IN THE EUROPEAN COURT OF HUMAN RIGHTS

Krzysztof Brejza v. Poland and 8 Other Applications

(Application nos. 27830/23, 26531/23, 27632/23, 27840/23, 27942/23, 27998/23, 35514/23, 35791/23, 36474/23)

Written Third Party Submissions

on behalf of

AMNESTY INTERNATIONAL

Pursuant to the notification dated 4 February 2025 that the President of the Section had granted permission under Rule 44 § 3 of the Rules of the European Court of Human Rights

---

26 FEBRUARY 2025

INTRODUCTION

1. Amnesty International makes this submission pursuant to the leave to intervene as a third party in the European Court of Human Rights' (hereinafter, this Court's) proceedings granted by the President of the Section under Rule 44 § 3 of the Rules of Court. With this brief, Amnesty International hopes to assist the Court by offering an analysis of relevant international human rights law, standards and obligations in the context of surveillance and the use of technology for this purpose, such as spyware like Pegasus.

2. Amnesty International has been investigating unlawful surveillance for many years and has documented mounting evidence of human rights abuses being committed by governments, as well as how companies cause, contribute to, or have their operations, products or services directly linked to such abuses resulting from unlawful digital surveillance. Amnesty International's Security Lab provides technical support to the Pegasus Project[1], an international investigative effort led by a consortium of more than 80 journalists from 17 media organizations in 10 countries, coordinated by the NGO Forbidden Stories.[2]

3. Amnesty International has shared its methodology[3] and published an open-source mobile forensics tool[4] and detailed technical indicators to assist information security researchers and civil society with detecting and responding to serious surveillance threats. Amnesty International's internal Security Lab has over the years performed in-depth forensic analysis of numerous mobile devices from human rights defenders and journalists around the world. This research has uncovered widespread, persistent and ongoing unlawful surveillance and human rights abuses perpetrated using spyware, including NSO Group's Pegasus spyware, across different locations.[5]

4. In its work, Amnesty International has submitted based on its findings that digital surveillance threatens several human rights including the right to private and family life, and access to effective remedy. Amnesty International believes that this current case raises important questions that are of significance in Poland, for similarly placed Council of Europe member states, and for domestic and regional legal systems around the world grappling with the intersection of human rights and digital surveillance through spyware, given this Court's global impact in developing human rights jurisprudence.

5. Our evidence-based research provides tangible insight into how the Court's conclusions regarding the human rights impacts of surveillance are experienced by human rights defenders globally. Based on this research, Amnesty International submits that, to comply with international and regional human rights law and standards, states should adopt a ban on highly invasive spyware such as Pegasus, because, as will be explained, its technical features render it incompatible with international human rights law and standards. We also posit that states must impose a moratorium on the use, sale, export or transfer of all spywares until a system of human rights safeguards is in place capable of preventing abuse, which is presently absent.

6. To present our evidence-based conclusions for the consideration of this Court, this submission is divided in three parts: Part A focuses on how spyware works generally, how it has been used in Poland, and briefly, how it has been deployed in Europe and globally. Part B discuss state obligations in relation to the right to privacy and the right to effective remedy in the context of surveillance and spyware use within the framework of this Court's jurisprudence and international standards. Building on this review, Part C offers our analysis on the incompatibility of the use of highly invasive spyware with states' international human rights law obligations.

---

[1] The Pegasus Project had significant impact that continues to reverberate around the world. For example, following the work of the Pegasus Project, the U.S. Department of Commerce announced NSO Group was being placed on a blocklist due to its "malicious cyber activity," a few weeks later, Apple launched a legal action against NSO Group to "curb the abuse of state sponsored spyware", and the European Parliament voted to create a new "committee of inquiry" to investigate abuses of Pegasus by European member states.

[2] A Paris-based media non-profit organisation with the aim to ensure access to information of public interest while deterring crimes and violence against journalists. See forbiddenstories.org/about-us/mission/our-mission.

[3] Amnesty International, Report, "Forensic Methodology Report: How to catch NSO Group's Pegasus", 18 July 2021, amnesty.org/en/documents/doc10/4487/2021/en/.

[4] The 'Mobile Verification Toolkit', a forensic research tool intended for technologists and investigators. It has been developed and released by the Amnesty International Security Lab in July 2021. It continues to be maintained by Amnesty International and other contributors. docs.mvt.re/en/latest/.

[5] Amnesty International's research on the topic of unlawful surveillance is collated here: securitylab.amnesty.org/.

A. THE OPERATION OF SPYWARE IN POLAND AND BEYOND

7. Spyware is a form of malicious software or "malware" that acts to interfere with the normal operation of a device such as a computer or smartphone, often to provide remote access and disclose information to unauthorized entrants. This kind of malware is typically covert and designed to avoid detection and analysis. Unlike conventional wiretapping and communications surveillance, which only allow real-time monitoring of specific communications, more advanced techniques, like spyware, provide access to the full range of one's data – even retrieving historic and deleted communications, messages and files on the person's device. The infected device's camera and microphone can also be subverted to spy on the owner or their surroundings.[6]

8. Pegasus, a spyware developed by the Israeli firm NSO Group, is a type of highly invasive spyware, which allows unlimited access to a device by default, and which cannot be limited in its functionality to only those functions that are necessary and proportionate to a specific use and target. Once a device is infected with highly invasive spyware, the operator has total remote access to the device and can track its location; access conversations - even on end-to-end encrypted apps; access emails; access contacts, and activate the microphone to listen to nearby conversations.[7] Since the purpose of spyware is to enable covert surveillance, a key characteristic is that it is hidden from detection. Given that spyware software is built to deliberately evade detection, its use is also not capable of being independently audited. In lay terms, this means that the operation of the spyware cannot be effectively overseen by someone other than the user-operator[8] or potentially the provider of the service. [9] Public reporting on spyware abuses has only been possible due to independent digital forensics research that has managed to find traces of its use, in spite of the efforts of spyware manufacturers to ensure their products evade detection.

