***Javadov and Others v. Azerbaijan*, Application No. 30573/22**
***Ganbarova v. Azerbaijan*, Application No. 45877/22**

Intervention as amici curiae by

Jane Duncan
Professor, University of Glasgow

Anneke Meerkotter
Executive Director, Southern Africa Litigation Centre (SALC)

Piers Pigou
Executive Director, IntelWatch

David Kaye
Director, UCI Law International Justice Clinic

pursuant to
Article 36(2) of the European Convention on Human Rights, Rule 44.3(a) of the Rules of Court, and the authorization of the Court's President of Section III, Judge Ioannis Ktistakis

18 April 2026

I. Introduction

1. This is the intervention of Intelwatch, Professor Jane Duncan of the University of Glasgow, the Southern Africa Litigation Centre ("SALC"), and the International Justice Clinic ("IJC") at the University of California, Irvine School of Law, in connection with application no. 45877/22, made by Aynur Ganbarova and others against Azerbaijan, and application no. 30573/22 made by Javad Javadov and Others against Azerbaijan.[1] The intervention is submitted in accordance with Article 36 of the European Convention on Human Rights ("ECHR") and Rule 44 of the Rules of Court. Leave to intervene was granted on 10 March 2026. Relying on reports and investigations, this intervention offers the following:
   - Examples and analysis of the global impact and implications of the Court's judgment on issues of surveillance, freedom of opinion and expression, and the right to privacy, particularly those in Global South countries, including those in Africa; and
   - An analysis on the severe impact of spyware on human rights in the Global South with observations on the stringent interpretation and application of ECHR, the African Charter on Human and Peoples' Rights ("ACHPR"), the American Convention on Human Rights ("ACHR"), and the International Covenant on Civil and Political Rights ("ICCPR"), particularly the requirements of legitimate aim, legality, and of necessity and proportionality, including the safeguards required to be put in place, when applied to the government use of spyware.
2. Connecting these two points, this intervention concludes that the anticipated global impact of this Court's decision on spyware use—including in the Global South, where checks and balances are often weak—calls for a granular review, especially of the existence of effective institutional safeguards and the fulfillment of conditions necessary to ensure the right to an effective remedy, such as implementing notification system for surveillance subjects and logging each step of spyware operations. These measures are critical, as the victims and public-led oversight are essential to reclaim control over surveillance in contexts where surveillance capacity has outpaced institutional oversight.

II. Background

3. Commercial spyware, such as Pegasus, has been used against journalists and human rights defenders in Africa and the Global South. In Africa, while cases in which the attribution of spyware use is confirmed remain rare, there are cases that suggest that governments are the likely culprits. Moroccan journalist Omar Radi, who reported on human rights abuses, had his cellphone infected with Pegasus.[2] As many as 10,000 people have likely been targeted with Pegasus in Morocco.[3] The devices of Togolese journalists Loïc Lawson and Anani Sossou were infected with spyware. Both journalists later faced criminal prosecution for their reporting.[4] More recently in Kenya, filmmakers and producers were arrested, and spyware was installed on their phones, during the filming of a documentary about the killing of protestors by security forces.[5] In Angola, journalist Teixeira Cândido was targeted with Predator spyware.[6]

---

[1] The International Justice Clinic advanced clinic students, Ethan Prom, Jake Hernandez, Jessica Leeds, Preston Taylor, and Tara Shafiei, as well as Hinako Sugiyama, a senior counsel and digital rights fellow, advised this intervention. Tachilisa Badala Balule, Associate Professor of Law at the University of Botswana contributed to this intervention.

[2] *Moroccan Journalist Targeted with Network Injection Attacks Using NSO Group's Tools*, Amnesty Int'l (22 June 2020), https://perma.cc/YP2Q-T9AN.

[3] Nathaniel Allen & Matthew La Lime, *How Digital Espionage Tools Exacerbate Authoritarianism Across Africa*, Brookings (Nov. 19, 2021), https://www.brookings.edu/articles/how-digital-espionage-tools-exacerbate-authoritarianism-across-africa/.

[4] *Pegasus Spyware Used to Target Togolese Journalists Loïc Lawson and Anani Sossou*, Comm. Prot. Journalists (23 Jan. 2024), https://cpj.org/2024/01/pegasus-spyware-used-to-target-togolese-journalists-loic-lawson-and-anani-sossou/.

[5] *Spyware Installed on Kenyan Filmmakers' Phones in Police Custody*, Comm. Prot. Journalists (10 Sept. 2025), https://cpj.org/2025/09/spyware-installed-on-kenyan-filmmakers-phones-in-police-custody/.

[6] '*I Literally Felt Naked': Angolan Journalist Teixeira Cândido Targeted with Predator Spyware,* Comm. Prot. Journalists (17 Feb. 2026), https://cpj.org/2026/02/i-literally-felt-naked-angolan-journalist-teixeira-candido-targeted-with-predator-spyware/.

