The Cost of Decryption

The ECHR's Warning Against Mass Surveillance in Podchasov v. Russia

Eirini Tsagkaraki
Postdoctoral Fellow of the Jean Monnet Center of Excellence AI-2-TRACE-CRIME, NUP
Special Scientist, School of Law, Neapolis University Pafos
Attorney at Law, LL.M., Ph.D. LMU Munich, Ph.D. University of Zurich

Georgios Pavlidis
UNESCO Chair & Jean Monnet Chair
Director of the Jean Monnet Center of Excellence AI-2-TRACE-CRIME, NUP
Associate Professor of International and EU Law School of Law, Neapolis University Pafos

This article examines the European Court of Human Rights judgment in Podchasov v. Russia (2024), a landmark decision addressing the compatibility of mandatory decryption laws with the right to privacy under Article 8 ECHR. For the first time, the Court directly engaged with the legal implications of end-to-end encryption, holding that state demands for service providers to decrypt encrypted messages constitute a disproportionate interference with private life and correspondence. Situating Podchasov within the Court's broader surveillance jurisprudence – from Roman Zakharov to Big Brother Watch and Ekimdzhiev – the paper explores how the ECtHR has progressively established structural limits on indiscriminate data access and reinforced the democratic value of encryption. The case illustrates not only the systemic deficiencies of Russian surveillance law, but also the growing recognition that encryption is a vital safeguard rather than an obstacle to justice in digital democracies. This study was prepared in the context of the Jean Monnet Center of Excellence AI-2-TRACE-CRIME and was funded by the European Union. Views and opinions expressed are however those of the author only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

1. Introduction

The judgment of the European Court of Human Rights (ECtHR) in Podchasov v. Russia (2024)[1] marks a significant development in the Court's evolving case law on digital privacy and surveillance. For the first time, the ECtHR directly addressed the compatibility of national legislation requiring service providers to decrypt end-to-end encrypted communications with the right to respect private life and correspondence under Article 8 of the European Convention on Human Rights (ECHR). In doing so, the ECtHR recognized that encryption technologies are not merely technical tools, but they also function as safeguards for individual rights in the digital age[2]. The significance of this judgment becomes even greater, considering that neither the Court of Justice of the European Union (CJEU) has addressed the relative issue to date with regard to Art. 7 of the Charter of Fundamental Rights of the European Union.

The case arose from Russian legislation obliging so-called "Internet Communication Organisers" (ICOs), including messaging platforms like Telegram, to store all user communications and related metadata and, more importantly, to provide law enforcement authorities with access to these data. The disclosure requirement included the keys required for decryption, in the case of encrypted communications. The applicant, a Telegram user, argued that these measures amounted to mass surveillance and exposed all users to indiscriminate access. Moreover, the applicant pointed out that end-to-end encryption prevents any third party, including the service provider, from accessing content

1. Podchasov v. Russia, App no. 33696/19 (ECtHR, 13 February 2024).
2. End-to-end encryption (E2EE) is a secure communication system that prevents third parties (including service providers) from accessing data transferred from sender to recipient. For more information on how this enhanced security messaging system works s. https://www.cloudflare.com/learning/privacy/what-is-end-to-end-encryption/ (last accessed on 09.07.2025).

without fundamentally compromising the security of the system.

The ECtHR unanimously found a violation of Article 8 ECHR. It emphasised that the contested Russian framework permitted generalised access to communications content without adequate safeguards against arbitrariness and abuse. Regarding decryption, the ECtHR held that requiring service providers to decrypt end-to-end encrypted messages led to an interference with all users' right to private life and correspondence indiscriminately, because the measures in question could not be limited to specific individuals, and therefore amounted to an interference that was neither necessary in a democratic society nor proportionate to the aims pursued. This reflects the idea that the integrity of encryption cannot be sacrificed in the name of security without undermining the essence of the right to privacy.

