EUROPEAN COURT OF HUMAN RIGHTS

Application no. 45877/22

AYNUR GANBAROVA AND OTHERS

Applicants

- v -

AZERBAIJAN[1]

Respondent

Application no. 30573/22

JAVADOV AND OTHERS

Applicants

- v -

AZERBAIJAN[2]

Respondent

(1) Access Now
(2) Committee to Protect Journalists (CPJ)
(3) Data Rights
(4) Human Constanta

Interveners

JOINT WRITTEN SUBMISSIONS[3]

21 April 2026

[1] and 24 other applications (see list appended to the Court's Statement of Facts).
[2] and 6 other applications (see list appended to the Court's Statement of Facts).
[3] Pursuant to leave granted by the President of the Third Section under Rule 44 §3 of the Rules of the Court, communicated by letter dated 10 March 2026 from the Section Registrar, M. Blaško.

1. Access Now, the Committee to Protect Journalists ("**CPJ**"), Data Rights, and Human Constanta ("**Interveners**") draw on their extensive experience in the protection and promotion of privacy and freedom of expression to assist the Court in three ways:

(1) By situating this case within the broader context of the use of intrusive spyware to target journalists, activists, and human rights defenders ("**HRDs**"), and the resulting chilling effects on freedom of expression.

(2) By demonstrating that this repression is enabled by direct state action and the failure of existing legal frameworks to prevent, regulate, or remedy spyware abuses.

(3) By setting out the implications of these failures under Articles 8, 10, and 13 of the Convention, including Member States' positive and negative obligations, and the importance of effective remedies in surveillance cases.

I. INVASIVE SURVEILLANCE TECHNOLOGIES RESTRICT AND SILENCE ACTIVISTS, JOURNALISTS, AND HRDS

A. Pegasus and similar spyware technologies constitute a form of highly intrusive and covert surveillance

2. Pegasus, a product of the Israeli cybersurveillance company NSO Group ("**NSO**") is one of the best-known surveillance programs. The spyware, which NSO states is only sold to government intelligence and law-enforcement agencies,[4] can secretly turn an individual's mobile phone into a 24-hour surveillance device, enabling the operator (government agencies using the tool) to remotely access the full contents and functions of the personal device. This includes access to the microphone, camera, any files or photos on the phone, network connections, contact information, message and browsing histories, passwords, email accounts, recordings, and more.[5] Pegasus allows the purchaser to access conversations, including those taking place over encrypted messaging apps, without the user's knowledge.[6]

3. Unlike more traditional spyware programs, Pegasus does not only rely on targets to open a link or download an attachment. Infection often requires no more than a zero-click attack or a network injection, meaning the spyware can take over a phone without the user's knowledge or interaction. Previous methods of protection no longer apply, leaving journalists under a constant threat of surveillance. For example, in 2019 WhatsApp discovered and closed the vulnerability exploited by NSO in which Pegasus operators were able to install the software via a single missed WhatsApp call, after which the call log can be deleted remotely, leaving no trace and no way for the phone's owner to know an intrusion ever occurred.[7]

---

[4] NSO Group, https://www.nsogroup.com/about-us.
[5] Tamar Kaldani and Zeev Prokopets, Pegasus Spyware and its impacts on Human Rights, Council of Europe, Information Society Department DGI (2022), p. 8.
[6] Id., pp. 7-10.
[7] Id., p. 8.

4. Pegasus and similar spyware technologies are a modern-day form of highly intrusive covert surveillance, enabling states to closely monitor individuals, extract and exploit their data, and map their personal and professional connections for years on end, without leaving a trace.