9. Digital surveillance through spyware, particularly Pegasus, has sparked significant concern over human rights abuses. In 2021, the Pegasus Project revealed that Pegasus had been deployed against journalists, activists, politicians, and other civil society members in at least 20 countries, including Poland.[10] The scope of the unlawful targeting with NSO Group's surveillance technology revealed in the Pegasus Project span the world.[11]

10. Other providers of spyware also active globally include Intellexa, who sell 'Predator', another form of highly invasive spyware. The Predator Files report, published by Amnesty International in 2023 as part of an investigation with the European Investigative Collaborations (EIC), revealed the use of Predator to target activists, journalists, academics and political figures world-wide.[12] Predator spyware was also linked to the hacking of journalists, opposition, and numerous public figures in Greece, triggering what has become known as #PredatorGate.[13] According to the Greens/EFA Group in the European Parliament, more than 70 countries are implicated in the global trade of spyware - as exporters, clients or both.[14]

---

[6] See amnesty.org/en/documents/asa39/7955/2024/en/ for this and more definitions under "Glossary".
[7] Amnesty International, Explainer, "What is spyware and what can you do to stay protected?", 14 December 2023, securitylab.amnesty.org/latest/2023/12/what-is-spyware-and-what-can-you-do-to-stay-protected/.
[8] 'User-operator' refers to the individual or entity that controls or operates the spyware software on the target device.
[9] It is important to note that spyware can infect a device when a target clicks on a malicious link or even without them doing anything. The infection methods include "1-click" attack, by which the device is infected when the target clicks on a compromised link. Compromised links can be sent many different ways including via text, email or on social media platforms. The infection can also occur through a "zero-click" attack: the device is infected without the user interacting with, or doing, anything. See: securitylab.amnesty.org/glossary/.
[10] Amnesty International, "Poland: Use of Pegasus Spyware to hack politicians highlights threat to civil society", 7 January 2022, amnesty.org/en/latest/news/2022/01/poland-use-of-pegasus-spyware-to-hack-politicians-highlights-threat-to-civil-society/. See also: The Guardian, "More Polish opposition figures found to have been targeted by Pegasus spyware", 17 February 2022, theguardian.com/world/2022/feb/17/more-polish-opposition-figures-found-to-have-been-targeted-by-pegasus-spyware.
[11] Amnesty International, Report, "Uncovering the Iceberg: The Digital Surveillance Crisis Wrought by States and the Private Sector", 23 July 2021, amnesty.org/en/documents/doc10/4491/2021/en/.
[12] Amnesty International, "The Predator Files: Caught in the Net", 9 October 2023, amnesty.org/en/documents/act10/7245/2023/en/.
[13] Amnesty International, "Greece's surveillance scandal must shake us out of complacency", 26 January 2023, amnesty.org/en/latest/news/2023/01/greeces-surveillance-scandal-must-shake-us-out-of-complacency/.
[14] spywarefiles.eu/#worldmap.

11. The findings of the Pegasus Project and other reports prompted the European Parliament to establish the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA Committee) in 2022.[15] Subsequent inquiries by the PEGA Committee substantiated by civil society and journalists' findings, confirming that Pegasus has been used extensively across the European Union (EU) in ways that, in the view of the PEGA Committee, violated EU standards on privacy, accountability and rule of law.[16] In fact, due to lack of meaningful measures to curb the misuse of spyware and provide adequate remedy and accountability pathways, Europe has been called the "Wild West of spyware".[17] In its final fact-finding report, the PEGA Committee concluded that EU states have used "national security" as a blanket term to use spyware for the undue surveillance of journalists and politicians, in a way that deprives the term of its core meaning.[18]

12. The PEGA Committee's report also explained that Poland procured Pegasus in 2017, which was only acknowledged by the Polish government in January 2022.[19] The PEGA Committee reported that Poland used Pegasus for surveillance carried out under "political purposes", which exhibited a clear lack of transparency, judicial oversight, and adherence to rule-of-law safeguards.[20] Poland's subsequent public investigation into the Pegasus spyware abuse revealed the targeting of nearly 600 individuals and uncovered the involvement of government officials.[21]

B. INTERPLAY BETWEEN THE DEPLOYMENT OF SPYWARE AND THE STATE OBLIGATION TO PROTECT HUMAN RIGHTS

i. Obligations under Article 8 of the Convention in relation to surveillance

13. The right to privacy is enshrined in Article 8 of the European Convention of Human Rights (hereinafter the Convention), in Article 17 of the International Covenant on Civil and Political rights (ICCPR), as well as other international human rights law instruments.[22] At its core, Article 8 of the Convention protects individuals against arbitrary interference by public authorities and private actors.[23] This translates into a negative obligation on the

---

[15] europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/PEGA/DV/2023/05-08/REPORTcompromises_EN.pdf

[16] European Parliament, Investigation of the use of Pegasus and equivalent surveillance spyware, Recommendation of 15 June 2023 to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2023/2500(RSP)), P9_TA(2023)0244, B9-0260/2023, europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.pdf.