4. Human rights bodies and experts have long, consistently confirmed the considerable harms of commercial spyware in general,[7] which are likely to be exacerbated in Africa and the Global South. In this region, checks and balances in many countries remain fragile. Under limited oversight, African governments have been enacting new laws that ostensibly protect against cybercrime while granting expansive surveillance powers and acquiring new tools in addition to spyware, depriving journalists and human rights defenders of almost the entirety of their informational control.[8]

III. The global impact of the Court's judgment on issues of surveillance, particularly in Africa and the Global South

5. With many states facing emerging issues with spyware, early jurisprudence from the European Court of Human Rights ("ECtHR") will establish standards that will be followed by other jurisdictions, particularly jurisdictions with regional human rights mechanisms.[9]
6. Judgments of the ECtHR have already had a pronounced influence on the African Court of Human and Peoples' Rights ("ACtHPR"). Since its inception in June 1998, the ACtHPR has referred to the ECtHR' rulings in more than a fifth of its finalized cases: "In fact, early evidence suggests that, of 62 finalized cases, the African Court has referred to the ECtHR in some 14 cases, primarily in judgments on the merits, and particularly when delving into new areas of jurisprudence."[10]
7. The best examples of this connection are cases concerning freedom of expression, such as *Lohé Issa Konaté v. Burkina Faso* (2014) and *Ingabire Victoire Umuhoza v. Rwanda* (2018). The ACtHPR cited the ECtHR judgments to establish rules about necessity and proportionality and penalties for defamatory speech. In *Konaté,* the ACtHPR found that Burkina Faso violated Article 9 of the African Charter and Article 19 of the ICCPR. To reach this ruling, the ACtHPR adopted the ECtHR principle, among other similar principles, that criminal defamation laws should only be used as a last resort. It was this proportionality standard that guided the African court to its ruling in *Ingabire* which relied on *Konaté,* as it was the first case for the court to directly address the freedom of expression.[11]
8. When it comes to digital surveillance, there is hardly any jurisprudence of the ACtHPR or subregional African courts, partly because there is no right to privacy explicitly recognized under the African Charter of Human and Peoples' Rights. Indeed, there is a general vacuum of surveillance-related jurisprudence in subregional and domestic courts: "In most African countries, despite state parties' obligations under international human rights system especially on the use of communication surveillance, there is no comprehensive set of rules on the subject both at the regional and domestic level."[12]
9. Other entities have also highlighted this gap in jurisprudence. The Collaboration on International ICT Policy for East and Southern Africa ("CIPESA") created a comprehensive overview of surveillance issues in Africa, acknowledging that in many countries, including Uganda, Kenya, and Nigeria, clear norms have yet been established on how to ensure state digital surveillance is conducted in a way that

---

[7] *See* David Kaye (Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression), *Report on the Adverse Effect of the Surveillance Industry on Freedom of Expression*, U.N. Doc. A/HRC/41/35 (28 May 2019); Euro. Comm'n for Democracy Through Law, *Report on a Rule of Law and Human Rights Complaint Regulation of Spyware* (2024) ("Venice Commission Report"), § 9; *Ghanem Al-Masarir v Kingdom of Saudi Arabia*, EWHC 119 §§ 82(a-f) (KB) (2026) (The Court credited Plaintiff (a human rights activist)'s testimony that being targeted by spyware led to depression, paranoia, affected his business, caused poor sleep, and created a fear of using digital devices).

[8] Inst. Dev. Studies, *Mapping the Supply of Surveillance Technologies to Africa: Case Studies from Nigeria, Ghana, Morocco, Malawi, and Zambia* (2023).

[9] *See Abdoulaye Nikiema (Norbert Zongo) v. The Republic of Burkina Faso*, No. 013/2011, Decision, ACtHR, § 70 (24 June 2014) (noting that some rules can be directly applied from European states, acknowledging that many African and European states stem from the same "legal family").

[10] The ACtHR Monitor, *The European Court of Human Rights Vis-à-vis the African Court of Human and Peoples Rights* (2020).

[11] *African Court Addresses Freedom of Expression in Burkina Faso, in Landmark Judgment*, N.E. Univ. Sch. L., Ctr. Glob. L. and Justice (3 Feb. 2015), https://cglj.org/2015/02/03/african-court-addresses-freedom-of-expression-in-burkina-faso-in-landmark-judgment/.

[12] Tomiwa Ilori, *Framing a Human Rights Approach to Communication Surveillance Laws Through the African Human Rights System in Nigeria, South Africa, and Uganda*, 5 Afr. Human Rts. Yearbook 134, at 136 (2021).

complies with human rights law.[13] A scholar highlighted the fact that there is a gap in jurisprudence in human rights law in Africa when it comes to digital surveillance and that Africa may look to other regions' jurisprudence on the matter.[14]

10. This vacuum of human rights norms is also evident in policy. Principle 25(3) of the Declaration of Principles on Freedom of Expression and Access to Information in Africa directs states to ensure the protection of journalistic sources in communication surveillance.[15] However, the African Commission on Human and Peoples' Rights ("African Commission") has not set specific standards required to achieve that goal.
11. With no clear norms from the regional African human rights institutions, many governments are expanding their authority and capacity of surveillance that has outpaced limited oversight.[16] Tachilisa Badala Balule, Associate Professor of Law at the University of Botswana, quotes Jane Duncan, Professor of Digital Society at the University of Glasgow: "In many countries where surveillance has been gaining traction, the development of appropriate oversight mechanisms has been noted to be lagging, resulting in a vacuum of democratic oversight[…]in some states that have in place official oversight mechanisms, they often lack the power and resources to perform their oversight role effectively[…]"[17]
12. Acknowledging the high likelihood that the ruling from the ECtHR on the present cases will influence African norms with respect to spyware use, this reality should be kept in mind when creating rules that will be applied outside the European context. New rules carefully and thoughtfully established by the ECtHR can provide a path towards greater human rights protections in countries where oversight is weak.