B. The use of Pegasus and similar spyware is widespread and unregulated

5. Since its first detection by the Citizen Lab at the Munk School of Global Affairs at the University of Toronto ("**the Citizen Lab**")[8] Pegasus has been systematically deployed to repress civil society and silence its members around the world.[9] The Citizen Lab exposed Pegasus operators in 45 countries and documented extensive government abuses of the spyware.[10] In 2021, the Pegasus Project investigation revealed that Pegasus spyware was used by governments worldwide to target more than 180 journalists, HRDs, academics, lawyers, diplomats, politicians, and others, between 2016 to 2021.[11] The Project found that, despite NSO claiming that it vets their clients based on human rights track records, it has sold Pegasus to authoritarian regimes.[12] Since then, countless others have been targeted by Pegasus.[13]

6. Pegasus targeting of journalists and HRDs is rarely an end in itself, but is commonly followed by retaliatory measures against those placed under surveillance. Civil society organizations have been documenting Pegasus's role in widespread human rights abuses and severe violations against journalists and activists globally.[14] After infection, activists, journalists, and HRDs, as well as their colleagues and loved ones, face intimidation, harassment, detention, and in some cases, are assassinated.[15] Pegasus is also often used in retaliation for journalists and civil society members exposing crimes and abuses, as well as against their families or legal representatives.[16] One illustration of this pattern is the case of journalist Szabolcs Panyi, targeted by Pegasus in 2019 and recently charged with espionage following his reporting on Russian influence operations ahead of the parliamentary elections.[17]

7. These retaliatory measures are not confined within national borders. The transnational nature of Pegasus means even those activists, journalists, and HRDs who seek safety in exile are at risk. Although NSO does not publicly disclose its client list and maintains that it sells Pegasus exclusively to authorised government

---

[8] Citizen Lab, NSO Group's iPhone Zero-Days Used Against a UAE Human Rights Defender, 2016.
[9] Access Now et al., Amicus Brief in *NSO Group Technologies* v. *WhatsApp Inc. et al.*, 9th Cir., 2020.
[10] Citizen Lab, Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries, 2018.
[11] Amnesty International, Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally, 2021.
[12] Forbidden Stories, About the Pegasus Project, July 2021.
[13] See, e.g., Access Now, Pegasus attacks in El Salvador: spyware used to target journalists and activists, 2022; Access Now, Pegasus spyware in the Azerbaijan-Armenia conflict, 2023.
[14] Amnesty International, Ruling against NSO Group in WhatsApp case, 2025.
[15] See, e.g., Citizen Lab, How Saudi-Linked Digital Espionage Reached Canadian Soil, 2018; The Washington Post, Jamal Khashoggi's wife targeted with spyware before his death, 2021.
[16] See, e.g., Statement of Carine Kanimba, to the U.S. House Intelligence Committee, 2022; Citizen Lab, Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware, 2017.
[17] See CPJ, Hungary files espionage charges against investigative journalist Szabolcs Panyi, 2026.

agencies, the widespread use of this invasive technology, which has been deployed in over 46 countries worldwide increases the risk of misuse and proliferation.[18] Its deployment is far from limited to authoritarian regimes.[19] Evidence is increasingly clear that Pegasus has been repeatedly and extensively used by states, both authoritarian and democratic, around the world to suppress human rights activists, silence journalists, and stifle criticism of governments.[20] These practices have also been documented in several Council of Europe Member States.[21]

8. By way of example, in the past two years, Access Now and the Citizen Lab identified ***at least eight EU-based*** journalists and activists who have been targeted with Pegasus, most of whom were living in exile in the EU. All of the victims were prompted to reach out for help because they received threat notifications from Apple alerting them that their devices may have been targeted with mercenary spyware.[22] Some of the notifications arrived years after the actual Pegasus targeting took place. The victims are:

a. ***Galina Timchenko***, co-founder and CEO of prominent Russian independent media Meduza living in exile in Latvia. Access Now and the Citizen Lab discovered that her iPhone was infected with Pegasus spyware around 10 February 2023. At the time of the infection, Timchenko was in Berlin attending a private event for exiled Russian independent media.[23]

b. ***Evgeny Erlikh***, an Israeli-Russian journalist, ***Evgeny Pavlov***, a Latvian journalist, and ***Maria Epifanova***, general director of an independent media Novaya Gazeta Europe. Access Now and the Citizen Lab found that all three had their devices infected with, or at least targeted by, Pegasus. Epifanova's phone was infected around 18 August 2020, soon after she was accredited to attend exiled Belarusian opposition leader Svetlana Tikhanovskaya's first press conference in Vilnius.[24]

c. An anonymous ***Russian journalist*** living in exile in Lithuania since Russia's invasion of Ukraine. Access Now and the Citizen Lab identified an attempt to infect their device around 15 June 2023, one day before the journalist had attended an event in Latvia for Russian journalists in exile.[25]

d. An anonymous ***Belarusian civil society member*** also living in exile in Lithuania. The Citizen Lab's analysis of their device confirmed that it was infected with Pegasus around 25 March 2021, which marks the Belarusian "Freedom Day," historically suppressed by the Belarusian authorities.[26]