[17] Politico, "How Europe became the Wild West of Spyware", 25 October 2023, politico.eu/article/how-europe-became-wild-west-spyware/.

[18] European Parliament, Investigation of the use of Pegasus and equivalent surveillance spyware, Recommendation of 15 June 2023 to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2023/2500(RSP)), P9_TA(2023)0244, B9-0260/2023, europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.pdf.

[19] European Parliament, Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA Committee), Report of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2022/2077(INI)), 22 May 2023, europarl.europa.eu/doceo/document/A-9-2023-0189_EN.pdf, p8, para. 3.

[20] European Parliament, Investigation of the use of Pegasus and equivalent surveillance spyware, Recommendation of 15 June 2023 to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2023/2500(RSP)), P9_TA(2023)0244, B9-0260/2023, europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.pdf para O.

[21] See Cyberscoop, "Inside Poland's groundbreaking effort to reckon with spyware abuses" 14 May 2024, cyberscoop.com/inside-polands-groundbreaking-effort-to-reckon-with-spyware-abuses/; Notes From Poland "Almost 600 people targeted with Pegasus under former Polish government" 16 April 2024, notesfrompoland.com/2024/04/16/almost-600-people-targeted-with-pegasus-spyware-under-former-polish-government/; The Record, "Polish Parliament strips official of immunity, clearing path for prosecution in spyware scandal", 28 June 2024, therecord.media/polish-parliament-strips-official-of-immunity-pegasus-spyware; see also Senate of the Republic of Poland, Final Report of the Extraordinary Commission for the investigation of cases of illegal surveillance, their impact on the electoral process in the Republic of Poland and the reform of the secret services, September 23, raport_koncowy_z_prac_komisji_nadzwyczajnej.pdf.

[22] The right to privacy is enshrined in Article 12 of the UDHR. Article 17 of the ICCPR states that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence," and that "everyone has the right to the protection of the law against such interference or attacks." Poland ratified the ICCPR on 18 March 1977, see: tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?CountryID=138&Lang=EN.

[23] European Court of Human Rights (ECtHR), *Libert v. France*, application no. 588/13, 22 February 2018, paras 40-42; ECtHR, *Drelon v. France*, applications nos. 3153/16 and 27758/18, 8 September 2022, para. 85.

state to refrain from actions that can impose an undue burden to the enjoyment of the right, and a positive obligation to guarantee its protection from arbitrary interference by private actors, including individuals as well as corporations and other private entities.[24] Similarly, the United Nations Human Rights Committee has explained that the right to privacy must be guaranteed against all arbitrary interference. [25]

14. According to the Convention the right to privacy can be restricted under certain conditions that are clearly outlined by paragraph 2 of Article 8. When assessing a state's negative obligations under Article 8(2), including in the context of surveillance operations,[26] this Court examines whether the interference adhered to legal requirements, pursued a legitimate aim contained in the exhaustive list under Article 8(2), and was necessary in a democratic society.[27] Any interference must be conducted under pre-existing legal provisions, and such provisions must be clear, foreseeable, and adequately accessible.[28] This Court has also established that the law must be articulated with sufficient clarity to provide individuals with a clear understanding of the conditions and circumstances under which authorities are authorized to implement covert surveillance or collect data.[29]

15. This Court has also identified rights violations deriving from surveillance laws that lacked sufficient safeguards or failed to provide effective remedies for individuals who believe their rights were violated.[30] In *Pietrzak and Bychawska-Siniarska and Others v. Poland,* this standard was further reinforced by a finding that a member state could be in violation of Article 8 obligations if the surveillance legislation framework lacks adequate safeguards, without needing to verify if there had been an actual act of surveillance beforehand, especially if the framework fails to establish an adequate access to remedy as per the Court's standards.[31]

16. This Court has consistently affirmed that even in pursuit of legitimate national security objectives, interference with rights under Article 8 will not be justified if they are not limited in scope to prevent abuse[32] or are arbitrary.[33] In this regard, the state must establish that its use of a surveillance measure addresses a pressing social need under one of the legitimate aims, beyond it being merely "useful" or "desirable".[34]

17. Consistent jurisprudence of this Court has established that when considering a measure that could be an interference with the right to privacy, such as surveillance operations, the relevant authorities must conduct a proportionality assessment.[35] This proportionality assessment includes determining whether less intrusive means could achieve the same objective and whether the surveillance is accompanied by sufficient safeguards to prevent abuse.[36] In addition, the necessity of surveillance must be convincingly made out, which requires a direct link between the measures taken and the legitimate aim pursued.[37]

18. To comply with the proportionality assessment detailed in this Court's jurisprudence, states must also consider the scope and amount of data collected during surveillance operations, as it must be strictly limited to what is necessary to achieve a legitimate aim.[38] Data collection must be precise, targeted, and tailored to address specific, pressing needs rather than being overly broad or speculative.[39] Blanket and indefinite retention of data, as well as