Podchasov must be situated within a broader line of ECtHR jurisprudence, beginning with Roman Zakharov v. Russia (2015) with regard to secret surveillance of communication[3], extending through Big Brother Watch and Others v. United Kingdom (2021)[4] with regard to a generalised storage and surveillance of users communication, and continuing with Ekimdzhiev and Others v. Bulgaria (2022)[5] with regard to the access of law enforcement authorities to stored communication data. Across these cases, the ECtHR has progressively clarified the limits of permissible surveillance under the ECHR. A common principle has emerged in this context: indiscriminate or unchecked retention and access to personal data, especially in digital contexts, imperils the right to private life. Podchasov confirms this principle and explicitly recognises the increased democratic necessity of strong encryption for the purpose of enhancing the protection of privacy and communication to a greater extent and the importance of decryption for the purpose of preventing and suppressing serious crime in a lesser extent.

2. Factual and Legal Background

At the heart of Podchasov v. Russia lies a contested legal framework obliging digital service providers to act as agents and instruments of state surveillance.[6] Under amendments to the Federal Law no. 149-FZ on Information, Information Technologies and Protection of Information (the "Information Act"), introduced in 2016, the so-called "Internet Communication Organisers" (ICOs) were subject to an expansive set of three obligations: i) the requirement to store the content of all user communications for six months and related metadata for one year, ii) the obligation of ICOs to provide law enforcement or security agencies with access to the stored data upon request and, iii) more importantly, the obligation, where communications were encrypted, to submit the information necessary to decrypt them. Effectively, this was rendering strong encryption incompatible with regulatory compliance.

Telegram Messenger,[7] one of the most popular messaging applications in Russia, had been classified as an ICO by Russian authorities in 2017. Telegram refused to comply with a decryption order issued by the Federal Security Service (FSB). The order demanded information and encryption keys, to allow decryption of communications from users allegedly involved in terrorism-related activities. Telegram responded that compliance was technically impossible, because users involved had activated the 'secret chat' function, which deployed end-to-end encryption[8]. This meant that only the communicating parties, not even Telegram itself, had access to the content. The consequence of providing a decryption key would have been the creation of a system-wide backdoor, undermining the privacy of all Telegram users.[9][10]

3. Roman Zakharov v. Russia, App no. 47143/06 (Paragraphs 15-138, ECtHR, 4 December 2015),
4. Big Brother Watch and Others v. United Kingdom, App. Nos. 58170/13, 62322/14, 24960/15 (ECtHR, 25 May 25 2021)
5. Ekimdzhiev and Others v. Bulgaria, App no. 70078/12 (ECtHR 11 January 2022, final on 11 April 2022).
6. Watt, E., State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law (Edward Elgar Publishing, 2021)
7. Telegram is 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.
8. Telegram did not have end-to-end (client-client) encryption by default. Instead, it used a custom-built server-client encryption scheme in its default "cloud chats". It was, however, possible to switch to end-to-end encryption by activating the 'secret chat' feature. The Court addressed the issue of compatibility with the right to private life and communication only with regard to the case of the users having switched to E2EE by activating the "secret chat" feature (s. Podchasov v. Russia, App no. 33696/19, Paragraph 56, ECtHR, 13 February 2024).
9. Alì, A., "Encryption backdoors on trial: the telegram case before the European Court of Human Rights" (2024) Comunità internazionale: rivista trimestrale della Società Italiana per l'Organizzazione Internazionale: LXXIX, no 3, pp. 525-539.
10. It shall be noted that the Telegram-FSB encryption dispute was not the first one to questioning the balance between security in terms of fighting crime and privacy in terms of protection of private life and correspondence. Quite similar to the Telegram-FSB encryption dispute was the Apple-FBI encryption dispute of 2016. In this case The Federal Bureau of Investigation (FBI) wanted Apple to create new software to enable the FBI to unlock a mobile phone owned by a person who took part in a terrorist attack in California in 2015. Apple declined FBI's request due to its policy to never undermine the security features of its products, clarifying that complying with such a request would jeopardize its clients' right to privacy and communication. FBI successfully applied for a court order, which Apple opposed. However, in the end FBI announced that it unlocked the iPhone and withdrew its request against Apple, but the controversy on "encryption backdoors" had already started (for more

The Russian judiciary backed the demands of the FSB at every stage. Telegram was fined, and access to its service was ordered to be blocked in 2018. The applicant in Podchasov, a regular Telegram user, joined a group complaint against the FSB's order. The key argument was that indiscriminate decryption obligations would render the private use of encrypted messaging tools effectively meaningless and would therefore lead to a breach of their right to respect for their private life and for the privacy of their communications.[11] For their part, the domestic courts dismissed the action as inadmissible, on the basis that the applicant's rights were not affected.