IV. State obligations concerning the state's use of spyware under international human rights law

A. Overview

13. To support the Court in charting a path toward sound human rights protections *globally*, this section provides a set of key, specific state obligations related to the use of spyware under international human rights law. From a global standpoint, this intervention synthesizes the major human rights instruments, namely the ECHR, ACHPR, ACHR, and ICCPR. They all explicitly reference the Universal Declaration of Human Rights as one of their normative bases, and their overall interpretations have generally harmoniously progressed through cross-reference of each other's judgments and deliberations.[18]
14. Many human rights bodies and experts have already contributed valuable perspectives on the assessment of spyware under international human rights law, often relying on this Court's existing jurisprudence as a primary source of norms. In addition to upholding those works, this amicus filing

---

[13] Collaboration on Int'l ICT Pol'y for E. and S (CIPESA). Africa, *Mapping and Analysis of Privacy Laws in Africa*, at 8 (2021), https://perma.cc/S8RB-J2ER.

[14] *See generally* Yohannes Eneyew Ayalew, *Untrodden Paths Towards the Right to Privacy in the Digital Era under African Human Rights Law,* 12 Int'L Data Priv. L 16, at 29–32 (2022).

[15] Afr. Comm'n on Hum. & Peoples' Rts., Declaration of Principles on Freedom of Expression and Access to Information in Africa principle 25 (Nov. 2019).

[16] A notable exception is South Africa, where its Constitutional Court struck down its interception law (see *infra* § 14); however, the Parliament has yet to amend the law.

[17] Jane Duncan & Allen Munoriyarwa, *Democratising Spy Watching: Public Oversight of Intelligence-driven Surveillance in Southern Africa*, at 69 (2025).

[18] This harmonious progress has been achieved through cross referencing between the Human Rights Committee and regional human rights courts in their decisions. *See e.g,* Erik Voeten, *Borrowing and Nonborrowing Among International Courts*, 39 J. Legal Stud. 547, at 562-66 (2010) (stating "The ECtHR referred to the case law of the IACHR in five majority judgments [...]. Three of these [cited] the IACHR's landmark *Velasquez Rodrıguez* decision . . . the IACHR has referred to ECtHR judgments in 60 percent of its 126 judgments since 2000"). Article 7 of the Protocol to the ACHPR obliges the ACtHPR to apply the ACHPR alongside any human rights treaties ratified by the country concerned, such as ICCPR. The Human Rights Committee references decisions by regional human rights courts or bodies in its General Comments. *See* Hum. Rgts. Comm., Gen. Comment No. 37 (2020) on the Right of Peaceful Assembly (Article 21), U.N. Doc. CCPR/C/GC/37 (23 July 2020), footnotes 15, 18, and 84.

places particular emphasis on specific obligations that—while not yet clearly required by this Court for other forms of secret surveillance—should be recognized in the context of spyware, given the associated new legal issues. To this end, this intervention has been informed by recent notable jurisprudence on secret surveillance, including that from outside Europe. These include, for example, *the Amabhungane Centre for Investigative Journalism NPC v President of the Republic of South Africa* (2021) ("*Amabhungane*"), in which the Constitutional Court of South Africa declared the Regulation of Interception of Communications and Provision of Communication-related Information Act unconstitutional,[19] and *The Members of José Alvear Restrepo Lawyers' Collective v Colombia* (2023) ("*CAJAR*"), in which the Inter-American Court of Human Rights ("IACtHR") held that Colombia's secret surveillance of a member of a civil society organization violated the ACHR.[20]

15. The ECHR, ACHPR, ACHR, and ICCPR robustly protect a set of rights that are particularly implicated by states' use of spyware. Those rights include the right to privacy and the right to freedom of expression.[21]
    - *The right to privacy*: The ECHR, ACHPR, ACHR, and ICCPR all guarantee the right to privacy.[22] While the ACHPR does not explicitly recognize the right to privacy, the African Commission and scholars have highlighted the fact that rights can be "implied with the combination of different rights that were included.[23] Privacy includes informational privacy, namely, "the ability of individuals to determine who holds information about them and how that information is used."[24]
    - *The right to freedom of expression*: The ECHR, ACHPR, ACHR, and ICCPR all guarantee freedom of expression. Article 19(2) of ICCPR sets its robust scope as "freedom to seek, receive and impart *information* and ideas of all kinds . . . regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media." Regional conventions generally *mirror* such a robust scope of protection.[25] In the digital age, privacy and free expression are closely interconnected, as the protection of privacy is a basis for people to express themselves without fear of retaliation.[26]
16. The use of spyware restricts the rights to freedom of expression and privacy most severely, compared to other forms of secret surveillance such as a secret mobile phone interception system this Court examined in *Roman Zakharov v. Russia* (2015). Spyware can covertly take full control of the electronic device, giving an attacker more information than possible from a physical house, in terms of the amount, variety, and historical depth of the data, as the U.S. Supreme Court recognized in *Riley v. California* (2014).[27] Spyware users can access any data indiscriminately, including those protected as journalistic sources or under attorney-client privilege, even bypassing encryption. Given this exceptionally severe intrusion on privacy, the mere possibility of being targeted by spyware poses a

