

POL 30/1563/2026

15 October 2026

Amnesty International Submission to the Open Public Consultation and Call for Evidence - Overall Evaluation of Regulation (EU) 2021/821

Introduction: The Continuing Crisis of Surveillance and Exports

Amnesty International welcomes the European Commission's Public Consultation on the Evaluation of the Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast) (hereafter "Dual Use Regulation"). The 2021 Recast provides notable improvements, such as the inclusion of human rights criteria for the export of cyber-surveillance tools, a catch-all clause, and transparency and reporting requirements. These advances must be safeguarded. However, it is clear that weaknesses in the Regulation and its implementation have failed to stop the export of rights-violating surveillance technologies contributing to human rights abuses in third countries. The Commission and Member States must act with urgency to address these shortcomings.

Amnesty International and others have long urged that the European Union must do more to stem the flow of dangerous surveillance exports.¹ At the time the Recast was adopted, civil society actors warned that it represented a "missed opportunity" and highlighted the need for a maximalist approach to its interpretation and implementation guidance in light of numerous surveillance scandals involving EU surveillance exports that had taken place during the lawmaking process.²

¹ Joshua Franco, Amnesty International, "Surveillance Exports: Time for the EU to Put its Money Where its Mouth is," <https://medium.com/amnesty-insights/surveillance-exports-time-for-the-eu-to-put-its-money-where-its-mouth-is-10b6cd3e4014> May 11, 2017 (accessed 14 October 2026); Amnesty International, "EU companies selling surveillance tools to China's human rights abusers" 21 September 2020 <https://www.amnesty.org/en/latest/press-release/2020/09/eu-surveillance-sales-china-human-rights-abusers/> (accessed 14 October 2026).

² Amnesty International, "New EU Dual Use Regulation agreement 'a missed opportunity' to stop exports of surveillance tools to repressive regimes," 25 March 2021, <https://www.amnesty.org/en/latest/news/2021/03/new-eu-dual-use-regulation-agreement-a-missed-opportunity-to-stop-exports-of-surveillance-tools-to-repressive-regimes/> (accessed 14 October 2026)

Indeed, a few months before the Recast came into force, a further dire warning came in the form of the Pegasus Project, which showed how NSO's Pegasus software was used around the globe to spy on journalists, activists, and high-level political officials alike.³ The full extent of this scandal is still coming to light.⁴ The PEGA Committee of the European Parliament was established to investigate, and highlighted how failures of EU export regulation contributed to the scandal.⁵

However, the Committee's recommendations have for the most part not been acted upon. Meanwhile, the surveillance crisis continues. In 2023, the "Predator Files" investigation by European Investigative Collaborations and Amnesty International revealed showed surveillance products of the Intellexa Alliance – which advertised itself as an "EU-based and regulated company" – had been found in at least 25 countries across Europe, Asia, the Middle East and Africa and had been used to undermine human rights, press freedom, and social movements across the globe.⁶

In 2026, it is beyond dispute that the global surveillance industry is out of control. With inadequate transparency regarding the surveillance industry⁷ or its exports, it has largely fallen to civil society and independent investigators to unearth how this technology has been sold and used to undermine rights. Cases of the abuse of Pegasus and Predator spyware against journalists and others have continued to be uncovered from Angola⁸ to the Dominican Republic⁹ to Morocco.¹⁰ In Serbia, journalists were found to face threats not only from NSO spyware, but from abuse of digital forensic tools, which were used to extract data from the devices of environmental protestors, and in other

³ Amnesty International, "Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally," 19 July 2021, <https://www.amnesty.org/en/latest/news/2021/07/the-pegasus-project-2/> (accessed 14 October 2026)

⁴ Amnesty International, "Morocco: 'We start with the verdict': Inside Morocco's surveillance machine," MDE 29/1447/2026, 1 October 2026, <https://www.amnesty.org/en/documents/mde29/1447/2026/en/> (accessed 14 October 2026)

⁵ European Parliament 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)), 15 June 2023, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.html (accessed 14 October 2026)

⁶ Amnesty International, "Global: 'Predator Files' investigation reveals catastrophic failure to regulate surveillance trade," 5 October 2023, <https://securitylab.amnesty.org/latest/2023/10/global-predator-files-investigation-reveals-catastrophic-failure-to-regulate-surveillance-trade/> (accessed 14 October 2026)