The statutory regime can be viewed in light of the Court's earlier findings in Roman Zakharov v. Russia (2015)[12]. In that context, the Grand Chamber found that Russia's secret surveillance framework – especially as it applied to mobile communications – violated Article 8 ECHR due to its lack of clear, foreseeable rules, and absence of meaningful oversight. The surveillance framework failed to ensure targeted, necessary surveillance rather than generalised interception. In Podchasov, these defects persisted and were arguably deepened by their extension to the digital sphere. Therefore, there appears to be a continued pattern of systemic flaws, now encompassing metadata retention and access to encrypted data by authorities without prior judicial oversight or sufficient safeguards against abuse.

The Russian surveillance architecture allowed the state to collect data, as well as to compel technical service providers to neutralise the very technologies, like encryption, that exist to secure private communications in the first place. The absence of targeted authorisations, independent oversight, or enforceable user remedies calls into question the legitimacy of this surveillance architecture system, which effectively places every internet user under suspicion.

International bodies intervened in the proceedings as third parties in favor of the applicants, arguing against the necessity and proportionality of requiring backdoor access to all encrypted messages. According to the European Information Society Institute (EISI) the decryption obligation compromised the privacy of all users for the sake of a small number of suspects, as it made all users vulnerable to unauthorised State surveillance, cybercriminal activities and other malicious actors. EISI also argued that less intrusive targeted alternatives to combat crime and protect national security existed, such as using live forensics on seized devices, guessing or obtaining private keys held by parties to the communication or using vulnerabilities in the target's software or sending an implant to targeted devices[13]. Similarly, Privacy International highlighted that the only way for Telegram to comply with the decryption obligation 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.

3. The Court's Reasoning under Article 8 ECHR

In its judgment, the ECtHR identified a threefold interference with the applicant's rights under Article 8 ECHR and considered the applicant's challenge against its surveillance jurisprudence, drawing clear parallels with previous case-law. In each of these judgments, the Court held that indiscriminate, untargeted surveillance measures – especially when accompanied by insufficient legal safeguards – are incompatible with Article 8. In Roman Zakharov v. Russia (2015)[14], the Court had already condemned the Russian regime of secret surveillance, identifying structural deficiencies such as the secret nature of surveillance measures and the broad scope of their application, the lack of meaningful judicial oversight and direct access by security services to telecommunications networks. Podchasov confirmed these concerns and extended them to the digital sphere[15]. In Big Brother Watch (2021),[16] the ECtHR warned that bulk interception must be 'subject to end-to-end safeguards' to avoid arbitrary interference. Likewise, in Ekimdzhiev and Others v. Bulgaria (2022)[17], the ECtHR declared that even the mere existence of a legal regime enabling generalised access to communications data constitutes a violation of Article 8, when lacking the necessary procedural guarantees. Following the same logic, Podchasov affirmed that a legal framework that empowers the state to access encrypted communications without the possibility of limiting the interference to specific targets strikes at the very heart of the right to privacy.

The Court justified its assessment on the threefold intervention with Article 8 of the Convention as follows:

First, the Court found that the systematic retention of the content of internet communications and associated metadata – which was carried out by private actors but under a legal

information on the Apple-FBI encryption dispute s. https://epic.org/documents/apple-v-fbi-2/ , last accessed on 09.07.2025).

11. On this issue, see Stahl, T., "Indiscriminate mass surveillance and the public sphere" (2016) Ethics and Information Technology, Vol. 18.1, pp. 33-39.
12. Roman Zakharov v. Russia, App no. 47143/06 (ECtHR, 4 December 2015)
13. Podchasov v. Russia, App no. 33696/19 (Paragraph 47, ECtHR, 13 February 2024).
14. Roman Zakharov v. Russia, App no. 47143/06 (ECtHR, 4 December 2015)
15. Podchasov v. Russia, App no. 33696/19 (Paragraph 55, ECtHR, 13 February 2024).
16. Big Brother Watch and Others v. United Kingdom, App. Nos. 58170/13, 62322/14, 24960/15 (ECtHR, 25 May 25 2021)
17. Ekimdzhiev and Others v. Bulgaria, App no. 70078/12 (ECtHR 11 January 2022, final on 11 April 2022).

obligation – constituted an interference with the right to respect for private life and correspondence attributable to the Russian State, irrespective of whether the retained data were then accessed by the authorities[18]. The Court expressed its surprise by the extremely broad duty of retention provided by the contested legislation and concluded that the interference was exceptionally wide-ranging and serious[19].