[19] *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others* (CCT 278/19; CCT 279/19) [2021] ZACC 3; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC) (4 February 2021) (2021).
[20] *Members of the "José Alvear Restrepo" Lawyers Collective v. Colombia, Preliminary Objections*, Merits, Reparations and Costs, Inter-Am. Ct. H.R. (ser. C) No. 506, (18 Oct. 2023) ("*CAJAR*").
[21] Spyware also implicates other fundamental rights, such as the right to peaceful assembly and association. It also may involve grave secondary impacts, implicating the right to life, the prohibition of torture, arbitrary detention, and the right to freedom of movement and due process. Among many sources, reports by organizations such as Citizen Lab, Amnesty International, Access Now, Mexico's Red en Defensa de los Derechos Digitales (R3D) have highlighted the various ways in which spyware has implicated these rights. David Kaye, *Testimony to the PEGA Committee of the European Parliament*, § 3 (27 Oct. 2022), https://perma.cc/JA5B-WK4P.f.
[22] International Covenant on Civil and Political Rights (ICCPR) art. 17(1); European Convention on Human Rights art. 8; American Convention on Human Rights art. 11.
[23] Afr. Comm'n on Hum. & Peoples' Rts., Resolution on the deployment of mass and unlawful targeted communication surveillance and its impact on human rights in Africa - ACHPR/Res.573 (LXXVII) (2023); Ayalew, *supra* note 14.
[24] Frank La Rue, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/HRC/23/40, § 22 (17 April 2013).
[25] ECHR art. 10; ACHPR art. 9; ACHR art. 13.
[26] A/HRC/41/35 *supra* note 7, at § 24.
[27] *Riley v. California*, 573 U.S. 373 (2014).

severe chilling effect that constitutes a restriction of the freedom of expression.[28]

B. State obligations to ensure that spyware is used only in a manner that the associated restrictions on fundamental rights are justified

17. The ECHR, ACHPR, ACHR, and ICCPR share a similar set of robust standards states must meet to justify the lawfulness of any interference with the rights to privacy and freedom of expression (so-called three-part test).[29]
    - *Legality:* The restriction must be prescribed by law, which is precise, public, and accessible.[30] States must implement robust safeguards sufficient to eliminate the risk of abuse of power and the chilling effect on individuals' exercise of rights caused by the state's conduct.[31]
    - *Legitimacy:* The restriction must serve a legitimate purpose, generally, either of (a) respecting the rights or reputations of others, and (b) protecting national security, public order (*ordre public*), or public health or morals.[32] A State must make an objective, specific, and individualized determination about the precise nature of the threat. A mere conclusory claim of national security or public order is never legitimate.[33]
    - *Necessity and proportionality:* The necessity test requires the method used must be the least restrictive, or the only means of achieving a legitimate aim. In the surveillance context, this entails demonstrating that the scope of data collection and use is limited to those "relevant and material [...] to a specific threat to a [l]egitimate [a]im alleged.[34] The proportionality test requires the existence of a benefit that is balanced by the degree of infringement of human rights.[35]
18. Given the extreme intrusiveness of spyware, the three-part test must be applied with particular rigor. Below are several key conditions for states to justify their use of spyware under the three-part test.

1. Legality

19. As the high rates of spyware abuse observed globally demonstrates, its unique capabilities challenge the effectiveness of institutional oversight in many countries. To respond to the gap, there must be robust, tailored safeguards put in place.[36] The intervenors recalled a remark by a former South African judge that she was required to examine warrant applications for the use of FinFisher spyware under the general interception law. While she stated that the "fall-back position" was the Constitution, it suggests the urgent need for an international clear norm that requires tailored safeguards.[37] The

---

[28] Venice Commission Report, *supra* note 7, § 17.
[29] ICCPR art. 19(3); While in its text Article 17 prohibits "arbitrary or unlawful" interference in the right to privacy, the long-standing practice of the Hum. Rgts. Comm., as well as the instruments of the United Nations High Commissioner for Human Rights (OHCHR), supports the interpretation that Article 17 requires any interference with the right to privacy to be (i) prescribed by the law and (iii) necessary and proportionate (ii) to achieve a legitimate aim. *See* OHCHR, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/27/37, §§ 21–23 (30 June 2014); ECHR art. 8; ACHR art. 11.
[30] For the ECHR, *see, e.g., Roman Zakharov v. Russia [GC]*, App. No. 47143/06, § 228 (Dec. 4, 2015). For the ACHPR, *see e.g., In the matter of Lohé Issa Konaté v. The Republic of Burkina Faso*, Application 004/2013, ACtHPR, § 131 (5 Dec. 2014). For the ACHR, *see e.g., CAJAR*, *supra* note 20 § 528. For the ICCPR, *see* Hum. Rgts. Comm., Gen. Comment 34, U.N. Doc. CCPR/C/GC/34, § 25 (July 2011).
[31] For the ECHR, e.g., *Zakharov*, *supra* note 30, § 231. For the ACHR, *e.g., CAJAR*, *supra* note 20, §538. For the ICCPR, *e.g,* Hum. Rgts. Comm., Gen. comment No. 37 (2020) on the right of peaceful assembly (article 21), §§ 62, 94; Madhewoo v. Mauritius, Communication No. 3163/2018, §§ 7.4, 7.6, U.N. Doc. CCPR/C/131/D/3163/2018 (16 Sept. 2023).
[32] *See* ECHR art. 10, 11; ACHR art. 15, 16; ACHPR art. 11.
[33] *See* CCPR/C/GC/34 *supra* note 30, § 35.
[34] The Electronic Frontier Frontier Foundation and Article 19, *Necessary & Proportionate International Principles on the Application of Human Rights Law to Communications Surveillance*, Principle 5, § 1(2014), https://necessaryandproportionate.org/principles/.
[35] *See* CCPR/C/GC/34 *supra* note 30, § 34.
[36] Jane Duncan, *National Security Surveillance in Southern Africa, An Anti-Capitalist Perspective* (2022) at 127 ("As there are particular risks associated with each technology, the most invasive should be regulated more stringently"); Venice Commission Report, *supra* note 7, §14.
[37] Jane Duncan, *Stopping the Spies: Constructing and Resisting the Surveillance State in South Africa*, at 131 (2018).