---

[18] Access Now, Is the EU protecting people from Pegasus spyware?, 2023; UK Foreign, Commonwealth and Development Office, The Pall Mall Process declaration, 2025.
[19] Id.
[20] Access Now, Media, Civil society demand ban on tech used for human rights abuses, 2023.
[21] Council of Europe, Pegasus and similar spyware and secret state surveillance, 2023.
[22] Apple, About Apple threat notifications and protecting against mercenary spyware, 2025.
[23] Access Now, Pegasus spyware used to target Putin's critic, 2023.
[24] Access Now, Civil society in Latvia, Lithuania, and Poland targeted with Pegasus spyware, 2024.
[25] Id.
[26] Id.

e. ***Natallia Radzina***, the editor-in-chief of an independent Belarusian media website, based in Poland. Because of her journalistic activities in Belarus, she was imprisoned and forced to leave the country. Access Now and the Citizen Lab found that her device was infected by Pegasus three times, with the first infection taking place just a day after Radzina attended Free Russia Forum's Third Anti-War Conference in Vilnius.[27]

f. ***Andrei Sannikov***, a prominent Belarusian opposition politician and activist living in exile in Poland. The Citizen Lab found that Sannikov's iPhone was infected with Pegasus around 7 September 2021. Sannikov ran for president in 2010 and was later arrested and jailed by the Belarusian KGB.[28]

9. Access Now and the Citizen Lab concluded that a single government operator was likely responsible for the targeting of at least three, and possibly all, of the above victims.[29] They were unable, however, to identify the perpetrators. Because NSO does not publish its customer list and governments do not disclose their use of Pegasus, it is exceedingly difficult for civil society with limited resources to definitively prove who is behind these attacks.

10. In the absence of effective regulation or transparency, mercenary spyware has become widely accessible to governments, with few safeguards governing its transfer or use. This environment has fuelled a global spyware boom, with the rapid proliferation of spyware tools across regions. Tools such as Graphite,[30] Hermit,[31] Predator,[32] and Reign,[33] among others, continue to spread without meaningful oversight or accountability, and are repeatedly deployed to repress political opposition, intimidate civil society, and undermine democratic freedoms.

C. Pegasus and similar spyware create a pervasive chilling effect

11. Secret surveillance, even the threat of it, has a chilling effect that extends far beyond individual journalists, activists, and HRDs, reaching their sources, networks, and communities and placing global press freedom at risk.[34] Scholars have documented the behavioural impact of the fear of being surveilled, finding the "chilling and conforming effects of commercial and state surveillance threaten democratic deliberation, self-government, and collective action."[35]

12. For journalists – who are frequent targets of Pegasus[36] – this surveillance

[27] Id.
[28] Id.
[29] Id.
[30] Citizen Lab, Graphite Caught, 2025.
[31] Lookout, Lookout Uncovers Hermit Spyware Deployed in Kazakhstan, 2022.
[32] Council of Europe, Journalist Thanasis Koukakis Targeted With Spyware Predator, 2026.
[33] Citizen Lab, A First Look at Spyware Vendor QuaDream's Exploits, Victims, and Customers, 2023.
[34] See Jonathan W. Penney, Understanding Chilling Effects, 106 Minnesota Law Review 1452, p. 1497 (2022) ("Chilling effects stem from uncertainty and ambiguity—[such as] when a person is . . . faced with ambiguity or uncertainty about the scope, nature, and possibility of surveillance.").
[35] Id., p. 1516.
[36] CPJ, Pegasus spyware targeted exiled journalists from Russia, Latvia, Belarus, 2024.

