private keys held by parties to the communication, using vulnerabilities in the target's software or sending an implant to targeted devices. While indiscriminate backdoors might be cheaper for the State than alternative investigative measures, they were expensive for society at large on account of the security risks they produced. The fact that the alternative methods were significantly more difficult to use on a large scale on account of their labour intensiveness, cost and logistical complexity should be viewed positively as hurdles forcing the prioritisation and targeting of measures.
(ii) Privacy International

48.
Privacy International gave a similar description of how end-to-end encryption worked. As the encryption and decryption of messages sent and received occurred on users' devices, end-to-end encryption ensured that only the intended recipients, and not even the communication service provider, had access to the message content. The ‘private’ key used to decrypt the message by the receiver was kept on the receiver's device and was not shared with anyone.

49.
Privacy International further submitted that the measures required by the contested legislation that involved

retaining and decrypting encrypted communications contradicted the national authorities' obligations to safeguard the confidentiality, privacy, security and integrity of communication and information technology systems. The implementation of such measures would force service providers, like Telegram, to make radical changes to their software and weaken the encryption schemes used. An obligation to decrypt encrypted communications compelled communications services providers to modify their existing services by creating backdoors which, once found, could be easily exploited by both legitimate and criminal actors. In other words, in the case of end-to-end encryption the only way for a communication services provider to comply with the obligation to decrypt communications would be to issue a software update that could not be targeted at specific users and would therefore indiscriminately affect all users of the application or service in question. Requiring telecommunication service providers to create software backdoors for indiscriminate access to encrypted communications could not therefore be limited to what was ‘necessary in a democratic society’.
The Court's assessment
(a) Existence of an interference and its scope

50.
The Court notes at the outset that the present case concerns the statutory requirement for ICOs to store the content of all Internet communications and related communications data, give law-enforcement authorities or security services access to those data at their request, and decrypt electronic messages if they are encrypted.

51.
As regards the storage by ICOs of Internet communications and related communications data, the Court reiterates that the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding. However, in determining whether the personal information retained by the authorities involves any of the various private-life aspects, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained (see S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, § 67, ECHR 2008).

52.
The Court finds that the storage by the applicant's ICO of the contents of all his Internet communications and related communications data interfered with his right to respect for his private life and correspondence (see paragraph 19 above for the domestic provisions; compare Breyer v. Germany, no. 50001/12, § 81, 30 January 2020, and Ekimdzhiev and Others v. Bulgaria, no. 70078/12, §§ 372 and 373, 11 January 2022). This storage amounts to an interference with his Article 8 rights, irrespective of whether the retained data were then accessed by the authorities. The storage, although carried out by private persons - the ICOs - is required by law; it follows that the interference is attributable to the Russian State (see Ekimdzhiev and Others, cited above, §§ 372 and 375).

53.
The Court further observes that the interference complained of relates not only to the storage of the data described above but also to the potential for national authorities to access those data (compare Breyer, § 61, and Ekimdzhiev and Others, § 376, both cited above).

54.
It is true that there is no evidence that the authorities accessed the applicant's data stored by Telegram. Since it is impossible for an individual or a legal person to know for certain whether their data has been accessed, it is appropriate to analyse the question whether the applicant may claim that he is a victim of interference with his rights under Article 8 owing to the mere existence of laws permitting authorities to do so with reference to the same criteria as the ones used in relation to secret surveillance (see Ekimdzhiev and Others, cited above, § 376).

55.
In Roman Zakharov (cited above), the Court has examined Russian legislation on secret surveillance and found that, having regard to the secret nature of the surveillance measures, the broad scope of their application, affecting all users of communications networks, and the lack of effective means to challenge the alleged application of secret surveillance measures at domestic level, the mere existence of legislation

permitting secret surveillance constitutes an interference with a user's private life (see Roman Zakharov, cited above, §§ 170-79). It finds no reasons to hold otherwise in the present case, as the Government have confirmed that access to retained Internet communications and related communications data is governed by the same legal regime which was examined in Roman Zakharov. The mere existence of the contested legislation therefore amounts in itself to an interference with the exercise of the applicant's rights under Article 8 (compare Ekimdzhiev and Others, cited above, §§ 383-84).

