The European Court of Human Rights Concludes Encryption Backdoor Mandates Violate the Right to Private Life of All Users Online

9-11 minutes

On 13 February the European Court of Human Rights (ECtHR) issued a ground-breaking judgment in the case of ***Podchasov v Russia***. The case concerned the statutory requirements that Russia imposed on the online messaging platform Telegram to automatically store all communications data for one year and the contents of all communications for six months, and to submit those data to law-enforcement authorities or security services together with encryption keys and any other information necessary to decrypt communication data.

The ECtHR categorically confirmed that solutions that weaken encryption or create backdoors to facilitate access by law enforcement authorities to encrypted communication data in the context of criminal investigations violate the right to private life, under Article 8 European Convention on Human Rights (ECHR) of all users.

The Facts of the Case

The applicant is a user of Telegram Messenger, a messaging application that provides by default a custom-built server-client encryption scheme and the option to switch to end-to-end encryption by activating the "secret chat" feature. In 2017, Telegram became legally obligated under Russian law to retain communication data for all users for one year and store the contents of all communications for six months.

The Federal Security Service ("the FSB"), acting under Section 10.1 of Federal Law no. 149-FZ on Information, Information Technologies, and Protection of Information (referred to as "the Information Act"), mandated Telegram to disclose all technical information, including the encryption key, that would facilitate the decryption of communications for six users under investigation for terrorism-related activities. Although the disclosure order mentioned six judicial authorizations, Telegram was not provided with these details.

Telegram refused to comply with the disclosure order, emphasizing that due to the activation of end-to-end encryption by the users under investigation, disclosing the necessary information would be technically impossible without creating a backdoor that could compromise the encryption for all users. Consequently, the company faced fines, and Telegram was subsequently blocked in Russia.

The applicant contested the disclosure order even though he had not been directly targeted. The applicant argued that providing encryption keys to law enforcement as required by the law violated his right to privacy and the privacy of communications under Article 8 ECHR. This was based on the premise that executing the disclosure order would have granted the FSB technical access to the communications of all users without the required judicial authorization stipulated by Russian law.

Court Decision

The Court concluded that the law providing for the retention of 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. It specifically found that a law permitting law enforcement agencies to gain generalized access to the content of electronic communications without sufficient safeguards impairs the very essence of the right to respect for private life under Article 8 of the Convention.

The Court examined the legal obligation to provide law enforcement authorities with the essential information for decrypting communications of individuals suspected of engaging in serious criminal activities. The Court considered the expert testimonies from Privacy international and European Information Society Institute (EISI), as well as relevant insights from several international entities such as the United Nations High Commissioner for Human Rights, the Council of Europe, the European Data protection Board, the

European Data protection Supervisor, and the jurisprudence of the Court of Justice of the European Union (CJEU). It concluded that decrypting end-to-end encrypted communications of those under investigation would inevitably result in a compromised encryption system for all platform users. **The Court explicitly stated that introducing backdoors to weaken encryption could potentially enable routine, widespread, and indiscriminate surveillance of personal electronic communications.** It noted that such backdoors might be exploited by criminal networks, posing a severe threat to the security of electronic communications for all users. Therefore the Court found this risk disproportionate to the legitimate objective pursued by the law.

The Court underscored the need for alternative solutions to decryption that do not undermine protective mechanisms, both through legislative measures and continuous advancements in technology. In particular, the Court took the view that alternative, less intrusive methods of accessing communications are currently available to law enforcement, such as exploiting vulnerabilities in the target's software, as was suggested by EISI in its third-party intervention.

CSAM Proposal Post-*Podchasov*

The importance of this ECtHR judgment should not be underestimated. It is the first time the Court addresses the legality of mandating backdoor access to encrypted communications for law enforcement purposes. The Court takes quite a strong stance in favor of encryption by recognising not only measures that break encryption, but also any measures that weaken the effectiveness and intended purpose of encryption (i.e client-side scanning). CDT and many international partners have consistently emphasized that breaking and weakening encryption would inevitably make everybody more vulnerable online. This stance has been reiterated, most notably in the context of the ongoing negotiations in the EU regarding the CSAM proposal. With this judgment, the ECtHR confirms that, irrespective of how noble or legitimate the goal pursued might be, legislative proposals that advocate for solutions that weaken or break encryption impair the rights and freedoms of all users online and not only the rights of those suspected of committing a crime. This judgment debunks the fallacy that "content moderation solutions" to gain access to encrypted content, such as those under consideration in the European Commission's CSAM proposal, can be targeted and available only to the "good guys" for the prevention of crime.

CDT has pointed out before that client-side scanning serves as a backdoor to encryption. This solution, as proposed by the European Commission and defendended by many in the context of the negotiations at the EU institutions, involves the interception and analysis of user-generated content on the client's device before it is encrypted and transmitted. While proponents argue that client-side scanning is employed to detect and prevent the dissemination of CSAM, it fundamentally compromises the integrity of end-to-end encryption. By allowing access to unencrypted content on the user's device, even for a brief moment, client-side scanning creates vulnerabilities that could potentially be exploited by malicious actors or abused by intrusive surveillance practices, which undermines the very essence of encryption, eroding user trust in secure communication platforms and posing a threat to the overall privacy landscape.

Surviving the Test of the CJEU

This judgment is a warning for EU legislators currently working on the CSAM proposal. The CJEU has a strong record when it comes to upholding privacy rights, as exemplified by the *Schrems* rulings where the Court struck down the *safe harbour agreement* and the *privacy shield* for concerns over surveillance policies in the U.S. It has also struck down EU legislative instruments over violations of privacy rights due to excessive data retention standards. It is certain that the CJEU will take into account the jurisprudence of the ECtHR on this matter as well, leading only to one likely outcome: the invalidation of the CSAM regulation to the extent it mandates access to contents communications encrypted end-to-end through methodologies such as client side scanning.

While the European Parliament has introduced some significant safeguards and guarantees in its position on the CSAM file, the Council is yet to adopt its general approach. However, the latest version of the Council's general approach failed to resolve the concerns raised by the Council's own legal service. In its leaked opinion, the legal service found that the general obligation to scan communications, and the technical solutions proposed by the Commission to do so, are illegal under EU law. Should the Council continue to ignore the numerous warnings from international actors and civil society, CDT is convinced that the final text will not survive the test of the CJEU.

Related Reading