creates a pervasive climate of fear.[37] Many fear contacting their sources out of concern that doing so could endanger them, while sources themselves grow increasingly afraid to engage. The resulting chilling effect significantly restricts the free flow of information. The mere threat of being targeted, particularly with such intrusive spyware, affects people's communication patterns, pushing them toward self-censorship.[38] Even when journalists take extra precautions, the covert nature of the spyware means that surveillance can occur at any time without their knowledge, creating "profound feelings of powerlessness."[39] Spyware tools are also rarely applied in an isolated manner but rather combined with other forms of online and offline intimidation and censorship.[40] The lack of meaningful accountability further intensifies this sense of powerlessness: not only is it extremely difficult to detect the presence of spyware, but it is even more challenging to determine who is responsible for its deployment.

13. Despite the persistent and extensive use of this spyware, little action has been taken to prevent future abuses. Instead, the growing commodification of digital surveillance allows governments to easily access sophisticated monitoring tools off-the-shelf without needing to build their own capabilities.[41] This dramatically lowers barriers to entry and blurs accountability, as the private surveillance industry operates in the shadows and is subject to little, if any, oversight.[42]

14. The examples discussed above demonstrate the severe vulnerability of journalists, activists, and HRDs, including those who sought safety in exile, to highly targeted spyware attacks, and the near-impossibility of identifying the perpetrators. The proliferation of surveillance technologies like Pegasus in the region, absent any meaningful regulation or oversight, all but guarantees further abuses.

II. THE CURRENT EUROPEAN LEGISLATIVE AND POLICY FRAMEWORKS FAIL TO PROVIDE ADEQUATE PROTECTION

15. Current frameworks by parties to the Convention aimed at preventing, deterring, and remedying spyware abuses are insufficient for two reasons. First, national security and public interest exceptions create significant protection gaps, and second, there is little to no implementation and enforcement of the policies.

16. As a result, there remains very little transparency regarding how Member States use or export Pegasus, and limited judicial or other independent oversight. Those targeted are unaware of the attacks, often for years, unless, as with the

[37] See Penney, *supra* note 34, p. 1506 ("surveillance . . . has been found to activate . . . emotional distress, anger, and anxiety"); see also *id.* at p. 1508 ("Observation alone has chilling and conforming effects, which . . . are amplified and compounded by the ambiguity and uncertainty of modern surveillance practices.").
[38] CPJ, When spyware turns phones into weapons, 2022; Human Rights Watch, The Deterioration of Media Freedom in Greece, 2025; *see also* Penney, *supra* 34 note, pp. 1524-1525 (finding that surveillance increases chilling effects); Citizen Lab, Digital Transnational Repression in Canada, 2022.
[39] CPJ, *supra* note 38.
[40] Human Constanta, Repression Without Borders, 2025, pp. 16-20.
[41] Id., pp. 28-29.
[42] Amnesty International, Inside NSO Group's Corporate Structure, 2021.

journalists and activists identified above, they receive an Apple threat notification or assistance from NGOs specialising in digital security. Even when individuals do become aware, the absence of disclosure and regulatory safeguards makes it incredibly difficult to attribute the attacks to a particular State, as governments deploy and export Pegasus in secrecy. Consequently, victims of Pegasus attacks have no avenues for redress before national authorities, in violation of their right to effective remedy under the Convention.[43]

A. The Convention imposes strict safeguards on secret surveillance

17. The right to privacy being fundamental, and applying online and in digital spaces as it does offline, this Court has held that secret surveillance can only be justified under Article 8 if it is in accordance with the law, pursues a legitimate aim, and is necessary in a democratic society.[44] Surveillance measures must be accessible, foreseeable, and sufficiently clear to protect against arbitrariness.[45] The Court also has emphasised the importance of effective safeguards, including independent and impartial oversight of surveillance mechanisms,[46] and effective ex post remedies.[47] The following subsections set out why existing frameworks by parties to the Convention are often inadequate and fail to fulfil the level of protection required under the Convention.