---

[24] ECtHR, *Lozovyye v. Russia*, application no. 4587/09 , 24 April 2018, para. 36.
[25] International Covenant on Civil and Political Rights (ICCPR), Article 17. See also: HRC, CCPR, General Comment 16: Article 17 (Right to Privacy), adopted on 8 April 1988, para. 1.
[26] ECtHR, *Roman Zakharov v Russia*, application no 47143/06, 4 December 2015, para 227.
[27] ECtHR, *Moldovan and Others v. Romania (no. 2), application nos. 41138/98 and 64320/01* 2005, para. 95.
[28] ECtHR, *Silver and Others v. the United Kingdom*, application nos. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, 25 March 1983, para. 87.
[29] ECtHR, *Falzarano v. Italy*, application no. *73357/14* ,15 June 2021, paras 27-29); ECtHR, *Shimovolos v. Russia*, application no. 30194/09, 21 June 2011, para. 68.
[30] ECtHR, *Szabó and Vissy v. Hungary*, application no. 37138/14,12 January 2016.
[31] See, for example: ECtHR, *Pietrzak and Bychawska-Siniarska and Others v. Poland*, application nos. 72038/17 and 25237/18 , 28 May 2024, paras 143 and 241-246.
[32] ECtHR, *Big Brother Watch and Others v. United Kingdom*, *application nos. 58170/13, 62322/14 and 24960/15*, 25 May 2021, para. 333.
[33] ECtHR*, Weber and Saravia v Germany*, application no. 54934/00, 29 June 2006, para. 106.
[34] ECtHR, *Dudgeon v. the United Kingdom*, application no. 7525/76, 22 October, 1981, paras 51-53.
[35] ECtHR, *Liebscher v. Austria*, application no. 5434/17, 6 April 2021, paras 64-69.
[36] ECtHR, *Roman Zakharov v Russia*, application no. 47143/06, 4 December 2015, paras 232-234, 260.
[37] ECtHR, *Szabó and Vissy v. Hungary*, application no. 37138/14,12, 12 January 2016, paras 54-55, 73.
[38] ECtHR, *Big Brother Watch and Others v. United Kingdom*, application nos. 58170/13, 62322/14 and 24960/15, 25 May 2021.
[39] ECtHR, *S. and Marper v. the United Kingdom* [GC], application nos. 30562/04 and 30566/04, 4 December 2008.

data collection that is excessive or indiscriminate fails to meet the standard of proportionality required under Article 8.[40] In this sense, states must comply with the principle of data minimization, requiring that the amount of data collected, and the duration of its retention be no more than what is absolutely necessary for the purpose.[41]

ii. Surveillance in the context of public figures

19. While public figures may reasonably expect to face greater scrutiny due to their public roles, this heightened visibility cannot justify the use of spyware or unlawful targeted surveillance.[42] This Court has consistently affirmed that any surveillance of public officials and politicians must adhere strictly to the principles of legality, necessity, and proportionality.[43] Even when invoking public interest justifications, states are obligated to establish clear and accessible legal grounds, secure prior authorization, and ensure independent oversight to prevent arbitrary or abusive practices.[44] The Court has emphasized that these safeguards are particularly crucial in the case of public figures, who are often at risk of being targeted for political purposes. Failing to uphold these standards not only violates individual rights but also undermines the rule of law by enabling misuse of surveillance powers against political opponents or critical voices.[45]

20. In terms of international law and standards, it is important to note that while surveillance can be permissible under the ICCPR for certain legitimate aims, it is not permissible under international law to use surveillance for the purpose of tracking persons based on their exercise of human rights or protected characteristics such as political belief.[46] Similarly to this Court's jurisprudence, national security cannot be used as a blanket term to justify undue limitations to the right.[47]

21. Both the Human Rights Committee and this Court have recognized that the right to privacy underpins other key rights for civic participation, such as freedom of expression and freedom of peaceful assembly and association. In the digital age, privacy and expression are intertwined with online privacy, serving as a gateway to secure exercise of these rights.[48] The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has explained that the 'interference with privacy through targeted surveillance is designed to repress the exercise of the right to freedom of expression.'[49] This is in part due to the "chilling effect"[50] that surveillance measures can have on rights such as privacy, which this Court has long recognised comes principally from the inadequacy of safeguards, such as the avenues to challenge surveillance.[51]

iii. Importance of independent oversight as a safeguard against surveillance

22. Finally, the Convention also requires independent oversight and effective remedies for individuals affected by surveillance.[52] These safeguards are crucial to uphold the rule of law and prevent surveillance from undermining

---

[40] ECtHR, *S. and Marper v the United Kingdom* [GC], application nos. 30562/04 and 30566/04, 4 December 2008, para. 119, 125.
[41] ECtHR, *Big Brother Watch and Others v. United Kingdom*, application nos. 58170/13, 62322/14 and 24960/15, 25 May 2021. See also Council of Europe's Convention 108+ on Data Protection.
[42] ECtHR, *Lingens v. Austria*, application no. 9815/82, 8 July 1986, para. 42.
[43] ECtHR, *Roman Zakharov v Russia*, application no 47143/06, 4 December 2015, paras 233-234 and 248; ECtHR, *Rotaru v. Romania*, application no. 28341/95, 4 May 2000, para. 59.
[44] ECtHR, *Klass and Others v. Germany*, application no. 5029/71, 6 September 1978, paras 48-50.
[45] ECtHR, *Big Brother Watch and Others v. United Kingdom*, application nos. *58170/13, 62322/14 and 24960/15*, 25 May 2021, para. 495.
[46] OHCHR, Report: The Right to Privacy in the Digital Age, 30 June 2014, UN Doc. A/HRC/27/37.
47 UN High Commissioner for Human Rights (OHCHR), The Right to Privacy in the Digital Age, 30 June 2014, UN Doc. A/HRC/27/37, digitallibrary.un.org/record/777869?ln=en, paras 23-24.
[48] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report: Surveillance and human rights, 28 May 2019, UN Doc. A/HRC/41/35, para. 24.
[49] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc A/HRC/41/35, 28 May 2019, para. 21.
[50] The chilling effect occurs when the existence or threat of surveillance discourages individuals from exercising these rights, particularly in sensitive areas such as journalism, activism, or political opposition.
[51] ECtHR, *Roman Zakharov v Russia*, application no 47143/06, 4 December 2015.
[52] ECtHR, *Big Brother Watch and Others v. United Kingdom*, application nos. 58170/13, 62322/14 and 24960/15, 25 May 2021.

the rights and freedoms by the Convention.[53] Our written submissions expand upon the requirements for such oversight and discuss what is required for a remedy to be effective in the context of surveillance in the following section.