Second, the Court noted the law enforcement authorities' potential access to this stored data. Under Russian law, this could be executed without the service provider being shown any prior judicial authorization and could also be direct and remote to all internet communications and related communications data[20]. The ECtHR concluded that the domestic law on law enforcement authorities' access to stored data does not – under these circumstances – provide for adequate and sufficient safeguards against arbitrariness and abuse.

Third, and most significantly, the Court highlighted the statutory requirement to decrypt encrypted communications, specifically end-to-end encrypted messages, as a disproportionate obligation that extended the interference to the very architecture of secure digital communication.[21] More specifically, the Court emphasized that encryption 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. Weakening encryption by creating backdoors would apparently make it technically possible to perform routine, general and indiscriminate surveillance of personal electronic communications. Thus, backdoors could also be exploited by criminal networks and would seriously compromise the security of all users' electronic communications. Taking into consideration the possible dangers of restricting encryptions, as described by experts of the field, the ECtHR highlighted the alternative "solutions to decryption without weakening the protective mechanisms, both in legislation and through continuous technical evolution".

Based on all the above, the ECtHR crucially found that in Podchasov Case the interference with the right to respect for private life and correspondence did not meet the requirements of "quality of law" and "necessity in a democratic society" and that the combination of interferences, i.e. retention, access, and decryption, amounted to a breach of the 'essence' of Article 8.[22] This concept, first developed in S. and Marper v. United Kingdom (2008)[23] and reaffirmed in Breyer v. Germany (2020)[24], emphasises that some infringements are so invasive, and so lacking in safeguards, that they are incapable of justification under proportionality assessment. In Podchasov, the Court concluded that the Russian regime 'impairs the very essence' of the right to private life and correspondence because it allows for generalised access to the content of electronic communications and requires weakening encryption technologies that are essential for the exercise of that right.

4. Encryption, Democratic Necessity and Surveillance Jurisprudence

In Podchasov v. Russia, the ECtHR affirmed that end-to-end encryption is not a legal obstacle to be overcome by the state, but rather a core democratic safeguard essential to the exercise of rights protected by the ECHR. The ECtHR recognised that encryption enables individuals to communicate securely in an era of pervasive digital surveillance, shielding not only private correspondence but also political expression, journalistic activity, and professional confidentiality. Compelling service providers to undermine such encryption by creating decryption backdoors, the Court held, would systematically expose users to state and non-state intrusions, thereby violating the essence of the right to respect for private life under Article 8 ECHR. This approach aligns with international legal and policy guidance.

Indeed, the judgment draws on the recommendations of the Office of the United Nations High Commissioner for Human Rights, which emphasise that encryption is vital for safeguarding the rights to privacy, expression, association, and non-discrimination, particularly for vulnerable groups, journalists, and human rights defenders[25]. More importantly,

18. Podchasov v. Russia, App no. 33696/19 (Paragraph 52, ECtHR, 13 February 2024). The Court, however, did not proceed with a separate assessment of the legality of bulk data retention, which was instead examined in conjunction with the other issues raised in the case; see Tuchtfeld, E., "No Backdoor for Mass Surveillance: The European Court of Human Rights Protects the Right to Encrypted Communication" Verfassungsblog (29 February 2024).
19. Podchasov v. Russia, App no. 33696/19 (Paragraph 70, ECtHR, 13 February 2024).
20. Podchasov v. Russia, App no. 33696/19 (Paragraph 72, ECtHR, 13 February 2024).
21. Shurson, J., "A European right to end-to-end encryption?" (2024) Computer Law & Security Review 55: 106063. S. also Podchasov v. Russia, App no. 33696/19 (Paragraph 76-79, ECtHR, 13 February 2024).
22. Chiara, P., "Statutory Requirements for Communications Service Providers to Decrypt Online Communications Impair the Essence of Article 8 ECHR" (2024) European Data Protection Law Review, Vol. 10.3, pp. 312-317.
23. S. and Marper v. United Kingdom [GC] App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008).
24. Breyer v. Germany App no 50001/12 (ECtHR, 30 January 2020)
25. See Podchasov v. Russia, App no. 33696/19, §§ 28, ECtHR, 13 February 2024, with reference to OHCHR, The right to privacy in the digital age, thematic report, A/HRC/51/17, 4 August 2022, Paragraphs 20-28, https://docs.un.org/en/A/HRC/51/17 (last accessed on 09.07.2025); See also OHCHR Special Rapporteur on the promotion and protection of the right to freedom of