B. Existing EU frameworks fail to meet Convention safeguards

18. ***PEGA Committee.*** In 2022, the European Parliament established the PEGA Committee in response to the Pegasus Project investigations to investigate the use of Pegasus and equivalent surveillance spyware by Member States.[48]

19. The Committee identified evidence of abuse and serious deficiencies in Member States' governance frameworks.[49] In response to these findings, the Committee made several recommendations aimed at ensuring the protection of EU citizens.[50] These recommendations centred around restoring and strengthening institutional and legal safeguards, including independent oversight, enabling authorities to investigate allegations of the use of the spyware, and increasing transparency. In light of its concern of the misuse of national security justifications to shield spyware deployment from scrutiny, the Committee also recommended a common legal definition for the term national security and avoiding the use of national security as an "unlimited carve out" from the application of EU laws.[51]

20. The Committee also highlighted that the harm caused by spyware extends beyond internal use, as Member States including Cyprus and Bulgaria have become

[43] See *infra* paras. 33-35.
[44] *Zakharov v. Russia*, App. No. 47143/06, §227.
[45] *Zakharov v. Russia*, App. No. 47143/06, §§228, 229.
[46] *Big Brother Watch v. The United Kingdom*, App. Nos. 58170/13, 62322/14 and 24960/15, §456.
[47] *Pietrzak et Bychawska-Siniarska v. Poland*, App. Nos. 72038/17 and 25237/18 §§241-245.
[48] Decision (EU) 2022/480 of the European Parliament of 10 March 2022.
[49] European Parliament, MEPs sound alarm on threat to democracy and demand reforms, 2023.
[50] See European Parliament Recommendation of 15 June 2023 (2023/2500(RSP)) (C/2024/494), §32.
[51] Id., §42.

export hubs for spyware to repressive regimes around the world, enabling countries outside the EU to develop surveillance capabilities.[52] The Committee therefore argued that the trade in and use of spyware must be regulated strictly.

21. Nevertheless, implementation of the Committee's recommendations has been inconsistent or absent, with implicated Member States taking little or no action.[53]

22. ***The European Media Freedom Act ("EMFA")***, adopted in April 2024, includes several safeguards aligned with PEGA recommendations, including mandatory prior judicial authorisation for State surveillance of journalists, notification duties when targeting journalists, and oversight mechanisms.[54] The Act seeks to safeguard the media's essential role of supporting democracy by, among other goals, preventing spyware from being used against journalists.

23. The Act explicitly prohibits Member States from using intrusive surveillance software, such as Pegasus spyware, on journalists and their sources.[55] When spyware must be used, the Act provides for fundamental safeguards.

24. However, the persistence of broad national security and public interest exceptions under EMFA create significant protection gaps. The Act also does not require prior judicial authorisation in "exceptional and urgent cases."[56] These gaps may lead to abuses by States, including those driven by ulterior motives to suppress freedom of expression, in violation of Article 18 of the Convention.

25. Finally, implementation of the Act remains deficient.[57] Some Member States, such as Finland, consider that their existing legislation is sufficient.[58] Others, including Hungary and Italy, have taken no action despite cases of secret surveillance within their boundaries.[59] The Commission has also so far failed to undertake any enforcement measures, including with respect to Article 4.[60]

26. ***Dual-Use Regulation.*** One of the PEGA Committee recommendations included repealing all export licenses that are not fully in line with the Dual-Use Regulation (2021/821), which is the main binding EU framework governing the export of spyware. The Regulation requires formal authorization for the export of cyber‑surveillance items, either categorically (Article 4) or on a catch‑all basis where the exporter has been informed of a risk of internal repression, or serious human rights or international humanitarian law violations (Article 5).[61]

---

[52] Id., §§25, 27.
[53] The Left, The Left Demands Urgent Action Against Mass Surveillance, 2025.
[54] European Commission, European Media Freedom Act.
[55] EMFA, Recital 25.
[56] EMFA, art. 4(4) & 4(5); see also Recital 26.
[57] Reports Without Borders, EU: Without political will to enforce it, the EMFA risks becoming a dead letter, 2025.
[58] Centre for Media Pluralism and Media Freedom, Implementation of the Media Freedom Act, 2025.
[59] Id.
[60] Reports Without Borders, *supra* note 57.
[61] Regulation (EU) 2021/821 of the European Parliament and of the Council, 2021, arts. 4 and 5.