23. To comply with the Convention, interferences under Article 8 require independent oversight which must include strict controls on the authorization, execution, and review of surveillance measures to protect individuals from excessive or unjustified monitoring.[54] For surveillance operations to be lawful, emphasis has been placed on establishing *a priori* judicial authorization that must be detailed, specific, and substantive to safeguard against abuse and unjustified intrusions into privacy.[55] In addition, this Court has clearly stated that generic or blanket authorizations are insufficient and inadequate, as they risk overbroad or indiscriminate surveillance.[56] The importance of independent and impartial judicial oversight has also been underscored to ensure that the approval process is free from political or administrative influence.[57]

24. Further, the judicial approval required by the Court standards must clearly define the scope and objectives of the surveillance, including the individuals targeted, the data to be collected, and the duration of the operation.[58] It must also involve a thorough assessment of the necessity and proportionality of the measures, ensuring that the interference is justified and tailored to the legitimate aim pursued.[59] Considering this "substantive" requirement, it is reasonable to expect that enough information about the technical implications of the tool to be used to conduct the surveillance operation should also be provided and taken into proper consideration. It is also reasonable to require that, in assessing the proportionality test, the oversight receives enough information about the means chosen to conduct the surveillance operation to assess whether such means are the least invasive available for the achievement of the legitimate aim stated.

iv. The right to effective remedy

25. All persons whose rights have been violated have a right to an effective remedy for such violation. This right derives from the general principle of international human rights law that every breach gives rise to a corresponding obligation to provide an effective remedy.[60] The right to an effective remedy is a "*core tenet of international human rights law*"[61] that is enshrined in customary international law.[62] The right to effective remedy includes the duty to *"provide those who claim to be victims of a human rights…violation with equal and effective access to justice…irrespective of who may ultimately be the bearer of responsibility for the violation*."[63]

26. Article 13 of the Convention guarantees an effective remedy for rights violations before a national authority. While the "authority" referred to in the text of Article 13 does not have to be a judicial authority, *"if it is not, its powers and the guarantees which it affords are relevant in determining whether the remedy before it is effective."*[64]

---

[53] ECtHR, *Roman Zakharov v Russia*, application no 47143/06, 4 December 2015 and ECtHR, *Big Brother Watch and Others v. United Kingdom*, application nos. 58170/13, 62322/14 and 24960/15, 25 May 2021.
[54] ECtHR, *Roman Zakharov v Russia*, application no 47143/06, 4 December 2015 and European Court of Human Rights, *Big Brother Watch and Others v. United Kingdom*, application nos. 58170/13, 62322/14 and 24960/15, 25 May 2021.
[55] ECtHR, *Roman Zakharov v Russia*, application no 47143/06, 4 December 2015 and European Court of Human Rights, *Big Brother Watch and Others v. United Kingdom*, application nos. *58170/13, 62322/14 and 24960/15*, 25 May 2021.
[56] ECtHR, *Kennedy v. United Kingdom*, application no. *26839/05*, 18 May 2010, para. 160.
[57] ECtHR, *Klass and Others v. Germany*, application no. 5029/71, 6 September 1978, para. 55
[58] ECtHR, *Szabó and Vissy v. Hungary*, application no. 37138/14,12 January 2016, para. 77.
[59] ECtHR, *Roman Zakharov v Russia*, application no. 47143/06, 4 December 2015, para. 260
[60] Chorzów Factory (Germany v. Poland), 1928 PCIJ (ser A) No. 17, at para 73: *("[I]t is a principle of international law, and even a general conception of law, that any breach of an engagement involves an obligation to make reparation.").*
[61] UN Human Rights Council, Report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development (10 May 2016), A/HRC/32/19, para. 6.
[62] Prosecutor v. André Rwamakuba, Case No. ICTR-98- 44C, Decision on Appropriate Remedy, para 40 (31 January 2007); Prosecutor v. André Rwamakuba, Case No. ICTR-98-44C-A, Decision on Appeal Against Decision on Appropriate Remedy, paras 23-5 (13 September 2007); and Cantoral-Benavides v. Perú, 2001 Inter-Am. Ct. H.R. (ser.C) No. 88, para. 40.
[63] General Assembly Resolution 60/147, Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of international Human Rights Law and of Serious Violations of International Humanitarian Law.
[64] ECtHR, *Judla v. Poland* [GC], application no. 30210/96, 26 October 2000, para. 157.

27. The remedy required by Article 13 must be "effective" in practice as well as in law, in that its exercise must not be unjustifiably hindered by the acts or omissions of state authorities.[65] To be effective, a domestic remedy has to offer minimum guarantees of promptness.[66] Given the nature of being subject to secret surveillance, it is highly unlikely, and in many circumstances impossible for an individual to know that they have been targeted. This is especially the case in the use of spyware such as Pegasus, which is designed to hide itself from detection and does not need the target to interact with it for it to be activated.[67] Therefore, to enable an individual to have all the necessary information to challenge whether they have been subjected to unlawful targeting, they should be notified about their having been so targeted.