however, this report highlights the fact that encryption may indeed in some cases be an obstacle to combating crime, but in other cases it may enable secure communication with victims of crime such as women, who face particular threats of surveillance, harassment and violence online[26].

To this respect, the ECtHR also refers to the Joint Statement issued on 20th May 2016 by Europol and the European Union Agency for Cybersecurity (ENISA) "on lawful criminal investigation that respects 21st Century data protection". Even the EU organizations have warned that weakening encryption would give investigators lawful access in the event of serious crimes or terrorist threats, and that it would also increase the attack surface for malicious abuse, which, consequently, would have much wider implications for society"[27].

The risks of conflating encryption with criminality are particularly salient in light of the Grand Chamber's ruling in Yüksel Yalçınkaya v. Türkiye (2023)[28], where the Court criticised the Turkish authorities for relying solely on the use of an encrypted messaging application (ByLock) as conclusive evidence of terrorist affiliation. While the factual context in Yalçınkaya differs from Podchasov, both cases illuminate a dangerous trend: the presumption of States that encrypted communication by citizens equates to criminal conduct. In Podchasov, the Court took a decisive stance against this logic, affirming that the use of secure technology is not, in itself, grounds for suspicion. Therefore, weakening encryption across an entire platform cannot be justified by reference to isolated criminal investigations.

The Court's judgment in Centrum för Rättvisa v. Sweden (2021)[29] upheld a regime of bulk interception only under strict legal safeguards and independent oversight mechanisms. In Podchasov, by contrast, the Russian system imposed blanket retention and decryption duties without any meaningful limitation, authorisation procedure, or external supervision. The absence of such safeguards rendered the measures disproportionate and incompatible with democratic necessity.

Importantly, the Court stressed that even when the goal is legitimate – such as combating terrorism or serious crime – the means employed must remain within the bounds of the rule of law and Convention values.

In Roman Zakharov v. Russia (2015),[30] the Grand Chamber addressed the covert interception of mobile telephone communications under Russian law, finding that the system lacked adequate safeguards and enabled security services to intercept communications without meaningful oversight. The case introduced the concept of a structural violation of Article 8 ECHR, even in the absence of proof that a specific applicant's communications had been intercepted, due to the generalised and unaccountable nature of the legal regime. This logic was extended in Big Brother Watch and Others v. United Kingdom (2021),[31] where the ECtHR reviewed UK legislation on bulk interception of internet traffic. While acknowledging that bulk regimes might, in principle, be compatible with the ECHR, the ECtHR insisted that they must be tightly framed, subject to safeguards, and operate with clear necessity and proportionality constraints.

Ekimdzhiev and Others v. Bulgaria (2022)[32] further expanded the Court's scrutiny to domestic regimes mandating the retention of communications metadata and permitting indirect access by national authorities. The Court stressed that even data stored by private providers can constitute an interference under Article 8 ECHR when access is possible without adequate procedural guarantees. The storage should not be seen as entirely separate from the question on the access of law enforcement authorities to the stored data. In that judgment, as in Podchasov, the Court found that legislation allowing unfettered access to stored data by security services, particularly without notification, judicial control, or access logs, failed to comply with the 'quality-of-the-law' requirement.