56.
Lastly, as regards the ICOs' statutory obligation to decrypt communications if they are encrypted (see paragraphs 20 and 24 above), the Court observes that the parties' observations on this issue are limited to end-to-end encrypted communications, that is, in the case of Telegram, communications through ‘secret chats’ (see paragraph 5 above). The parties did not make any submissions in respect of the encryption scheme used in ‘cloud chats’ and the Court will therefore not examine it.

57.
The applicant argued that it was technically impossible to provide the authorities with encryption keys associated with specific users of the Telegram messenger application. In order to enable the decryption of end-to-end encrypted communications it would be necessary to weaken the encryption technology used by the Telegram messenger application. However, because these measures could not be limited to specific individuals, they would affect everyone indiscriminately. This argument is based on the submissions by the Telegram company in the domestic proceedings (see paragraph 8 above). The applicant's position is corroborated by the third-party interveners (see paragraphs 44, 45, 48 and 49 above) and is also supported by international material (see, in particular, paragraphs 28 and 34 above). The Government, by contrast, did not provide any arguments or information capable of refuting the applicant's submissions that the measures ICOs would have to take to comply with the statutory obligation to decrypt end-to-end encrypted communications would affect all users of their services. The Court accordingly accepts that the applicant was affected by the contested legal provisions.

58.
The Court concludes that the continuous storage of the applicant's Internet communications and related communications data by Telegram, the authorities' potential access to these data and Telegram's obligation to decrypt them if they are encrypted, pursuant to the Information Act and its implementing regulations, amounted to an interference with the applicant's Article 8 rights.

59.
The Court observes in addition that in the present case personal data are 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.
(b) Justification for the interference
(i) General principles

60.
The Court finds that although the case falls to be examined primarily from the standpoint of the storage of the applicant's personal data, it must also be considered, where appropriate, in the light of the Court's case-law on secret surveillance (see paragraph 59 above). The applicable safeguards are in any event essentially similar and should offer effective guarantees against the inherent risk of abuse and keep the interference with the rights protected by Article 8 to what is ‘necessary in a democratic society’ (see Ekimdzhiev and Others, cited above, §§ 291-93 and 395, with further references).

61.
The Court reiterates that any interference can only be justified under Article 8 § 2 if it is in accordance with the law, pursues one or more of the legitimate aims to which paragraph 2 of Article 8 refers and is necessary in a democratic society in order to achieve any such aim. The wording ‘in accordance with the law’ requires the impugned measure to have some basis in domestic law. It must also be compatible with the rule of law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must therefore be accessible to the person concerned and foreseeable as to its effects (see Roman

Zakharov, cited above, §§ 227-28).

62.
The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article. The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes (see S. and Marper, cited above, § 103, and, in the context of bulk interception of communications, Big Brother Watch and Others, cited above, § 330), and especially where the technology available is continually becoming more sophisticated (see, in the context of storage of personal data, Uzun v. Germany, no. 35623/05, § 61, ECHR 2010 (extracts); Catt v. the United Kingdom, no. 43514/15, § 114, 24 January 2019; and Gaughran v. the United Kingdom, no. 45245/15, § 86, 13 February 2020; see also, in the context of secret surveillance, Roman Zakharov, § 229, and Big Brother Watch and Others, § 333, both cited above). The protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern technologies in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such technologies against important private-life interests (see, mutatis mutandis, S. and Marper, cited above, § 112).

63.
In the context of the collection and processing of personal data, it is essential to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness (ibid., § 99; see also P.N. v. Germany, no. 74440/17, § 62, 11 June 2020). The domestic law should notably ensure that retained data are relevant and not excessive in relation to the purposes for which they are stored, and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored. The domestic law must also afford adequate guarantees that retained personal data were efficiently protected from misuse and abuse (see S. and Marper, cited above, § 103). The core principles of data protection require the retention of data to be proportionate in relation to the purpose of collection and insist on limited periods of storage (ibid., § 107).