28. In line with this, this Court has routinely recognised the importance of *post-facto* notification as both a necessary safeguard against the abuse of surveillance powers and as a critical component of securing the right to an effective remedy under Article 13:

> "*The question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for any recourse by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their justification retrospectively. As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should be provided to the persons concerned."*[68]

29. Independent judicial oversight over the deployment and authorization of surveillance is a key element of the right to effective remedy because it, among other things, enables an individual to challenge the surveillance *post facto.* However, where spyware obscures detection, it cannot be independently and effectively overseen which limits the scope for judicial scrutiny of its use. For similar reasons this Court has recognised that "*a control mechanism for covert surveillance operations should preferably be based on an independent control body acting on its own initiative and possessing the legal instruments necessary to detect and combat abuses.*"[69] It is often virtually impossible for targets to even prove the existence of surveillance, either because of technical hurdles or the covert nature of its use. These factors limit access to effective remedy and further expand the chilling effect on human rights that surveillance necessitates. This supports the conclusion that states must refrain from using and otherwise ban highly invasive spyware given that it is inherently incompatible with their obligation to protect the right to privacy and guarantee right to effective remedy.

C. INCOMPATIBILITY OF SPYWARE WITH STATES' HUMAN RIGHTS OBLIGATIONS

i. Highly invasive spyware is incompatible with international and regional human rights law and standards and must therefore be banned

30. As our research shows, spyware has been weaponized by governments to target human rights defenders, journalists, diplomats, members of government, and even political opposition to silence dissent, generate a chilling effect, and dismantle civil society networks.[70] Digital surveillance is often used in tandem with other tactics that can indicate a deterioration of the enjoyment of human rights by all. Amnesty International submits that the unchecked proliferation of spyware is eroding human rights, including freedom of expression, privacy, and the right to effective remedy.

---

[65] ECtHR, *İlhan v. Turkey* [GC], application no. 22277/93, 27 June 2000, para. 97.
[66] ECtHR, *Kadiķis v Latvia (No. 2),* application no. 62393/00, 4 May 2006, para. 62.
[67] It is important to note that spyware can infect a device when a target clicks on a malicious link or even without them doing anything. The infection methods include "1-click" attack, by which the device is infected when the target clicks on a compromised link. Compromised links can be sent many different ways including via text, email or on social media platforms. The infection can also occur through a "zero-click" attack: the device is infected without the user interacting with, or doing, anything. See: securitylab.amnesty.org/glossary/.
[68] ECtHR, *Szabó and Vissy v. Hungary*, application no. 37138/14,12 January 2016, para 86; ECtHR, *Weber and Saravia v Germany*, application no. 54934/00, 29 June 2006, para 135; ECtHR, *Roman Zakharov v Russia*, application no 47143/06, 4 December 2025, para. 287.
[69] ECtHR, *Pietrzak and Bychawaska-Siniarska and Others v Poland*, application nos 72038/17 and 25237/18, 28 August 2024, para. 195.
[70] See, for example: Amnesty International, "*Thailand: "Being ourselves is too dangerous": Digital violence and the silencing of women and LGBTI activists in Thailand"*, 16 May 2024, amnesty.org/en/documents/asa39/7955/2024/en/; and generally: securitylab/amnesty.org.

31. Digital surveillance can not only have a direct impact in the enjoyment of an individual's human rights, but it can also cause a pervasive chilling effect. This is demonstrated by Amnesty International's research, which shows that human rights defenders and journalists who fear being subjected to surveillance will be less likely to speak out critically of their government or report on certain issues, for fear of being targeted and putting themselves, their sources, colleagues, and loved ones at risk.[71] As this Court has long held, the chilling effect of surveillance comes principally from the inadequacy of safeguards, such as the avenues to challenge surveillance,[72] which this Court has ruled are lacking in Poland.[73] It is this inability to know whether a person may be under surveillance or to challenge it that in part creates a chilling effect on rights and further limits its chance to access redress.

32. Further, Amnesty International's technical investigations have highlighted how highly invasive spyware such as Pegasus cannot comply, by design, with the proportionality assessment that mandates utilizing the least invasive measure to achieve legitimate aims. [74] Spyware such as Pegasus is an extremely intrusive tool whose access to data in a device cannot be limited. Given that its access to data cannot be limited to only what is reasonably required for the purposes of the surveillance operation, highly invasive spyware cannot comply with the principle of data minimization established in this Court's jurisprudence, as outlined in paragraph 18. As noted by the European Data Protection Supervisor, with the use of such highly invasive tools, *"[t]he level of interference with the right to privacy is so severe that the individual is in fact deprived of it. In other words, the essence of the right is affected. Therefore, its use cannot be considered proportionate – irrespective of whether the measure can be deemed necessary."*[75] This aligns with the reasoning presented by the former UN Special Rapporteur on Counterterrorism, who argues that spyware that is incapable of being meaningfully limited in its functionality, and whose use cannot be audited independently, should be subject to a ban.[76]

33. Amnesty International's research has highlighted that highly invasive spyware such as Pegasus cannot be independently audited, i.e. inspected. Due to this, it cannot be determined whether its use has been limited in its functionality. Moreover, as explained in paras 7 and 8 above, once a device has been infected with Pegasus, access is granted to all areas. Simply put, by design, there are no avenues to independently verify and guarantee that its use is compatible with key state obligations in the context of surveillance operations, or indeed, whether it has been abused to target people based on the exercise of their human rights, or in a manner incompatible with the safeguards and standards established by this Court. In other words, the inability to independently audit the use of spyware such as Pegasus means that it is impossible to verify whether any safeguards were adhered to before, during and after its use, as is required for any surveillance operations as per this Court's jurisprudence. It also means that it is impossible to verify whether such targeting was undertaken within existing legal structures, or whether such structures provide adequate protection from the arbitrary interference with the right.