Podchasov advances this jurisprudence by engaging directly with the technical architecture of surveillance.[33] Where earlier cases focused on interception or metadata access, Podchasov addresses the core question of whether States may legitimately require service providers to undermine encryption technologies. These technologies are, by their very nature, designed to prevent even the service provider from accessing user content. The Court's recognition that such

opinion and expression, Report on encryption, anonymity, and the human rights framework, A/HRC/29/32, 22 May 2015; see also 2018 Follow-up Report: "Encryption and Anonymity Follow-up Report" (A/HRC/38/35/Add.5), 13 July 2018.

26. OHCHR, The right to privacy in the digital age, thematic report, A/HRC/51/17, 4 August 2022, Paragraph 21, https://docs.un.org/en/A/HRC/51/17 (last accessed on 09.07.2025).
27. Joint Statement issued on 20th May 2016 by Europol and the European Union Agency for Cybersecurity (ENISA) "on lawful criminal investigation that respects 21st Century data protection", Considerations on decryption, S. https://www.europol.europa.eu/cms/sites/default/files/documents/on_lawful_criminal_investigation_respecting_21st_century...%20%281%29.pdf (last accessed on 09.07.2025).
28. Yüksel Yalçınkaya v. Türkiye [GC] App no 15669/20 (ECtHR, 26 September 2023).
29. Centrum för Rättvisa v. Sweden [GC] App no 35252/08 (ECtHR, 25 May 2021).
30. Roman Zakharov v. Russia, App no. 47143/06 (ECtHR, 4 December 2015).
31. Big Brother Watch and Others v. United Kingdom, App. Nos. 58170/13, 62322/14, 24960/15 (ECtHR, 25 May 25 2021).
32. Ekimdzhiev and Others v. Bulgaria, App no. 70078/12 (ECtHR 11 January 2022, final on 11 April 2022).
33. Chiara, P., "Una svolta nel dibattito sulla crittografia: la sentenza Podchasov c. Russia della Corte EDU. Verso alcuni diritti di cybersicurezza?" (2025) Diritto & Questioni Pubbliche, Vol. 24.1, pp. 1-18.

requirements 'impair the very essence' of Article 8 marks a turning point. It confirms that surveillance infrastructure must respect, not dismantle, the technological guarantees that protect private life in the digital sphere.

A finale distinction must be made here. In K.U. v. Finland (2008)[34], the Court recognised a positive obligation on states to ensure that individuals could be identified and held accountable when using the internet to harm others – for example, by requiring service providers to disclose user information in cases of child endangerment. That judgment acknowledged the legitimate interests in protecting individuals from harm in online environments. However, Podchasov demonstrates that positive obligations cannot be used to justify indiscriminate or structurally flawed surveillance regimes. The imperative to protect must be balanced against the risks of overreach, particularly where measures compromise the rights of the entire user base and not just identified suspects.[35]

5. Concluding Reflections and Broader Implications for State Practice

The judgment in Podchasov v. Russia serves not only as a rebuke of Russia's disproportionate surveillance practices[36], but also as a clarion call to all states that seek to legislate in ways that compel the circumvention of encryption or mandate indiscriminate data retention. In a digital environment increasingly dependent on encrypted communications for personal, political, journalistic, and commercial integrity, the Court's decision sends an unambiguous message: generalised access to encrypted data, particularly where it implies weakening the encryption infrastructure itself, violates the essence of Article 8 ECHR.

Naturally it cannot be overlooked that the Court's assessment of decryption as disproportionate to the interference with the right to privacy is based on the fact that targeted decryption is currently technically impossible. This means that if future technical developments allow for targeted decryption of data avoiding the indiscriminate interference with all users' protection of private life and correspondence, then this targeted interference with the right to private life and correspondence might obviously be considered as proportionate to the aims pursued.

But for now, it is unanimously acknowledged that Podchasov arrives at a time when multiple legislative proposals – including within the European Union – are attempting to recalibrate the relationship between security and privacy in the online space. A prominent example is the proposed EU Regulation on preventing and combating child sexual abuse material (CSA Regulation). Although the Proposal does not establish a systematic interception obligation for providers, it can authorise detection orders requiring platforms to scan encrypted communications, potentially introducing client-side scanning mechanisms that intercept messages before they are encrypted. The EDPB and EDPS, in their Joint Opinion 4/2022, have warned that such measures would 'entail the risk that providers offer less encrypted services" and ultimately "weaken the role of encryption in general and undermine the respect for the fundamental rights of European citizens', as "the structural incompatibility of some detection order with E2EE becomes in effect a strong disincentive to use E2EE"[37].