tailored legislation that specifies the instances in which a state may use spyware (e.g., the nature of the offenses that may give rise to spyware use) is also imperative.[38]

20. On top of those required as "minimum safeguards" in *Zakharov*, below are some examples of possible safeguards; however, given spyware's extreme covertness and therefore high likelihood of abuse, it remains unclear whether it will sufficiently eliminate the risk of abuse, even when states implement all of these safeguards.[39]

a) Robust *ex-ante* authorizations

21. To prevent any illegal spyware use from being wrongfully authorized, the warrant process must exhibit specific features to ensure its effectiveness.[40] For example:
    - an independence of the judge is structurally ensured (i.e., those tasked with supervisory roles in the authorization process should not have roles that give rise to any conflict of interest);[41]
    - a judge's understanding of technical aspects involved in spyware use should be structurally ensured, by, for example, appointing a technical expert with whom a judge can consult;[42]
    - the judge instruct law enforcement to use spyware strictly within the scope of authorization through, for example, designating a set of key words in a warrant to be used to sift protected or non-relevant data;[43] and
    - There should be a mechanism to ensure the verification of the application and evidence put forth in an ex-parte warrant application process. This can be in forms of the appointment of a public advocate authorized to challenge the application and cross-examine the evidence submitted by law enforcement, as suggested by the Council of Europe Commissioner for Human Rights as well as the South African Constitutional Court in *Amabungane*.[44]

b) Professional secrecy protections

22. Global jurisprudence has consistently provided rigorous protections to professional communications, such as those between journalists and their sources and attorneys and their clients. For example:

---

[38] *See Zakharov*, *supra* note 30 § 243-44; *CAJAR*, *supra* note 20,§ 538.

[39] *Zakharov*, *supra* note 30 §§ 231-234.

[40] Additionally, as this Court ruled in previous cases, any warrant granted should be specific in the authorized scope of spyware use. They should identify a person, the kinds and contents of data that can be accessed through spyware use, how to limit the data access to the authorized scope, and the time limits. *See Zakharov*, *supra* note 30, §§ 264-265.

[41] *Zakharov*, *supra* note 30, § 280; *see also Amabungane*, *supra* note 19, §§ 85–94 ("As such, structures, mechanisms and processes that strengthen the independence of an institution or office are imperative even where the incumbent is a Judge.").

[42] When it comes to warrant application for spyware use, if the "judge does not consider the types of technology used when granting interception directions, it is evident that this most invasive form of surveillance [spyware use] is grossly under-regulated." and "the judge should be empowered to consult with a technical expert to assess the application before granting it." Duncan, *supra* note 37, at 153. In the United States Foreign Intelligence Surveillance Court, "technical amici" can be appointed to lend technical expertise. Amici at FISC court are "tasked with presenting legal arguments that advance the protection of privacy and civil liberties or lend expertise and further the Court's understanding of intelligence collection, communications technology, or other relevant areas." The Privacy and C.L. Oversight Bd., *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, at 47 (2023).

[43] *See Zakharov*, *supra* note 30, § 264; *Sorokin and Others v. Russia*, App. no. 73825/13, § 62 (27 June 2024) (finding the search and seizure of computers and hard drives incompatible with art. 10 of ECtHR because the judge did not "instruct the investigative authorities to use any sifting procedure or otherwise ensure that the unrelated personal and professional information [...] was not accessed by authorities").

[44] In 2015, the Council of Europe Commissioner for Human Rights recommended States to consider introducing "security cleared public interest advocates into surveillance authorization processes" to represent the interests of intended subjects of surveillance. Council of Eur. Comm'r for Human Rts., *Democratic and Effective Oversight of National Security Services*, at 12, § 8(2015); *Amabungane*, *supra* note 19 §§ 95–100. This Court also suggested a public advocate system as an idea of the kinds of verification procedures that may be implemented while maintaining the appropriate confidentiality. *Chahal v. United Kingdom*, App. No. 22414/93, § 144 (15 Nov. 1996)*; Saure v. Germany*, Ap. No. 8819/16, § 53 (8 Nov. 2022) (confirming that "measures affecting fundamental human rights must be subject to some form of adversarial proceedings," "even when national security is at stake"). Since its initial adoption, the public advocate system has been expanded in different jurisdictions. *See, e.g.*, Hinako Sugiyama, *In This Era of Spyware, Parliament Must Codify Safeguards in Surveillance Law*, Daily Maverick (2 June 2025), https://perma.cc/XY25-EZCE.