64.
In the context of secret surveillance, where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. To meet the requirement of ‘foreseeability’, the domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures. Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (see Roman Zakharov, cited above, §§ 229-30). For a detailed description of safeguards that should be set out in law for it to meet the ‘quality of law’ requirements and to ensure that secret surveillance measures are applied only when ‘necessary in a democratic society’, see Roman Zakharov, §§ 231-34, and Big Brother Watch and Others, §§ 335-39, both cited above.

65.
Lastly, the Court reiterates that confidentiality of communications is an essential element of the right to respect for private life and correspondence, as enshrined in Article 8. Users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, although such a guarantee 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 (see K.U. v. Finland, no. 2872/02, § 49, ECHR 2008, and Delfi AS v. Estonia [GC], no. 64569/09, § 149, ECHR 2015).
(ii) Application of the above principles in the present case

66.

The Court considers that in the present case the questions of lawfulness and of the existence of a legitimate aim cannot be dissociated from the question of whether the interference was ‘necessary in a democratic society’ (see, in respect of the storage of personal data, S. and Marper, § 99; Breyer, § 85; and Ekimdzhiev and Others, § 420, all cited above; see also, in respect of secret surveillance, Roman Zakharov, § 236, and Big Brother Watch and Others, § 334, both cited above). It will therefore examine them together below.

67.
The retention and storage of Internet communications and related communications data in the present case had a legal basis in the Information Act (see paragraph 19 above), which must be read in conjunction with the legal provisions governing the law-enforcement authorities' access to the data stored and their further use, as set out in the Information Act, the Code of Criminal Procedure and the Operational-Search Activities Act (see paragraphs 15 and 25 above; see also, for similar reasoning, Breyer, cited above, §§ 85 and 97).

68.
The Court further notes that while technological capabilities have greatly increased the volume of communications traversing the global Internet, the threats being faced by Contracting States and their citizens have also proliferated. These include, but are not limited to, global terrorism, drug trafficking, human trafficking and the sexual exploitation of children. Many of these threats come from international networks of hostile actors with access to increasingly sophisticated technology enabling them to communicate undetected (see Big Brother Watch and Others, cited above, § 323). The Court is satisfied that the contested legal provisions pursued the legitimate aims of protecting national security, preventing disorder and crime and protecting the rights and freedoms of others.

69.
Therefore, it remains to be considered 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’.
(α) Storage of Internet communications and communications data

70.
The Court notes that in the current, increasingly digital age, technological capabilities have greatly increased the volume of Internet communications so that a significant part of communications take digital form. The contested legislation requires the continuous automatic retention and storage of the contents of all Internet communications for a duration of six months and the related communications data for a duration of one year. It applies to all Internet communication services used to transmit voice, textual, visual, sound, video or other electronic communications (see paragraph 19 above). It affects all users of Internet communications, even in the absence of a reasonable suspicion of involvement in criminal activities or activities endangering national security, or of any other reasons to believe that retention of data may contribute to fighting serious crime or protecting national security. It covers the contents of all communications and all communications data without any circumscription of the scope of the measure in terms of territorial or temporal application or categories of persons liable to have their personal data stored. The Court is struck by the extremely broad duty of retention provided by the contested legislation and concludes that the interference is exceptionally wide-ranging and serious (compare Ekimdzhiev and Others, cited above, § 394, concerning retention of communications data only).

71.
Taking into account the seriousness of the interference, the Court will examine with particular attention whether the domestic law provides adequate and sufficient safeguards against abuse relating to the access by the law-enforcement authorities to the Internet communications and related communications data stored by ICOs pursuant to the Information Act.
(β) Potential access to the stored data for the purposes of targeted secret surveillance

72.
As regards the statutory requirement to give law-enforcement authorities or security services access to the stored data at their request, the Court reiterates that access to the data in individual cases must be accompanied, mutatis mutandis, by the same safeguards as secret surveillance (see Ekimdzhiev and Others, cited above, § 395). It takes note of the Government's argument that access has to be authorised by a court. It observes, however, that 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. Indeed, pursuant to orders issued by the government, ICOs must install equipment giving the security services direct access to the data stored (see paragraphs 24-26 above). The law-enforcement authorities thus have direct remote access to all Internet communications and related communications data.