The Podchasov judgment reinforces these concerns. It affirms that technological design features such as end-to-end encryption are not simply policy choices, but safeguards under the ECHR. Requiring providers to introduce decryption capabilities or retain content data not only undermines the confidentiality of communications for targeted individuals, but also erodes trust in digital infrastructure. More broadly, the judgment offers a doctrinal recalibration of what 'proportionate surveillance' must mean in digital democracies. While earlier ECtHR case law allowed for certain forms of interception and metadata retention under safeguards, Podchasov marks a shift: despite the certain challenges to criminal investigations arising from encryption technologies, it draws a structural red line at legal obligations that require the weakening of encryption across an entire user base. The cost of access to private communications cannot be the permanent vulnerability of all communications.

This is not to suggest that security interests are illegitimate, nor that surveillance powers are inherently incompatible with the ECHR. But the judgment demands that such powers respect technological limits, legal safeguards, and democratic values.[38] As legislatures and regulators across Europe

34. K.U. v. Finland App no 2872/02 (ECtHR, 2 December 2008).
35. On this issue – specifically, the doubts surrounding the usefulness of adopting a 'balancing' model to guide either macro-level policy development or micro-level decision-making concerning individual warrants – see Bronitt, S. and James, S., "Regulating Telecommunications Interception and Access in the Twenty-first Century: Technological Evolution or Legal Revolution?" (2006) Prometheus: Critical Studies in Innovation, Vol. 24(4), pp. 413–428.
36. The Court decided that it had jurisdiction to examine the relevant application, 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.
37. Joint Opinion 4/2022 issued by European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS) on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, issued on 28th July 2022, https://www.edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202204_csam_en_0.pdf (last accessed on 09.07.2025).
38. See also Pavlidis, G., "Asset recovery in the European Union: implementing a "no safe haven" strategy for illicit proceeds"

consider the future of encryption, this judgment provides a principled benchmark for policymaking that is compatible not only with Article 8 ECHR but also with Article 7 of the Charter of Fundamental Rights of the EU.

References

- Alì, A., "Encryption backdoors on trial: the telegram case before the European Court of Human Rights" (2024) Comunità internazionale: rivista trimestrale della Società Italiana per l'Organizzazione Internazionale: LXXIX, no 3, pp. 525-539.
- Bronitt, S. and James S., "Regulating Telecommunications Interception and Access in the Twenty-first Century: Technological Evolution or Legal Revolution?" (2006) Prometheus: Critical Studies in Innovation, Vol. 24(4), pp. 413–428.
- Chiara, P., "Statutory Requirements for Communications Service Providers to Decrypt Online Communications Impair the Essence of Article 8 ECHR" (2024) European Data Protection Law Review, Vol. 10.3, pp. 312-317.

(2022) Journal of Money Laundering Control, Vol. 25.1, pp. 109-117.

- Chiara, P., "Una svolta nel dibattito sulla crittografia: la sentenza Podchasov c. Russia della Corte EDU. Verso alcuni diritti di cybersicurezza?" (2025) Diritto & Questioni Pubbliche, Vol. 24.1, pp. 1-18.
- Pavlidis, G., "Asset recovery in the European Union: implementing a "no safe haven" strategy for illicit proceeds" (2022) Journal of Money Laundering Control, Vol. 25.1, pp. 109-117.
- Shurson, J., "A European right to end-to-end encryption?" (2024) Computer Law & Security Review 55: 106063.
- Stahl, T., "Indiscriminate mass surveillance and the public sphere" (2016) Ethics and Information Technology, Vol. 18.1, pp. 33-39.
- Tuchtfeld, E., "No Backdoor for Mass Surveillance: The European Court of Human Rights Protects the Right to Encrypted Communication" Verfassungsblog (29 February 2024).
- Van Daalen, O.L., "The right to encryption: Privacy as preventing unlawful access", (2023) Computer Law and Security Review 49: 105804.
- Watt, E., *State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law* (Edward Elgar Publishing, 2021)