⁷ Amnesty International, "Uncovering the Iceberg: The Digital Surveillance Crisis Wrought by States and the Private Sector," DOC 10/4491/2021, 23 July 2021, <https://www.amnesty.org/en/documents/doc10/4491/2021/en/> (accessed 14 October 2026)

⁸ Amnesty International, "Angola: Prominent journalist hacked with Predator spyware," 18 February 2026, <https://www.amnesty.org/en/latest/news/2026/02/angola-spyware/> (accessed 14 October 2026)

⁹ Amnesty International, "Dominican Republic: Pegasus spyware discovered on prominent journalist's phone," 2 May 2023, <https://securitylab.amnesty.org/latest/2023/05/dominican-republic-pegasus-spyware-journalists-phone/> (accessed 14 October 2026)

¹⁰ Amnesty International, "Morocco: 'We start with the verdict': Inside Morocco's surveillance machine," MDE 29/1447/2026, 1 October 2026, <https://www.amnesty.org/en/documents/mde29/1447/2026/en/> (accessed 14 October 2026)

cases used to secretly install other spyware on the devices of a student activist and a journalist.¹¹ Journalists continue to be targeted with spyware within the EU as well.¹²

Beyond these tools, types of surveillance technologies not listed in Annex I have continued to spread, with devastating impacts on human rights. The spread of Facial Recognition Technology (FRT) is of particular concern. From the occupied West Bank,¹³ to New York City,¹⁴ Hyderabad¹⁵ and Buenos Aires,¹⁶ Amnesty International has documented how this technology, often developed by EU-based companies or using EU made components, has been used to eviscerate privacy, reinforce discrimination, undermine the right to protest, shrink civic space and even help entrench and maintain the system of Apartheid against Palestinian people.

In the United States, a combination of AI-powered tools have enabled constant mass monitoring, surveillance, and assessments of people, often for the purpose deliberately targeting non-US citizens who speak out for Palestinian rights, amid the country's ongoing unlawful clampdown on migrants, refugees and asylum seekers.¹⁷

Against this backdrop, it has become increasingly clear that many types of surveillance technology, notably FRT, other biometric surveillance tools, highly-invasive spyware, and risk profiling systems by public authorities in law enforcement, social security and migration¹⁸ pose inherent risks to human rights, and that their use – and therefore export – must be banned.

It is past time for the EU to take meaningful action to stop this. The Commission and Member States must act urgently to ensure that *Dual-Use Regulation can put a meaningful check on dangerous*

¹¹ Amnesty International, "Serbia: "A Digital Prison": Surveillance and the suppression of civil society in Serbia," EUR 70/8813/2024, 16 December 2024, <https://www.amnesty.org/en/documents/eur70/8813/2024/en/> (accessed 14 October 2026)

¹² Amnesty International, "Italy: New case of journalist targeted with Graphite spyware confirms widespread use of unlawful surveillance," 13 June 2025, <https://securitylab.amnesty.org/latest/2025/06/italy-new-case-of-journalist-targeted-with-graphite-spyware-confirms-widespread-use-of-unlawful-surveillance/> (accessed 14 October 2026)

¹³ Amnesty International, "Israel and Occupied Palestinian Territories: Automated Apartheid: How facial recognition fragments, segregates and controls Palestinians in the OPT," MDE 15/6701/2023, 2 May 2023, <https://www.amnesty.org/en/documents/mde15/6701/2023/en/> (accessed 14 October 2026)

¹⁴ Amnesty International, "Inside the NYPD's Surveillance Machine," <https://banthescan.amnesty.org/index.html> (accessed 14 October 2026)

¹⁵ Amnesty International, "Ban The Scan Hyderabad," <https://banthescan.amnesty.org/hyderabad/> (accessed 14 October 2026)

¹⁶ Amnesty International, "Argentina: Unchecked deployment of AI-driven surveillance reinforces a techno-authoritarian infrastructure of social control," 19 August 2026, <https://www.amnesty.org/en/latest/news/2026/08/argentina-unchecked-deployment-of-ai-driven-surveillance-reinforces-a-techno-authoritarian-infrastructure-of-social-control/> (accessed 14 October 2026)