73.
The Court considers that the requirement to show an authorisation to the communications service provider before obtaining access to a person's communications is an important safeguard against abuse by the law-enforcement authorities, ensuring that proper authorisation is obtained in all cases of secret surveillance. The manner in which the access to the stored data is organised in Russia gives the security services technical means to circumvent the authorisation procedure and to access stored Internet communications and communications data without obtaining prior judicial authorisation. Although the possibility of improper action by a dishonest, negligent or overzealous official can never be completely ruled out whatever the system, the Court considers that a system, such as the Russian one, which enables the secret services to access directly the Internet communications of each and every citizen without requiring them to show an interception authorisation to the communications service provider, or to anyone else, is particularly prone to abuse. The need for safeguards against arbitrariness and abuse appears therefore to be particularly great (see Roman Zakharov, cited above, §§ 269-70).

74.
The Government have confirmed that access to retained Internet communications and related communications data is governed by the same legal regime which was examined in Roman Zakharov (cited above) in the context of interceptions of mobile telephone communications. In that case the Court found that Russian legal provisions governing secret surveillance measures did not meet the ‘quality of law’ requirement because they did not provide for adequate and effective guarantees against arbitrariness and the risk of abuse. They were therefore incapable of keeping the ‘interference’ to what was ‘necessary in a democratic society’. It found, in particular, that the circumstances in which public authorities were empowered to resort to secret surveillance measures for the purposes of detecting, preventing and investigating criminal offences or protecting Russia's national, military, economic or ecological security were not defined with sufficient clarity. The authorisation procedures were not capable of ensuring that secret surveillance measures were ordered only when ‘necessary in a democratic society’. The supervision of interceptions did not comply with the requirements of independence, powers and competence which were sufficient to exercise effective and continuous control, public scrutiny and effectiveness in practice. The effectiveness of the remedies was undermined by the absence of notification at any point of secret surveillance, or adequate access to documents relating to secret surveillance (see Roman Zakharov, cited above, §§ 243-305).

75.
The Court does not see any reason to reach a different conclusion in the present case. It therefore finds that the domestic law does not provide for adequate and sufficient safeguards against abuse relating to the access by the law-enforcement authorities to the Internet communications and related communications data stored by ICOs pursuant to the Information Act.
(γ) Statutory requirement to decrypt communications

76.
Lastly, as regards the requirement to submit to the security services information necessary to decrypt electronic communications if they are encrypted, the Court observes 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 (see paragraphs 28 and 34 above). 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. This should be given due consideration when assessing measures which may weaken encryption.

77.

As noted above (see paragraph 57 above), it appears 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 backdoors would apparently make it technically possible to perform routine, general and indiscriminate surveillance of personal electronic communications. Backdoors may also be exploited by criminal networks and would seriously compromise the security of all users' electronic communications. The Court takes note of the dangers of restricting encryption described by many experts in the field (see, in particular, paragraphs 28 and 34 above).

78.
The Court accepts that encryption can also be used by criminals, which may complicate criminal investigations (see Yüksel Yalçınkaya v. Türkiye [GC], no. 15669/20, § 312, 26 September 2023). However, it takes note in this connection of the calls for alternative ‘solutions to decryption without weakening the protective mechanisms, both in legislation and through continuous technical evolution’ (see, on the possibilities of alternative methods of investigation, the Joint Statement by Europol and the European Union Agency for Cybersecurity, cited in paragraph 33 above, and paragraph 24 of the Report on the right to privacy in the digital age by the Office of the United Nations High Commissioner for Human Rights, cited in paragraph 28 above; see also the explanation by third-party interveners in paragraph 47 above).