34. Given that highly invasive spyware is designed to subvert human rights safeguards and accountability, even the most rigorous safeguards would be incapable of preventing abuses of such tools. Accordingly, Amnesty

---

[71] Amnesty International, "*It's Enough for People to Feel it Exists: Civil Society, Secrecy, and Surveillance in Belarus*," 7 July 2016, amnesty.at/media/1119/amnesty-surveillance-in-belarus.pdf; Amnesty International, *"The Global Shadow of Uzbekistani Surveillance*, 31 March 2017, youtube.com/watch?v=nRPjLEBn2j0; Amnesty International, "*These walls have ears": The chilling effect of surveillance in South Sudan,* 2 February 2021, amnesty.org/en/documents/afr65/3577/2021/en/; Amnesty International*, "Being ourselves is too dangerous": Digital violence and the silencing of women and LGBTI activists in Thailand*, amnesty.org/en/documents/asa39/7955/2024/en/, 16 May 2024; Amnesty International, "*A Digital Prison": Surveillance and the suppression of civil society in Serbia*, amnesty.org/en/documents/eur70/8813/2024/en/, 16 December 2024. See also Daragh Murray, Pete Fussey, Kuda Hove, Wairagala Wakabi, Paul Kimumwe, Otto Saki, Amy Stevens, 'The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe', *Journal of Human Rights Practice*, Volume 16, Issue 1, February 2024, Pages 397–412, academic.oup.com/jhrp/article/16/1/397/7234270. And see, for example: amnesty.org/en/latest/news/2023/05/dominican-republic-pegasus-spyware-journalists-phone/

[72] ECtHR*, Roman Zakharov v Russia*, application no 47143/06, 4 December 2015.

[73] ECtHR, *Pietrzak and Bychawaska-Siniarska and Others v Poland*, application nos. 72038/17 and 25237/18, 28 August 2024.

[74] Amnesty International (n 71). See also, securitylab.amnesty.org/.

[75] European Data Protection Supervisor, Preliminary Remarks on Modern Spyware, 15 February 2022, p. 8

[76] Fionnuala Ní Aoláin, Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism "Global regulation of the counter-terrorism spyware technology trade: scoping proposals for a human-rights compliant approach", April 2023, para. 66.

International has called for the prohibition of the use of highly invasive spyware, such as Pegasus.[77] In this sense, it is fundamental that states comply with their human rights obligations, particularly by refraining from using highly invasive spyware technology and in establishing and following robust oversight and safeguards to prevent surveillance from being weaponized against dissent.

35. This Court has also repeatedly cautioned against the misuse of surveillance to monitor or suppress political opposition, recognizing its severe implications for human rights.[78] In this regard, this Court has highlighted the risks posed by unchecked surveillance powers in targeting dissenting voices, which can erode the rule of law.[79] Similarly, it has noted that surveillance can create a climate of fear, discouraging opposition politicians and activists from engaging in legitimate activities.[80] This Court has also stressed that inadequate safeguards heighten the risk of surveillance being used arbitrarily for political purposes.[81] This case is therefore an opportunity for this Court to continue to build on such clear standards towards the protection of individuals' human rights against undue interference deriving from covert surveillance operations.

ii. Stronger human rights-based safeguards must be required for states to legitimately use other forms of spyware

36. For reasons set out above, the use of highly invasive spyware such as Pegasus should be banned globally due to the risks its design poses to human rights. Unless the use of spyware is governed by strict human rights safeguards as outlined by this Court, even types of spyware that do have technical design features that enable their compliance with human rights standards will pose unacceptable risks to states upholding their human rights obligations. For this reason, Amnesty International, alongside a growing list of international legal experts and authorities, [82] have called for a moratorium on the use or transfer of all spyware until such time as it can be demonstrated that human rights-compliant safeguards are in place that are capable of preventing abuse in practice.

37. As outlined in Part B, this Court has established core safeguards that all surveillance operations, regardless of the means used, must comply with. Further, in addition to their negative obligations, states also have a positive duty to protect against arbitrary or unlawful interference with human rights by private actors, including business enterprises. While this obligation flows from the jurisprudence of this Court in interpreting Article 8 of the Convention,[83] it is also reflected in the UN Guiding Principles on Business and Human Rights. If a state allows

---

[77] See also: Amnesty International, The Predator Files: Caught in the Net, amnesty.org/en/documents/act10/7245/2023/en 9 October 2023. EDRi, a European collective of 47+ non-governmental organisations, experts, advocates and academics working to defend and advance digital rights across the continent calls for a ban on all spyware: edri.org/our-work/press-release-brussels-rocked-by-major-spyware-scandal-urgent-call-for-ban/.

[78] ECtHR, *Roman Zakharov v Russia*, application no 47143/06, 4 December 2015 paras 232-234.

[79] ECtHR, *Roman Zakharov v Russia*, application no 47143/06, 4 December 2015, para. 248.

[80] ECtHR, *Big Brother Watch and Others v United Kingdom*, Application nos. 58170/13, 62322/14 and 24960/15, 25 May 2021, para. 495.

[81] ECtHR, *Szabó and Vissy v. Hungary*, application no. 37138/14,12 January 2016, para. 53.