¹⁷ Amnesty International, "USA/Global: Tech made by Palantir and Babel Street pose surveillance threats to pro-Palestine student protestors & migrants," 21 August 2025, <https://www.amnesty.org/en/latest/news/2025/08/usa-global-tech-made-by-palantir-and-babel-street-pose-surveillance-threats-to-pro-palestine-student-protestors-migrants/> (accessed 14 October 2026)

¹⁸ Amnesty International, "Global: Risk profiling systems used to identify potential offenders are in breach of international law and must be banned – new report," 10 June 2026, <https://www.amnesty.org/en/latest/news/2026/06/risk-profiling-systems/> (accessed 14 October 2026)

surveillance exports. This will require ensuring that more technologies are subject to export authorization processes, that transparency is improved, that export authorisations are scrutinized for risks they pose to full range of human rights, and that due diligence is made meaningful and mandatory, as well as subject to oversight and transparency requirements.

Need to Include More Technologies

It is clear that the human rights crisis from the export and use of surveillance tech extends beyond the technologies listed in Annex I of the Regulation. In this regard, it is positive that the 2024 Commission guidelines on the catch-all clause explicitly mention “Facial and emotion recognition technology” (2.2.1.), and “location tracking devices” (2.2.2.), as “Potential non-listed cyber-surveillance items” (2.2.).¹⁹ However, the guidelines also clarify that video surveillance systems are not considered cyber-surveillance items, which seems at odds with the guidelines’ later advice that exporters should consider whether a product “could be used as a part or component” of a system leading to violations, given that video surveillance systems form part of facial recognition systems.²⁰

This highlights a problem in the definition of cyber-surveillance items, especially when interpreted narrowly. Further guidelines should reflect the evolution of the market for surveillance technologies, including the many components of surveillance tools that – viewed in isolation – may fall short of Art. 2(20)’s requirement that they be “specially designed to enable the covert surveillance”, such as when provided as cloud-based or software as a service models.²¹

Similarly, the guidelines also do not incorporate other AI-based technologies, which can be used for surveillance and human rights violations, such as risk profiling technologies used by law enforcement, migration and other authorities. In any event, it is clear that the list of potentially rights-harming technologies extends beyond those named in the guidelines. The Commission and Member States should ensure that these technologies are subject to export authorization, and where necessary banned from export.

This need is demonstrated by the AI Act, which the EU adopted in 2024 to regulate the development and use of AI technologies²². The AI Act imposes bans (Article 5 - Prohibited AI practices) or otherwise restricts the use of numerous dangerous AI technologies that pose risks to human rights,

¹⁹ European Commission, "Commission Recommendation (EU) 2024/2659 on Guidelines on the Export of Cyber-Surveillance Items under Article 5 of Regulation (EU) 2021/821 of the European Parliament and of the Council," October 11, 2024, https://eurlex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402659

²⁰ See note 13.

²¹ Kolja Brockmann and Lauriane Héau, Stockholm International Peace Research Institute (SIPRI), “Spyware as a service: Challenges in applying export controls to cloud-based cyber-surveillance software,” 17 February 2025, <https://www.sipri.org/commentary/topical-background/2025/spyware-service-challenges-applying-export-controls-cloud-based-cyber-surveillance-software> (accessed 14 October 2026)

²² Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance), <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>

including through cyber surveillance within the EU, but perversely allows for those same technologies to be exported to third countries. While the European Commission's impact assessment accompanying the proposal for the AI Act noted that 'dual use' products and technologies which have AI features and can be used for both military and civil purposes, would fall into the scope of the AI Act,²³ this was not reflected in the actual text of the proposal.²⁴

Amnesty, among civil society partners, campaigned for regulating the export of AI technologies from the EU²⁵, which would also align with EU's aims to "shape global norms and standards and promote trustworthy AI that is consistent with Union values and interests."²⁶ In view of this, a proposal by Members of the European Parliament sought to include "providers placing on the market or putting into service AI systems referred to in Article 5 outside the Union where the provider or distributor of such systems is located within the Union"²⁷ within the scope of the AI Act, arguing that "In order for the Union to be true to its fundamental values, AI systems intended to be used for practices that are considered unacceptable by this Regulation, should equally be deemed to be unacceptable outside the Union because of their particularly harmful effect to fundamental rights as enshrined in the Charter. Therefore, it is appropriate to prohibit the export of such AI systems to third countries by providers residing in the Union."²⁸

However, these proposals were rejected. Similarly, the EU's Corporate Sustainability and Due Diligence Directive (CSDDD) excludes downstream activities from the scope of due diligence requirements where exports are covered by the Dual-use Regulation.²⁹ Accordingly, the Regulation should be used to close this gap.