79.
The Court concludes that in the present case the ICO's statutory obligation to decrypt end-to-end encrypted communications risks amounting to a requirement that providers of such services weaken the encryption mechanism for all users; it is accordingly not proportionate to the legitimate aims pursued.
(δ) Conclusion

80.
The Court concludes from the foregoing that the contested legislation providing for the retention of all Internet communications of all users, the security services' direct access to the data stored without adequate safeguards against abuse and the requirement to decrypt encrypted communications, as applied to end-to-end encrypted communications, cannot be regarded as necessary in a democratic society. In so far as this legislation permits the public authorities to have access, on a generalised basis and without sufficient safeguards, to the content of electronic communications, it impairs the very essence of the right to respect for private life under Article 8 of the Convention. The respondent State has therefore overstepped any acceptable margin of appreciation in this regard.

81.
There has accordingly been a violation of Article 8 of the Convention.

## ALLEGED VIOLATION OF ARTICLE 13 OF THE CONVENTION

**82.**

The applicant complained under Article 13 of the Convention that he did not have at his disposal an effective domestic remedy for his complaint under Article 8. Having regard to the facts of the case, the submissions of the parties and its findings under Article 8, the Court considers that there is no need to give a separate ruling on the admissibility and the merits of the complaint under Article 13 (see Centre for Legal Resources on behalf of Valentin Câmpeanu v. Romania [GC], no. 47848/08, § 156, ECHR 2014).

## APPLICATION OF ARTICLE 41 OF THE CONVENTION

**83.**

Article 41 of the Convention provides:

‘If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party.’

**Damage**

84.
The applicant claimed 10,000 euros in respect of non-pecuniary damage.

85.
The Government submitted that the applicant could not claim any award in respect of non-pecuniary damage as his rights had not been violated.

86.
The Court considers that the finding of a violation constitutes sufficient just satisfaction for any non-pecuniary damage caused to the applicant (see Roman Zakharov, cited above, § 312).

**Costs and expenses**

87.
The applicant did not submit any claim in respect of costs and expenses.

**FOR THESE REASONS, THE COURT**

Holds, unanimously, that it has jurisdiction to deal with the applicant's complaints in so far as they relate to facts that took place before 16 September 2022;

Declares, unanimously, the complaint concerning the alleged violation of the right to respect for private life and correspondence admissible;

Holds, unanimously, that there has been a violation of Article 8 of the Convention;

Holds, by five votes to two, that there is no need to examine the complaint under Article 13 of the Convention;

Holds, by six votes to one, that the finding of a violation constitutes in itself sufficient just satisfaction for any non-pecuniary damage sustained by the applicant;

Dismisses, by six votes to one, the applicant's claim for just satisfaction.

Done in English, and notified in writing on 13 February 2024, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Olga Chernishova Pere Pastor Vilanova

Deputy Registrar President

In accordance with Article 45 § 2 of the Convention and Rule 74 § 2 of the Rules of Court, the separate opinion of Judge Serghides is annexed to this judgment.

P.P.V.

O.C.

**PARTLY DISSENTING OPINION OF JUDGE SERGHIDES**

**1.**

The applicant's complaint was that his right to respect for his private life and correspondence had been violated due to the statutory requirement for ‘Internet communication organisers’ (ICO) to store the content of all Internet communications and related communications data, and to submit those data to law-enforcement authorities or security services at their request, together with the information necessary to decrypt electronic messages, if they were encrypted.

**2.**

While I agree with points 1-3 of the operative provisions of the judgment, I respectfully disagree with points 4-6.

**3.**

In particular, I disagree with (a) paragraph 82 of the judgment and point 4 of its operative provisions to the effect that, having found a violation of Article 8 in the present case, there is no need to give a separate ruling on the admissibility and merits of the complaint under Article 13; (b) paragraph 86 of the judgment and point 5 of its operative provisions, which hold that the finding of a violation constitutes in itself sufficient just satisfaction for any non-pecuniary damage sustained by the applicant; and (c) point 6 of the operative provisions dismissing the applicant's claim for just satisfaction.