- *Journalistic source*: This Court ruled in *Nagla v. Latvia* (2013) that "the right of journalists not to disclose their sources [...] is part and parcel of the right to information, to be treated with the utmost caution."[45] Further, this Court confirmed, in *Sorokin v. Russia* (2022), the protected information should not be disclosed unless "the interests of investigation in securing evidence were sufficient to override the general public interest in the protection of journalistic sources."[46] The IACtHR similarly ruled that journalistic sources have been considered an "unassailable category of information" in *CAJAR*.[47] The South African Constitutional Court found in *Amabungane* that when the subject of surveillance is a journalist, the interception law must "provide for additional safeguards calculated to minimise the risk of infringement of the confidentiality of [...] journalists' sources."[48]
- *Attorney-client communication*: This Court has required special protection for attorney-client communication.[49] The IACtHR similarly ruled in *CAJAR* that surveillance must "never invade the protected sphere of a lawyer's professional activism to defend clients and his or her communications with them."[50] The South African Constitutional Court clarified in *Amabungane* that the "legal system is reliant on the confidentiality of communications between lawyer and client," which "in turn promotes the rule of law," and thus, similar to journalistic sources, when the surveillance subject is a practising lawyer, the law must put in place additional safeguards."[51]

23. Spyware allows indiscriminate data extraction, so special measures should be taken to ensure professional secrecy. For example:
    - As an entry point, as *Amabungane* requests, judges must be notified whether the targets of spyware use are journalists or lawyers so that they can apply the most stringent review of warrant application.[52]
    - Second, as this Court ruled in *Sorokin*, where the search of a journalist's devices was at issue, and in *Särgava v. Estonia* (2021), where a lawyer's device was at issue, a measure to separate protected information and prevent disclosing it to law enforcement should be implemented.[53] However, it is unclear how commercial spyware can implement such sifting measures in practice.
    - Another example is granting the professional community a monitoring authority of warrant execution and data analysis. In *CAJAR,* the IACtHR noted Brazilian domestic law that grants the Bar Association an authority to monitor both the execution of warrants and the subsequent analysis of data. The Bar Association representative ensures that documents unrelated to the investigation are not accessed or seized and oversees the entire inspection process to safeguard judicial limits and professional secrecy.[54]

c) *Ex-post* independent audit for each use case

24. Judicial pre-authorization alone may not be sufficient to ensure protection against rights violations. Therefore, each use of spyware should be subject to an independent audit.[55] An independent oversight should monitor the entire process of each spyware use—including its pre-authorization, duration, and

[45] *Nagla v. Latvia*, App. No. 73469/10, § 97 (16 Oct. 2013).
[46] *Sorokin supra* note 43, § 61.
[47] *CAJAR supra* note 20 § 242 (Mudrovitsch, J., concurring).
[48] *Amabungane*, *supra* note 19, § 119.
[49] *See, e.g., Saber v. Norway*, App. No. 459/18, § 51 (Dec. 17, 2020).
[50] *CAJAR*, *supra* note 20, § 220.
[51] *Amabungane*, *supra* note 19, §§ 117, 119.
[52] *Id.* § 157, sec. 8.
[53] *Sorokin supra* note 43, § 63; *Särgava v. Estonia*, App. No. 698/19, §§ 98, 99 (16 Nov. 2021) ("While the question of sifting and separating privileged and non-privileged files is undoubtedly important in the context of hard copy material, it becomes even more relevant in a situation where the privileged content is part of larger batches of digitally stored data").
[54] *CAJAR*, *supra* note 20 § 227.
[55] *See Zakharov*, *supra* para 30, §§ 272-285. International human rights bodies have confirmed the need for "rigorous independent oversight" for hacking. *See* OHCHR, *The Right to Privacy in the Digital Age*, § 19, U.N. Doc. A/HRC/51/17, (4 Aug. 2022).

its termination—can conduct independent investigations of alleged abuse of spyware.[56] In this vein, the South African Constitutional Court in *Amabungane* required an "automatic review" system, where an independent judge will review all the interception conducted.[57] The IACtHR in *CAJAR* noted that the use of intelligence activities must be subject to "constant review" to protect against its abuse.[58]

d) Exclusionary rules

25. To disincentivise spyware abuse, states should include language in their legislation that prohibits the admission of evidence obtained via illicit spyware methods. No ECtHR case law exists that explicitly requires state legislatures to include exclusionary evidentiary rules. However, such a requirement is warranted because of the extraordinarily severe restriction of human rights by the abuse of spyware as well as the existence of similar requirements under international law. The IACtHR in *CAJAR* disqualified any evidence gathered through spyware as a "direct, necessary consequence" of the privileges enjoyed by attorney-client communication.[59] Several African states have implemented exclusionary evidence rules within their constitutions.[60]

e) Data integrity

26. International human rights law requires, when the government collects people's data, a mechanism to maintain the data integrity and prevent unauthorized third-party access.[61] The sensitivity of the data to be extracted through spyware use makes these safeguards even more important. However, commercial spyware complicates this requirement, as often the spyware vendors rather than the states control the data.[62] Even if the contract grants the government inspection or audit rights, its control over the security systems remains limited, questioning states' ability to perform the data integrity obligation. Moreover, some spyware has the function to alter or delete the data, conflicting with the data integrity requirement.