²³ Commission Staff Working Document Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts, SWD/2021/84 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021SC0084>

²⁴ Proposal For a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>

²⁵ Amnesty International, "Lawmakers reluctant to stop EU companies profiting from surveillance and abuse through the AI Act," 5 December 2023, <https://www.amnesty.eu/news/lawmakers-reluctant-to-stop-eu-companies-profiting-from-surveillance-and-abuse-through-the-ai-act/>

²⁶ 1.3. Consistency with other Union policies, Explanatory Memorandum, AI Act Proposal <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206#footnoteref5>

²⁷ Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 — C9-0146/2021 — 2021/0106(COD)); Amendment 147, Proposal for a regulation, Article 2 — paragraph 1 — point c a (new) https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:C_202400506

²⁸ Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 — C9-0146/2021 — 2021/0106(COD)); Amendment 29, Proposal for a regulation, Recital 10, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:C_202400506

²⁹ European Coalition for Corporate Justice, Anti-Slavery International, Frank Bold, "Corporate Sustainability Due Diligence Directive Transposition Guide," August 2026, <https://corporatejustice.org/wp-content/uploads/2026/09/08-ECCJ-Transposition-guide-rhr.pdf>

To ensure that human rights harms from technology are prevented, including through the export of technology prohibited within the EU,³⁰ it would be appropriate to enact a horizontal ban on exports of dual-use technologies that fall under the scope of Article 5 of the EU AI Act.

Further, before granting export authorization to AI systems that fall under Annex III of the AI Act (high-risk AI systems), authorities should ensure that in addition to complying with the requirements set in the Dual Use Regulation, these technologies also comply with the relevant provisions of the AI Act in relation to data and data governance, documentation and record-keeping, transparency and provision of information to users, human oversight, robustness, accuracy and security, where these are not mandated under the Dual-Use Regulation.

The Commission and Member States must ensure that the Dual Use Regulation is capable in practice of safeguarding against harms from these new forms of surveillance exports that pose risks to human rights, and of preventing the export of technologies incompatible with human rights law (see below).

Need for Stronger Transparency

To be clear, transparency is not a substitute for effective state scrutiny and robust safeguards, but the inadequacy of current transparency measures, including the delay in their publication, hinders the ability of journalists, civil society and the public at large to shed light on dangerous exports.

“Greater transparency” is amongst the stated aims of the Dual-Use Regulation.³¹ However, while the Regulation requires (regarding cyber-surveillance items) disclosure of “the number of applications received by item, the issuing Member State and the destinations concerned by those applications, and on the decisions taken on those applications,” it omits other important elements, such as a requirement to disclose the names of companies or products involved, which hinders the usefulness of these measures for detecting abuses.³²

Further, as Human Rights Watch has pointed out, the January 2024 European Commission Guidelines on the Article 26 “direct member states to separately list the technologies and the countries to which they were exported, making it often impossible to determine which technologies went to which countries.”³³

³⁰ Amnesty International, “Toxic double standards: How Europe sells products deemed too dangerous for Europeans to the rest of the world – Joint briefing,” 26 September 2024, <https://www.amnesty.eu/news/toxic-double-standards-how-europe-sells-products-deemed-too-dangerous-for-europeans-to-the-rest-of-the-world-joint-briefing/>; Amnesty International, “The EU Corporate Sustainability Due Diligence Directive must fully cover the arms sector” 10 March 2023, <https://www.amnesty.eu/news/the-eu-corporate-sustainability-due-diligence-directive-must-fully-cover-the-arms-sector/>

³¹ “Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items,” (hereinafter “Dual-Use Regulation”), EUR-Lex, May 20, 2021, <https://eurlex.europa.eu/eli/reg/2021/821/oj/eng>, Preamble

³² Dual-Use Regulation at Art. 26.2

³³ Human Rights Watch, “Looking the Other Way EU Failure to Prevent Surveillance Exports to Rights Violators,” <https://www.hrw.org/report/2026/05/12/looking-the-other-way/eu-failure-to-prevent-surveillance-exports-to-rights>, p. 25