**4.**

As regards the Court's decision that there is no need to examine the Article 13 complaint, I would argue that since this complaint was raised by the applicant, the Court has a duty to examine it, failing which the applicant's right to an effective remedy would not be afforded any protection whatsoever by the Court. Like any other Convention right that has allegedly been infringed, the right under Article 13 must be examined and given practical and effective protection by the Court, as required by the principle of effectiveness and that of indivisibility of rights, and by the right of individual application, which is the cornerstone of the Convention. However, the Court cannot afford an applicant effective protection if it decides, as it has in the present case, not to deal with the relevant complaint.

**5.**

Turning now to the matter of non-pecuniary damage, the applicant claimed 10,000 euros (EUR) (see paragraph 84 of the judgment), while the Government submitted that he could not claim any award in respect of non-pecuniary damage as his rights had not been violated (see paragraph 85 of the judgment). However, the Court has found that there was a violation of Article 8 in the present case - a violation which, in my view, was severe. I also submit that the applicant sustained non-pecuniary damage in the present case and should therefore have been granted a monetary award in that regard under Article 41 of the Convention. I have had the opportunity in a number of separate opinions to criticise the Court's decision to reject claims for non-pecuniary damage under Article 41 merely by relying on a standard phrase, namely, ‘the finding of a violation constitutes in itself sufficient just satisfaction of any non-pecuniary damage sustained by the applicant’. It will suffice for me to refer to three such opinions criticising this standard manner of rejecting monetary claims in respect of non-pecuniary damage, thereby sparing me the need to reiterate the same arguments again here: see, therefore, paragraphs 3-16 of my partly dissenting opinion in Tingarov and Others v. Bulgaria, no.

42286/21, 10 October 2023; paragraphs 22-38 of my partly concurring, partly dissenting opinion in Yüksel Yalçınkaya v. Türkiye [GC], no. 15669/20, 26 September 2023; and paragraphs 4-10 of the joint partly dissenting opinion I authored with Judge Felici in Grzęda v. Poland [GC], no. 43572/18, 15 March 2022.

**Noot**

**Auteur:** O.L. van Daalen[1]

**Noot**

**1.**

Encryptietechnologie is een van de belangrijkste manieren om informatie te beveiligen. Je kan met encryptietechnologie de vertrouwelijkheid van informatie beschermen, zodat mensen zonder de juiste sleutel niet bij die informatie kunnen. En je kan met encryptiechnologie de integriteit van informatie waarborgen, zodat het kan worden gedetecteerd wanneer informatie is veranderd.

**2.**

Er zijn allerlei verschillende soorten encryptietechnologie. Een belangrijk onderscheid is tussen technologie waarbij de encryptiesleutel alleen in handen is van de gebruiker, en technologie waarbij ook anderen over die sleutel beschikken.

**3.**

Dat is een belangrijk onderscheid, want wie de sleutel heeft, kan bepalen wie toegang krijgt tot versleutelde informatie.

**4.**

Als de sleutel alleen in handen is van de gebruiker (en meestal zal zijn opgeslagen op het apparaat van de gebruiker), dan betekent het dat anderen niet bij de versleutelde informatie kunnen. Een ander, bijvoorbeeld de politie, is dan genoodzaakt toegang te krijgen tot het apparaat waarop de sleutel is opgeslagen, of zal de eigenaar van het apparaat moeten verplichten om de sleutel af te staan.

**5.**

Dat is anders als de sleutel bijvoorbeeld wordt beheerd door een cloudprovider - in dat geval kan de politie de sleutel onder omstandigheden opvragen bij die provider.

**6.**

In de afgelopen jaren zijn steeds meer chat-apps, zoals iMessage, WhatsApp en Signal, overgestapt op end-to-end-encryptie. Dat is encryptie waarbij de sleutel waarmee de communicatie is versleuteld alleen toegankelijk is voor de verzender en de ontvanger. Anderen die de communicatie onderscheppen, zoals

bijvoorbeeld de geheime dienst, kunnen de communicatie niet ontsleutelen, want ze hebben de sleutel niet.