27. However, the Regulation is not equipped to address distinct challenges raised by the spyware trade, including lack of transparency, weak due diligence obligations, absence of systematic end-use monitoring, and internal market asymmetries.[62]

C. Non-EU parties similarly fail to afford required protections

28. Frameworks by non-EU parties likewise fail to provide effective safeguards against spyware abuse, often lacking meaningful protections or relying on broad national security or public safety exceptions. For example, ***Azerbaijan*** expanded surveillance powers through a centralized platform without independent oversight or remedies.[63] ***Serbia*** permits covert surveillance with ineffective oversight mechanisms.[64] ***Montenegro*** applies safeguards selectively, despite formal judicial authorization requirements.[65]

III. INVASIVE SPYWARE TECHNOLOGIES THREATEN THE RIGHTS TO PRIVACY AND FREEDOM OF EXPRESSION

A. Spyware undermines the rights to privacy and freedom of expression

29. Articles 8 and 10 of the Convention impose ***negative obligations*** on States not to interfere with individuals' rights to privacy and freedom of expression, respectively. Any interference must be lawful, necessary and proportionate, and national security and public safety exceptions must be applied with restraint and interpreted restrictively.[66]

30. The threshold for justifying such interference under both Articles 8 and 10 is especially high where measures are directed against journalists, given their role as public "watchdogs."[67] The Court has repeatedly affirmed the special importance of safeguards afforded to the press.[68] It has, for example, found searches of journalists' professional and private premises disproportionate under Article 8, even where certain procedural safeguards were in place;[69] held that limitations on the confidentiality of journalistic sources require the most careful scrutiny under Article 10;[70] concluded that surveillance of a journalist without prior authorization by an independent body violated both Articles 8 and 10.[71] Even in cases involving journalists' disclosure of national security information, the Court has held that the measures adopted by the state interfered with rights protected under Article 10.[72]

---

[62] See Access Now, New EU dual use export control rules finally adopted, but leave a lot of room for improvement, 2021; CDT, From Export Control to Unknown Exports, 2025.
[63] Human Rights Watch, Azerbaijan's Surveillance Platform Risks Sweeping Privacy Violations, 2025.
[64] Amnesty International, Surveillance and the suppression of civil society in Serbia, 2024, pp. 57-59.
[65] BIRN, Montenegro Struggles with Democratic Oversight of State Surveillance, 2025.
[66] *Klass v. Germany*, App. No. 5029/71, §50; *Rotaru v. Romania*, 28341/95, §47.
[67] See, e.g., *Szabadságjogokért v. Hungary*, App. No. 37374/05, §26.
[68] *Goodwin v. The United Kingdom*, App. No. 17488/90, §39; see also *Weber and Saravia v. Germany*, App. No. 54934/00, §149; *Tillack v. Belgium*, App. No. 20477/05, §53.
[69] *Ernst v. Belgium*, App. No. 33400/96, §§115-117.
[70] *Goodwin v. The United Kingdom*, App. No. 17488/90, §§39-40.
[71] *Telegraaf Media Nederland Landelijke Media v. the Netherlands*, App. No. 39315/06, §§97-102.
[72] See, e.g., *Gîrleanu v. Romania*, App. No. 50376/09, §§71-72.

31. Moreover, Articles 8 and 10 of the Convention impose ***positive obligations*** on States to protect journalists, activists, and HRDs.[73] For example, the Court has found that Article 10 requires States to investigate unlawful acts of violence against a newspaper and its staff,[74] and to create an environment conducive to freedom of expression.[75] It has also found that Article 8 requires States to establish safeguards against secret surveillance by private parties,[76] and to conduct effective investigations into alleged crimes.[77] Given the harassment, intimidation, and human rights abuses associated with the use of spyware technologies, these obligations must encompass investigative scrutiny of such technologies.

32. International human rights law likewise imposes positive obligations on states to protect and promote privacy and freedom of expression, even against intrusive spyware technologies.[78]

B. Targets of spyware have no effective right to remedy

33. Where states have easy access to spyware technologies and a secretive industry frustrates attribution and accountability, spyware victims have limited avenues for redress, contrary to their right to effective remedy under Article 13.