The most recent Annual Report on the dual-use regulation illustrates these shortcomings. Published in June 2026, it includes data only as recent as 2024. It lists only three types of information regarding cyber-surveillance items: the overall numbers of approvals and denials, the categories of items for which applications were made, and the country of destination, without any ability to draw connections between these disparate categories. While it somewhat worryingly notes that the number of denials is decreasing, it provides no meaningful way to scrutinize which tools are being exported where, nor whether the authorization process is functioning as intended.³⁴

This lack of transparency falls well short of what is required to fulfil the purpose of the transparency requirements. It is noteworthy that the PEGA Committee of the European Parliament, in this regard, has called for disclosure of: “information on the dual-use item in question; the number of licences applied for; the name of the exporting country; a description of the export company and whether this company is a subsidiary; a description of the end user and destination; the value of the export licence; and why the export licence was approved or denied; [and] emphasises that these reports should be made public on a quarterly basis”. The Committee further urged that the “exception to the requirement to provide information to the Commission on grounds of commercial sensitivity, defence and foreign policy or national security reasons must be abolished.”³⁵

In order to serve the function of enabling public oversight, the Commission and member states must ensure that transparency requirements include at least these elements, as well as the names of exporting companies and products, their corporate structures across jurisdictions, end users, and any human rights impact assessments undertaken.

Need for Stronger Human Rights Safeguards

Repeated surveillance scandals, including those documented by Amnesty International, demonstrate that stronger, and more comprehensive human rights safeguards are needed to protect against EU exports being used in ways that violate human rights. The Commission and Member States must ensure 1. That all exports that pose risks to human rights are subject to mandatory denial, 2. that the full range of human rights considerations is taken into account, 3. that surveillance-specific safeguards are considered and 4. that technology incompatible with human rights is not authorized for export.

Mandatory Denial of Exports that Pose Human Rights Risks

³⁴ REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the implementation of Regulation (EU) 2021/821 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items, 25 June 2026, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52026DC0296>

³⁵ European Parliament 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)), 15 June 2023, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.html, para. 64 (accessed 14 October 2026)

Ensuring that human rights are taken account of by member states and the EU is amongst stated aims of the Regulation.³⁶ This is most clear in several references made to the EU Council Common Position on exports, which requires states to deny exports where there is a clear risk that they might be used in connection with serious violations of international humanitarian law or “internal repression,” which is defined broadly with reference to the Universal Declaration on Human Rights and other international treaties.³⁷

However, this requirement of denial based on human rights risks is absent from Article 9, which merely allows, but does not mandate, the denial of non-listed items over human rights considerations, and also absent from Article 16.

In this regard, it is noteworthy that the PEGA Committee, in its final report, recommends “that export permits of dual-use goods must not be given where goods are or may be intended for use in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law.”³⁸

Amnesty International agrees and urges the Commission and Member States to make clear that export authorisations – for listed or non-listed items – must be denied where they pose clear risks to human rights.

Full Range of Human Rights Risks Must be Considered

Repeated reporting on the human rights impacts of unlawful surveillance have made clear that it routinely results in violations of a broad range of civil, political, economic, social and cultural rights.

In order to serve its purpose to protect human rights from harmful exports of technology, the Commission and Member States must make clear that the full human rights landscape of a proposed destination country or use is taken into account when deciding upon export authorisations.

This should include, for example, whether there have been violations of the right to protest, or the rights of workers to organize, whether human rights defenders, including journalists and others critical of the authorities are able to exercise their rights safely, whether patterns of discrimination

³⁶ Dual-Use Regulation, Preamble.

³⁷ “Internal repression includes, *inter alia*, torture and other cruel, inhuman and degrading treatment or punishment, summary or arbitrary executions, disappearances, arbitrary detentions and other major violations of human rights and fundamental freedoms as set out in relevant international human rights instruments, including the Universal Declaration on Human Rights and the International Covenant on Civil and Political Rights.” COUNCIL COMMON POSITION 2008/944/CFSP of 8 December 2008

defining common rules governing control of exports of military technology and equipment, Art. 2, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02008E0944-20190917>

³⁸ European Parliament 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)), 15 June 2023, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.html, para. 61 (accessed 14 October 2026)

against marginalized groups persist, whether victims of human rights abuses are able to access remedy in practice.