**7.**

Het is dan ook niet verrassend dat in het debat over de regulering van encryptietechnologie juist dit soort end-to-end-encryptiediensten het meest onder vuur liggen. Het probleem is bij die technologie immers dat de wettelijke bevoegdheden van de geheime diensten en politie om onder omstandigheden toegang te krijgen tot communicatie, in de praktijk minder relevant worden. De informatie die daarmee kan worden verkregen is immers versleuteld.

**8.**

Je zou kunnen zeggen dat dat een specifiek voorbeeld is van een bredere maatschappelijke ontwikkeling die de Amerikaanse jurist Lawrence Lessig al in de jaren negentig van de vorige eeuw signaleerde. Die ontwikkeling noemde hij code as law: het idee dat de code, de technologie waarmee we ons omringen, steeds meer de rol overneemt van law, de regels die bepalen wat we wel en niet mogen en kunnen doen. In de context van end-to-end-encryptie: de code bepaalt dat alleen degene die beschikt over de sleutel toegang krijgt tot de informatie, terwijl de law in theorie de overheid meer bevoegdheden geeft om toegang te krijgen tot die informatie.

**9.**

De vraag is hoe je hiermee om moet gaan. In een ideaal scenario zou de technologie 1-op-1 de regels reflecteren; de encryptietechnologie moet dan zo worden ontwikkeld dat de overheid onder omstandigheden, zoals beschreven in de wet, toegang moet kunnen krijgen tot onversleutelde informatie. (Ik ga er daarbij gemakshalve even vanuit dat de wet voldoende waarborgen biedt om grondrechtelijke toetsing te doorstaan).

**10.**

Het probleem is alleen dat zo'n oplossing in de praktijk allerlei ongewenste neveneffecten heeft.

**11.**

Om te zorgen dat de overheid onder omstandigheden toegang kan krijgen, kan je twee dingen doen. Of je gaat de sleutel opslaan bij een derde partij (die de sleutel alleen onder omstandigheden verstrekt). Zo'n centrale opslagplaats van sleutels is natuurlijk een aantrekkelijk doelwit voor geheime diensten en hackers, en het is moeilijk om daartegen goed te beveiligen. Of je kan ervoor kiezen om het encryptie-algoritme te verzwakken, zodat de overheid hier onder omstandigheden bij kan. Maar ook daarvoor geldt dat je met zo'n maatregel niet alleen de deur openzet voor, bijvoorbeeld, de Nederlandse overheid - ook andere partijen zullen gebruikmaken van dat soort verzwakkingen.

**12.**

Hiermee samenhangend is er ook een praktisch probleem, want niet alleen de Nederlandse overheid zal toegang willen tot versleutelde informatie - ook andere regimes willen gebruik maken van de mogelijkheid om toegang te krijgen tot versleutelde informatie. Sommige van die regimes hebben heel andere regels, regels die mogelijk in strijd zijn met Europese grondrechten (denk aan Rusland, waar deze zaak over ging).

**13.**

De regulering van encryptie raakt dus minstens drie belangen. Ten eerste de belangen van de overheid, die onder omstandigheden toegang wil tot versleutelde informatie. Ten tweede de belangen van mensen wier communicatie de overheid wil analyseren; die mensen willen dat het proces voor het krijgen van toegang tot informatie met voldoende waarborgen is omkleed. En tot slot de belangen van alle andere mensen die gebruik maken van dezelfde encryptietechnologie. Zij willen dat onrechtmatige toegang tot versleutelde informatie door criminele organisaties wordt uitgesloten of in ieder geval beperkt.

**14.**

De vraag is hoe je de spanning tussen deze verschillende belangen moet wegen. En in de zaak Podchasov geeft het EHRM daarop een antwoord, aan de hand van artikel 8 EVRM (dat het recht op privacy beschermt).