[82] UN Office of the High Commissioner for Human Rights (OHCHR), Report: The right to privacy in the digital age, August 2022, A/HRC/51/17; David Kaye, Special Rapporteur on freedom of opinion and expression 2014-2020: ohchr.org/en/press-releases/2019/06/un-expert-calls-immediate-moratorium-sale-transfer-and-use-surveillance; Fernand de Varennes, Special Rapporteur on minority issues; Irene Kahn, Special Rapporteur on freedom of opinion and expression: ohchr.org/en/press-releases/2023/02/spain-un-experts-demand-investigation-alleged-spying-programme-targeting; Mary Lawlor, Special Rapporteur on the situation of human rights defenders, Clement Nyaletsossi Voulé, Special Rapporteur on the rights to freedom of peaceful assembly and of association: ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening; E. Tendayi Achiume, Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, Report, "Racial and Xenophobic discrimination and the use of digital technologies in border and immigration enforcement", 22 September 2021, UN Doc A/HRC/48/76, p.19 para. 66(b). Fionnuala Ní Aoláin, Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism "Global regulation of the counter-terrorism spyware technology trade: scoping proposals for a human-rights compliant approach" April 2023; Michelle Bachelet, UN High Commissioner for Human Rights 2018-2022: Statement to the Committee on Legal Affairs and Human Rights, Parliamentary assembly Council of Europe – Hearing on the implications of the Pegasus spyware, 14 September 2021.

[83] ECtHR, *X and Y v. The Netherlands*, Application no. 8978/80, 26 March 1985, para. 23; see also ECtHR, *Moldovan and Others v. Romania (Judgment No. 2)*, Applications nos. 41138/98 and 64320/01, 30 November 2005, para. 93; ECtHR, *Fadeyeva v. Russia*, Application no. 55723/00, 9 June 2005, para. 89; ECtHR, *Ouranio Toxo and Others v. Greece*, Application no. 74989/01, 20 January 2006, para. 37; ECtHR, *Von Hannover v. Germany [No. 2]* [GC], Applications nos. 40660/08 and 60641/08, 7 February 2012, para. 98; ECtHR, *Lozovyye v. Russia*, application no. 4587/09, 24 April 2018, para. 36.

spyware providers to operate without regulation or oversight, it may be complicit in human rights abuses, particularly those arising from Article 8. Similarly, if a state allows a business entity to use such tools without proper oversight and fails to provide effective remedy to those impacted by its misuse, then it may likewise be responsible for failing to comply with its duty to protect against and provide remedy for human rights harm by private actors.

38. Amnesty International submits that having such standards enshrined in legislation, as well as demonstrated, consistent implementation, oversight, and enforcement, are fundamental to consider a system as human-rights compliant. While the safeguards established in this Court's jurisprudence, as well as by other legal authorities must be comprehensively implemented for states to comply with international law and standards, Amnesty International emphasises these four in particular:

    i. First, digital surveillance may only occur where a time-limited warrant has been issued by an independent judicial authority because of individualized reasonable suspicion of wrongdoing, in line with international human rights law and standards. Additionally, the use of spyware must be done without discrimination; restricted to the most serious cases of individualised reasonable suspicion, without using national security or public safety as blanket terms; and authorized by an independent judicial authority only where it has been established that less restrictive means would be ineffective to meet a legitimate aim, taking account of the human rights harms implicit in the use of such tools.

    ii. Second, the use of spyware, as well as the overall system and rules governing such tools, must be subject to independent oversight by judicial and/or other independent oversight authorities that can ensure that the use of spyware complies with international human rights law and standards.

    iii. Third, states have the positive obligation to inform all persons who have been subjected to surveillance of this fact, and the grounds upon which it was conducted, the material collected and any potential remedies as soon as notification can be made without jeopardising the legitimate purpose of the surveillance. States must also remove barriers to remedy for victims of unlawful surveillance and ensure that both judicial and non-judicial paths to remedy are available in practice. States must also include routine effective judicial and parliamentary oversight of laws and practices governing surveillance operations.

    iv. Fourth, the appropriate authorities must proactively make available to the public all relevant information, including the overall legal framework governing communications surveillance; the entities authorized to conduct surveillance; the procedures to be followed for authorizing communications surveillance, and for the use, sharing, storage, and destruction of communications material; and statistics about the use of such surveillance, including the number and type of investigations for which the use of spyware was requested, approved or denied.

39. Besides these safeguards directly linked to the rights to remedy and privacy, Amnesty International submits that other safeguards to be included in legislation in order to protect from the pervasive harms of digital surveillance, would include regulating the export of surveillance technologies such that it ensures the denial of export authorizations where there is a substantial risk that the export in question could be used to violate human rights; establishing accountability mechanisms designed to provide victims of surveillance abuses a pathway to remedy, including financial and legal support; and regulating private actors to prevent disproportionate interference with human rights.

CONCLUSION

40. Based on our submissions above, Amnesty International respectfully encourages this Court to (1) use this case as an opportunity to further strengthen its standards on digital surveillance and the use of spyware, principally by finding that a ban on highly invasive spyware is required under the Convention; (2) to reaffirm that states must immediately put in place legislation with adequate safeguards for the specific use of spyware as part of surveillance operations, which must include adequate independent judicial and parliamentary oversight, as well as remove barriers to access to remedy to victims; (3) that such legislation must be fully enforced, and states should be mandated to transparently report on the oversight of such use; (4) to reiterate the harms that surveillance poses to human rights and the rule of law and (5) to affirm that the use of highly invasive spyware is fundamentally incompatible with the realisation and enjoyment of human rights.