As the Commission noted in its 2024 Guidelines, “The misuse of non-listed cyber-surveillance items may negatively impact a broad spectrum of human rights, and directly interferes with the right to privacy and to data protection. Arbitrary or unlawful surveillance may also violate other human rights, such as the right to freedom of expression, association and assembly, freedom of thought, conscience and religion, as well as the right to equal treatment or prohibition of discrimination, and the right to free, equal and secret elections. In particular cases, the surveillance, including monitoring or collecting of information of the natural persons, such as human rights defenders, activists, political figures, vulnerable populations and journalists, may lead to intimidation, suppression, arbitrary detention, torture or even extrajudicial killings. Therefore, exporters should include these aspects relating to serious violations of human rights in their assessments.”³⁹

What is true for exporters must also be true for Member States scrutinizing export authorizations. Because these are the sorts of violations that have been documented to be associated with unlawful surveillance, they are those that member states must scrutinize when deciding upon export authorizations. A proper assessment of human rights risks requires a full consideration of all of the human rights protected under the UDHR.

Importance of Analysing Legal and Practical Safeguards

A key consideration as to whether the use of surveillance technology can be compatible with human rights law – and thus whether its export should be allowed – hinges on the existence of comprehensive legal safeguards in the destination country regarding the use and oversight of surveillance and other invasive technology, as well as their efficacy in practice. Gaps in such safeguards lead to chilling effects, which themselves can violate human rights.

As we have noted elsewhere, it is crucial to emphasize that such chilling effects reflect a failure of states (or corporate actors) to uphold their human rights obligations and responsibilities. They flow predictably and directly from the failure to establish safeguards to prevent abuse.⁴⁰ It is well-

³⁹ European Commission, "Commission Recommendation (EU) 2024/2659 on Guidelines on the Export of Cyber-Surveillance Items under Article 5 of Regulation (EU) 2021/821 of the European Parliament and of the Council," October 11, 2024, at 1.3.2, https://eurlex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402659

⁴⁰ “UN experts: Safeguard human freedoms from systematic digital interference, surveillance and chilling effects on civic space,” Joint Statement of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, the Special Rapporteur on the situation of human rights defenders and the Special Rapporteur on the right to privacy, 27 April 2026, <https://www.ohchr.org/sites/default/files/statements/20260427-safeguard-hr-freed-syst-digi-inter-surv-chill-civic-space-sr-freedom-peaceful-en.pdf>; “Pushed into the Shadows: Evidencing digital surveillance chilling effects and the erosion of the rights to freedom of assembly and of association.” Study by the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Gina Romero, Pete Fussey and Daragh Murray, <https://www.ohchr.org/sites/default/files/documents/form/digital-surveillance-chilling-effects-shadows-erosion-freedom-1-en.pdf>; Daragh Murray, Pete Fussey, Kuda Hove, Wairagala Wakabi, Paul Kimumwe, Otto Saki, Amy Stevens, “The

established that where safeguards are lacking, for example, where people are unable to know when, how or on which basis they may be subject to surveillance, where abuses go uninvestigated, or where remedy is unattainable in practice, “widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified [...]. In such circumstances the threat of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right [to private and family life].”⁴¹

Amnesty International’s research bears this out.⁴² In nearly all contexts where safeguards are lacking, the fear of surveillance abuses has itself led to concrete human rights harms. Activists have reported that fears that their offices were bugged, their phone calls listened in on, their locations tracked and their online communications at risk of hacking.⁴³ The psychological stress of the fear of surveillance and the self-censorship this fear causes, undermined the ability to conduct daily activities of activists – meeting, making phone calls, arranging public protests, raising funds – made more difficult, undermining their ability to function.

The harms of chilling effects extend beyond national borders, and go beyond the exercise of civil and political rights, for example leading activists to forego participation in associations, assembly, as well as accessing medical services, work, and education.⁴⁴ In some instances, this has also included foregoing contact with family and friends even in exile.⁴⁵

Accordingly, the Commission and Member States must ensure that export authorization processes take account of the existence of legal safeguards and their efficacy in practice when deciding whether to authorize exports.

Compatibility of Technology with Human Rights

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, <https://doi.org/10.1093/jhuman/huad020>

⁴¹ European Court of Human Rights, *Zakharov v. Russia* Application no. 47143/06, para. 171.