34. This Court has held that breaches of Articles 8 and 10 require proof "beyond a reasonable doubt."[79] It is extremely difficult, if not impossible, for targets of spyware attacks to meet the required burden of proof to pursue domestic or other remedies, for several reasons, including:

a. Absence of notification: Victims of spyware typically learn they were targeted only years later, and usually through device notifications or independent organisations rather than State authorities.

b. Lack of domestic administrative systems to verify infection: Most Member States provide no procedures enabling individuals to verify whether they have been subjected to surveillance. Victims are therefore entirely dependent on NGOs or research institutions specialized in digital-security to detect infections, an approach that is often discredited by governments and spyware companies as insufficient to guarantee conclusive results.

c. Difficult to prove culpability: Spyware vendors' client lists are secret, and States have no obligation to disclose their spyware use. Consequently, attribution is extraordinarily difficult and often impossible, leaving victims unable to identify the responsible state actor.

---

[73] It is well established that the effective exercise of rights protected by the Convention may also require positive State measures. See, e.g., *Tierfabriken v. Switzerland*, App. No. 32772/02, §79.
[74] *Gündem v. Turkey*, App. No. 23144/93, §§41-46.
[75] *Dink v. Turkey*, App. Nos. 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09, §106.
[76] *Kopke v. Germany*, App. No. 420/07.
[77] See, e.g., *Assenov v. Bulgaria*, App. No. 24760/94, §117.
[78] OHCHR, Expansion of Digital Surveillance and Impacts on Journalists and Human Rights Defenders, 2024; General comment No. 24: Article 19: Freedoms of opinion and expression, §23.
[79] See, e.g., *Ismayilova v. Azerbaijan*, App. Nos. 65286/13 and 57270/14, §111.

d. Issues of admissibility of evidence: Courts often reject independent forensic analyses in favour of state assessments,[80] leaving victims without admissible evidence in the absence of meaningful domestic investigations.

35. Owing to the nature of the spyware industry and the structural obstacles described above, victims of spyware infections are effectively unable to prove violations of their rights under Articles 8 and 10 and are consequently deprived of an effective remedy, in breach of Article 13 of the Convention.[81]

C. States must bear the burden of proof in secret surveillance cases

36. Given the opacity surrounding states' use of spyware, once victims provide minimum feasible evidence of targeting, the burden must shift to states to justify their actions.[82] This Court has held that the covert nature of surveillance makes it inherently difficult for individuals to prove they were targeted, and therefore, when applicants provide *prima facie* evidence, the burden shifts to the government.[83]

37. The need to ease, and where appropriate, shift, the burden of proof onto states is particularly important where journalists are the alleged victims of surveillance, given the heightened level of protection they enjoy under the Convention.[84] Journalists cannot reasonably be expected to furnish conclusive proof of covert, state-operated surveillance technologies. Accordingly, they must benefit from an eased evidentiary burden, including the drawing of adverse inferences where the state controls the relevant information. It is therefore for the state to bear the burden of demonstrating that any interference with Article 8 rights was lawful, necessary, and proportionate.

38. Where states fail to respect and protect journalists' freedom of expression and privacy, it creates a chilling effect which, as this Court has emphasized, "works to the detriment of society as a whole."[85]

Natalia Krapiva, Senior Tech-Legal Counsel, Access Now, on behalf of the Interveners

[80] However, in a few cases, courts have successfully accepted testimonies by researchers from the Citizen Lab, see, e.g., Article 19, Mexico: Investigations into the use of Pegasus spyware must continue, 2024; Citizen Lab, Saudi Arabia Ordered to Pay £3m to London Dissident Over Pegasus Spying, 2026.
[81] See *supra* §§8-10.
[82] *Salman v. Turkey*, App. No. 21986/93, §100; *Varnava v. Turkey*, App. No. 16064/90, §184.
[83] *Potoczká and Adamčo v. Slovakia*, App. No. 7286/16, §§49-51.
[84] See, e.g., *supra* note 67; *Tromsø and Stensaas v. Norway*, App. No. 21980/93, §64.
[85] *Kaperzyski v. Poland*, App. No. 43206/07, §70.