2. Legitimacy

27. Human rights bodies and experts have consistently warned that states' self-claimed, vague and "poorly empirically based" legitimate aims, such as "counter-terrorism" or "counter-extremism" have been inviting abuse of surveillance powers.[63] This Court clarified in *Zakharov* that, where the Russian government claimed national security interest as a legitimate aim for secret phone interception

---

[56] David Kaye, *supra* note 21, § 23(a) (2022).
[57] *Amabungane*, *supra* note 19, §§ 49-54.
[58] *CAJAR*, *supra* note 20, § 8.
[59] *CAJAR*, *supra* note, 20 § 230. Human Rights Committee's General Comment No. 20 advises against admitting statements or confessions obtained through torture.
[60] *See*, *e.g.*, *See* Const. of Mozambique (2004), art. 65(3) ("All evidence obtained through the use of torture, coercion, offences against the physical or moral integrity of the person, the abusive intrusion into their private and family life or into their home, correspondence or telecommunications, shall be invalid."); Constitution of Cape Verde (1980), art. 33(6) ("All evidence obtained by torture; coercion; assault on physical or moral integrity; illegal invasion of correspondence, telephone, domicile, or privacy, or other illicit means, shall be null and void."); Const. art. 50(4) (2010) (Kenya) ("Evidence obtained in a manner that violates any right or fundamental freedom in the Bill of Rights shall be excluded if the admission of that evidence would render the trial unfair, or would otherwise be detrimental to the administration of justice."); Const. of Zimbabwe (2013), § 70(3) ("In any criminal trial, evidence that has been obtained in a manner that violates any provision of this chapter must be excluded if the admission of the evidence would render the trial unfair or would otherwise be detrimental to the administration of justice or the public interest.").
[61] *Madhewoo*, *supra* note 31, § 7.6; *Amabhungane*, *supra* note 19, § 107.
[62] *See*, Jonathon Rozen, *Spyware Cases in Europe and Africa Spotlight Privacy and Accountability*, Harv. Kenn. Sch. (Mar. 9, 2026), https://bit.ly/4dVOUZC ("'Under Polish law, IT systems that process classified information[…]must be accredited. The aim is to ensure that users of the system have exclusive control over the information processed there [...]. The prosecutor's office has brought charges against the people who were responsible for verifying the security of Pegasus but failed to do so'").
[63] *See, e.g.*, Fionnuala Ní Aoláin (Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism), *Human Rights Implications of the Development, Use and Transfer of New Technologies in the Context of Counterterrorism and Countering and Preventing Violent Extremism*, U.N. Doc A/HRC/52/39, §§ 13–14 & n.21 (1 March 2023).

system, the aim must be grounded in "factual indications for suspecting that person of planning, committing or having committed criminal acts or *other acts* that may give rise to secret surveillance measures," yet with some broadness.[64] The more intrusive nature of spyware requires a more objective, specific, and compelling ground to justify its use.

3. Necessity and proportionality

28. The covert and indiscriminate access to data, and the resulting harm, sets an extremely high bar for states to demonstrate that their use of spyware is necessary and proportionate, as many bodies have pointed out.[65]
29. *Necessity:* It is unclear how the function of indiscriminate access to data can be reconciled with the requirement of limiting data access to what is relevant and material for the purpose pursued. In the context of digital device searches, this Court has required mechanisms that filter or sift data so that authorities cannot access material non-responsive to the investigative objective, for example in *Sorokin*.[66] However, it remains unclear how commercial spyware can implement such "sifting" measures effectively.[67]
30. *Proportionality:* Even where the necessity test is satisfied, spyware use must be limited to the instances in which the anticipated benefits of surveillance outweigh the resulting restrictions on human rights. Given the profound chilling effect associated with the use of such technology, situations in which spyware use can be justified are likely to be rare.[68] Moreover, the increased cybersecurity risks posed by spyware further complicate its justification, as it exploits vulnerabilities in device or network systems, thereby lowering the security levels and endangering privacy *en masse*.[69]

C. State obligations to ensure that spyware is used only in a manner that complies with the duty to provide an effective remedy

31. The ECHR, ACHPR, ACHR, and ICCPR all impose on states the duty of providing an effective remedy when any right is violated.[70] To discharge the duty, the state must (i) make reparations to individuals whose human rights have been violated by its conduct, (ii) investigate the violations to amend existing laws, policies, and practices to prevent future recurrence, and (iii) hold actors responsible in the judicial system.[71] To perform those duties, while not exhaustive, notification to surveillance subjects and logging of spyware use is particularly important.
32. *Notification:* Legal norms on notification to surveillance subjects, including when and what to notify, already exist as this Court's work as the main source. Regarding "when," the ECtHR consistently rules that the notification should be provided *as soon as* it can be made without jeopardising the purpose of surveillance since *Klass and Others v. Germany* (1978).[72] Regarding "what," The Court

---

[64] *Zakharov*, *supra* note 31, § 260.

[65] Venice Commission Report, *supra* note 7, § 85; *Aoláin, supra* note 63, § 50.

[66] *Sorokin*, *supra* note 43, § 63 (finding the search and seizure of computers and hard drives was incompatible with art. 10 of ECHR as there was no "sifting procedure [...] which could protect the confidentiality of [...] information unrelated to [the alleged crime]).