⁴² Amnesty International, South Sudan: “These walls have ears”: The chilling effect of surveillance in South Sudan, 2 February 2021, AFR 65/3577/2021, <https://www.amnesty.org/en/documents/afr65/3577/2021/en/>; Amnesty International, ‘Inside the NYPD’s Surveillance Machine’, 14 May 2026, <http://banthescan.amnesty.org/decode>; Amnesty International, ‘Israel and Occupied Palestinian Territories: Automated Apartheid: How facial recognition fragments, segregates and controls Palestinians in the OPT’, 2 May 2023, <https://www.amnesty.org/en/documents/mde15/6701/2023/en/>.

⁴³ Amnesty International, It’s enough for people to feel it exists: Civil society, secrecy and surveillance in Belarus, 7 July 2016, EUR 49/4306/2016, <https://www.amnesty.org/en/documents/eur49/4306/2016/en/>

⁴⁴ Amnesty International, ‘Israel and Occupied Palestinian Territories: Automated Apartheid: How facial recognition fragments, segregates and controls Palestinians in the OPT’, 2 May 2023, <https://www.amnesty.org/en/documents/mde15/6701/2023/en/>.

⁴⁵ Amnesty International, “We Will Find You, Anywhere”: The Global Shadow of Uzbekistani Surveillance, <https://medium.com/amnesty-insights/we-will-find-you-anywhere-the-global-shadow-of-uzbekistani-surveillance-254405805860>

While safeguards may help in diminishing the risk associated with the use of certain technologies, there are an increasing number of technologies that are, by their nature, incompatible with human rights. The Commission and Member States must ensure that these technologies be banned from use and accordingly, their export authorisations denied.

This includes many forms of modern highly invasive spyware. Amnesty International calls for a global ban on these forms spyware, because they allow unlimited access to a device and their use cannot be independently audited.

Because of these features, even a human rights compliant regulatory framework would be inadequate to prevent human rights violations linked to highly invasive spyware with these characteristics, as has long been argued by Amnesty International.⁴⁶ This accords with the findings of the UN Special Rapporteur on Freedom of Peaceful Assembly and of Association, who has called on states to strictly prohibit “uses and transfer of intrusive digital tools failing to comply with human rights protections, including highly invasive spyware (whose functionality cannot be limited or whose use cannot be independently audited).”⁴⁷ Similarly, the European Data Protection Supervisor noted that “the 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.”⁴⁸ This aligns with the reasoning presented by the former Special Rapporteur on counter-terrorism, who argued that spyware that it is incapable of being meaningfully limited in its functionality, and whose use cannot be audited independently, should be subject to a ban.⁴⁹

In human rights terms, the inability of highly invasive spyware, such as NSO Group’s Pegasus or Intellexa’s Predator, to be limited in the amount of data it accesses means that its use cannot comport with the human rights law requirement of necessity and proportionality, since by definition it cannot be the least intrusive tool. The inability to independently audit the use of such spyware – which intentionally obscures the traces of its use – means that the human rights safeguards of independent oversight – which is also crucial to the right to remedy – cannot be effective at detecting abuses. As

⁴⁶ See, for example, Amnesty International. “A Digital Prison”: Surveillance and the Suppression of Civil Society in Serbia (EUR 70/8813/2024), 16 December 2024, <https://www.amnesty.org/en/documents/eur70/8813/2024/en/>; Amnesty International, Thailand: “Being ourselves is too dangerous”: Digital violence and the silencing of women and LGBTI activists in Thailand (Index: ASA 39/7955/2024), 16 May 2024, <https://www.amnesty.org/en/documents/asa39/7955/2024/en/>, Section 5.1.

⁴⁷ UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, *Unmasking the chilling effects of the digital surveillance ecosystem: the erosion of assembly and association rights*, 21 April 2026, UN Doc. A/HRC/62/45, para. 112(h)(i)(i).

⁴⁸ European Data Protection Supervisor, Preliminary remarks on modern spyware, 15 February 2022, p.8, https://www.edps.europa.eu/data-protection/our-work/publications/papers/edps-preliminary-remarks-modern-spyware_en

⁴⁹ UN Special Rapporteur on Counter-Terrorism, Position Paper, Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach, December 2022, para. 46, <https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spywaretechnology-trade.pdf>

such, highly invasive spyware can never be used in a human rights compliant manner and should be permanently banned.