**15.**

De zaak gaat over de chatdienst Telegram, die ook een end-to-end-encryptiemogelijkheid aanbiedt. De Russische geheime dienst, de FSB, verplichtte Telegram om de encryptiesleutels van de chats van bepaalde telefoonnummers te verstrekken. Telegram gaf aan dat dit in de praktijk neerkwam op een verplichting om de chatapp zo aan te passen dat een backdoor wordt geïnstalleerd - zij had immers geen toegang tot de sleutels van communicatie die met end-to-end encryptie was versleuteld.

**16.**

De eerste vraag is of een verplichting die er in de praktijk op neerkomt dat end-to-end-encryptie moet worden verzwakt, moet worden aangemerkt als een inmenging in het recht op privacy zoals beschermd in artikel 8 EVRM. Dat is niet zo vanzelfsprekend als het lijkt - het gaat hier immers over een overheidsmaatregel, het aanpassen van de encryptie, die het slechts mogelijk maakt dat de overheid nadien toegang krijgt tot die informatie. Het EHRM wijdt hier weinig woorden aan, behalve dat ze vaststelt dat zo’n verplichting alle gebruikers van de dienst, dus ook de klagers, zou raken (par. 75).

**17.**

Die overweging, dat zo’n verplichting alle gebruikers van de dienst zou raken, speelt wel een centrale rol in de volgende stap van de analyse, namelijk of de inmenging gerechtvaardigd is. Het EHRM benadrukt eerst dat encryptie een enorm belangrijke rol speelt in de bescherming van privacy, vertrouwelijke communicatie en andere grondrechten (par. 76). Het is ook een belangrijke manier om mensen te beschermen tegen hacken en andere vormen van onrechtmatige toegang. Het EHRM vervolgt dat een verzwakking van end-to-end-encryptie ondertussen alle gebruikers zou raken, inclusief veel niet-verdachten (par. 77). Overheden kunnen makkelijker in bulk communicatie onderscheppen (in strijd met grondrechten). En criminelen kunnen makkelijker de informatie exploiteren. En het EHRM merkt op dat er ook onderzoek wordt gedaan naar andere manieren om toch toegang te krijgen tot versleutelde informatie zonder de encryptie te verzwakken (par. 78).

**18.**

Het EHRM concludeert daarom dat een verplichting om end-to-end-encryptie te ontsleutelen in de praktijk neerkomt op een eis om de encryptie van alle gebruikers te verzwakken. Zo'n eis is volgens het EHRM dus niet proportioneel.

**19.**

Het belang van deze uitspraak voor informatiebeveiliging, privacy en vertrouwelijke communicatie kan moeilijk worden onderschat. Al zolang end-to-end-encryptie bestaat, wordt er door overheden opgeroepen om de technologie te verzwakken. Het security-argument, namelijk dat dit in de praktijk iedereen onveiliger maakt, was tot voor kort vooral een beleidsmatig argument. Nu staat vast dat het ook een grondrechtelijk argument is.

**20.**

Maar wat moeten we nu met het probleem dat de overheid niet meer de bevoegdheden kan uitoefenen die zij in de wet wel heeft gekregen? Daarvoor is het goed om preciezer te kijken naar de paragraaf waarin het EHRM opmerkt dat er ook onderzoek wordt gedaan naar alternatieven om toch toegang te krijgen tot versleutelde informatie. Want die alternatieven zijn ook niet zonder problemen.

**21.**

Eén alternatief waaraan nu bijvoorbeeld in Europa wordt gewerkt, is een aanpak waarbij het mogelijk wordt om app-providers te verplichten chats te laten analyseren op de telefoon, dus vóórdat encryptie wordt toegepast. Dat wordt afgeschilderd als een oplossing waarbij de encryptietechnologie intact blijft, maar toch communicatie kan worden geanalyseerd. Het is een aanpak die ook weer allerlei fundamenteelrechtelijke vragen oproept. Laten we hopen dat deze vragen worden geaddresseerd vóórdat de rechter eraan te pas hoeft te komen.

---

**Footnotes**

[1] O.L. van Daalen is advocaat en oprichter van Root Legal en onderzoeker bij het Instituut voor Informatierecht (IViR).