[67] Venice Commission Report, *supra* note 7, § 85 (concerning spyware, "the screening of authorised and unauthorised (or relevant and irrelevant) information may be difficult as a technical matter.")

[68] Eur. Data Protection Supervisor, *Preliminary Remarks on Modern Spyware* (2022), at 8 (In the context of spyware use, "[t]he essence of the right is affected. Therefore, its use cannot be considered proportionate–irrespective of whether the measure can be deemed necessary."); Venice Commission Report, *supra* note 7, §§ 14–17, 28; A/HRC/51/17, *supra* note 55, §§ 13, 19.

[69] *See, e.g.*, Brief for AccessNow et al. as Amicus Curiae, *WhatsApp v. NSO Group Techs. Ltd.*, No. 20-16408, §§ 6–7 (9th Cir. 23 Dec. 2020) (noting that NSO Group exploited a vulnerability on WhatsApp's servers—a company with over 1.5 billion users—to infiltrate target's devices).

[70] ECHR art. 13; ACHPR art. 7(1)(a); ACHR art. 25(1)–(2) (1969); ICCPR art. 2(3).

[71] *See* Hum. Rgts. Comm., Gen. Comment 31, §§ 16–18, U.N. Doc. CCPR/C/21/Rev.1/Add.13 (26 May 2004). For the ACHPR, *see e.g.,* Abdel Hadi, Ali Radi & Others v. Republic of Sudan, Communication 368/09, Afr. Comm'n H.P.R., § 92 (5 Nov. 2013).

[72] *Klass and Others v. Germany*, § 58, Series A no. 28 (6 September 1978).

clarified in *Ekimdzhiev and Others v. Bulgaria* (2022) that a proper notification may include, "(a) the number of the surveillance application; (b) the requesting authority; (c) the number of the surveillance warrant; (d) the authority which has issued that warrant; and (e) the period during which there has been unlawful surveillance."[73] In the similar vein, in *CAJAR*, the IACtHR affirmed the ability to gain comprehensive knowledge of the information collected on them is protected as part of the right to information self-determination.[74] The African Commission has also expressly required the "notification of the decision authorizing surveillance within a reasonable time of the conclusion of such surveillance."[75] The Constitutional Court of South Africa in *Amabungane* has similarly reasoned that notification within ninety days must be the default.[76]

33. However, the practical implementation of those norms has lagged behind globally. While many countries, including member states of the Council of Europe, have implemented *some* notification systems often with nebulous grounds for exception or infinite delay.[77]
34. The use of spyware makes it imperative to close this gap, as the notification to surveillance is even more critical especially when institutional oversight within the government is not expected to function properly to detect abuse—particularly in the context of spyware, where the technologies outpaced regulatory capacity. In such a situation, an agential approach, meaning the accountability effort of victims and their supporters in civil society are even more important to reclaim the regulation, and a notification is a focal point for such an approach.[78] To that end, while upholding the existing norms, a clearer and stricter rules should applied to the present cases, for example, the delay in notification is illegal unless it must meet the above strict three–part test of legality, legitimacy, and necessity and proportionality, and never justified solely on broad national security grounds.[79]
35. *Logging:* In order for surveillance subjects to confirm whether there is any violation, a comprehensive log of every step taken during the course of spyware use is necessary.[80] However, there is a question on whether states' use of commercial spyware, such as Pegasus, can fulfill this obligation. Spyware of this nature is often designed in a way that leaves no trace of infection and data access,[81] nullifying the right to remedy. A state that procures software architecturally designed to impede accountability cannot guarantee the right to an effective remedy from the use of spyware.

V. Conclusion

36. Therefore, we respectfully recommend that this Court take the present case as an opportunity to chart a path toward robust protections of the rights to privacy and freedom of expression against the abuse of spyware and digital surveillance globally, and therefore to undertake a careful review. Safeguarding these rights is a fundamental prerequisite for the protection of human rights, democracy, and the rule of law.

---

[73] *Ekimdzhiev and Others v. Bulgaria*, App. No. 70078/12, § 130 (11 Jan. 2022). *See also Denysyuk and Others v. Ukraine*, App. No. 22790/19 § 119 (13 Feb. 2025) ("individuals should, in principle, be able to access documents providing sufficient information concerning the factual and legal reasons for ordering the surveillance in order to be able to exercise their right to bring legal proceedings in an effective manner").
[74] *CAJAR*, *supra* note 20, §§ 585, 586.
[75] Afr. Comm'n on Hum. & Peoples' Rts., *supra* note 15, Principle 41(3)(d) (2019).
[76] *AmaBhungane*, *supra* note 19 § 40.
[77] Venice Commission Report, *supra* note 7, §§ 66, 67.
[78] Duncan & Munoriyarwa, *supra* note 17 at 19–22.
[79] Brief for Privacy Int'l et. al. as amicus curiae § 37, Mikolaj Pietrzak v. Poland, App. No. 72038/17, Dominikaychawska-Siniarska ao v. Poland, App. No. 25237/18 (14 Oct. 2020).
[80] *Zakharov*, *supra* note 30, § 272.
[81] Brief for Amnesty Int'l as amicus curiae, § 8, *Krzysztof Brejza v. Poland and 8 Other Applications,* App. No. 27830/23 (26 Feb. 2025).