This category of technology also includes Facial recognition technology (FRT) for identification (also referred to as 1:n, or one-to-many), which is built upon mass surveillance, and its use creates impermissible violations of the rights to privacy, equality and non-discrimination, as well as associated human rights, including freedom of expression, peaceful assembly and association.⁵⁰

Amnesty International's research has documented how this technology has been used to undermine protest rights, including of Black Lives Matter activists in the USA, as well as human rights in other contexts, including Buenos Aires, the Occupied Palestinian Territory, and Hyderabad, India.⁵¹ As identified by Amnesty International and other civil society actors and investigative journalists, some of these technologies have been exported from EU Member States to third countries where these have been used to commit human rights violations or have risked entrenching surveillance. A 2020 Amnesty International investigation found that three companies based in France, Sweden and the Netherlands sold digital surveillance systems, such as facial recognition technology and network cameras, to key players of the Chinese mass surveillance apparatus. In some cases, the export was directly for use in China's indiscriminate mass surveillance programmes, with the risk of being used against Uyghurs and other predominantly Muslim ethnic groups throughout the country.⁵² In 2021, Amnesty International highlighted the staggering lack of transparency in relation to the involvement in Hyderabad's surveillance infrastructure of companies based in France and Portugal.⁵³ Amnesty International's "Automated Apartheid" report identified the involvement of a Dutch company in maintaining and further entrenching Israel's system of apartheid against Palestinians.⁵⁴ Similar exports of AI-based surveillance technologies have been documented by Access Now and partners on the export of EU-made surveillance technologies to countries in Latin America,⁵⁵ as well as more recently by Investigate Europe on export of facial recognition technologies from the EU to Brazil,⁵⁶

⁵⁰ Amnesty International, Ban the Scan, <https://banthescan.amnesty.org/>

⁵¹ Ban the Scan, New York City, <https://banthescan.amnesty.org/nyc/index.html>; Amnesty International, 2 May 2023, Israel and Occupied Palestinian Territories: Automated Apartheid: How facial recognition fragments, segregates and controls Palestinians in the OPT, MDE 15/6701/2023, <https://www.amnesty.org/en/documents/mde15/6701/2023/en/>; Ban the Scan, India, <https://banthescan.amnesty.org/hyderabad/index.html>.

⁵² Amnesty International: Out of Control: Failing EU Laws for Digital Surveillance Export, 21 September 2020, <https://www.amnesty.org/en/documents/EUR01/2556/2020/en/>

⁵³ Amnesty International, Ban The Scan Hyderabad; 9 November 2021; <https://banthescan.amnesty.org/hyderabad/>

⁵⁴ Amnesty International, Automated Apartheid: How facial recognition fragments, segregates and controls Palestinians in the OPT, 2 May 2023, <https://www.amnesty.org/en/documents/mde15/6701/2023/en/>

⁵⁵ Access Now, the Asociación por los Derechos Civiles (ADC), the Laboratório de Políticas Públicas e Internet (LAPIN), and LaLibre.net - "Surveillance Tech in Latin America Made Abroad, Deployed at Home", August 2021, <https://www.accessnow.org/wp-content/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf>

⁵⁶ Investigate Europe & Pulitzer Center's AI Accountability Network, Blocked in Europe, deployed abroad: The facial recognition system monitoring Brazil's schoolchildren, 13 March 2026, <https://www.investigate-europe.eu/posts/facial-recognition-software-ai-europe-brazil-school-children>. This system has since been suspended by the Brazilian Data Protection Authority (https://www.linkedin.com/posts/nicoschmidt_in-march-leonardo-coelho-and-i-revealed-activity-7491365484450467842-

India,⁵⁷ Uruguay.⁵⁸ The latter investigations are noteworthy given their publication after the EU's AI Act has prohibited the very same technologies, deeming them to pose unacceptable risk to fundamental rights within the Union.

Other AI-powered tools that are incompatible with – or pose unacceptable risks to – human rights include:

- biometric technologies (including so-called emotion recognition systems) that enable mass surveillance and discriminatory targeted surveillance,
- AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage,
- automated risk assessment and profiling systems in the context of migration, policing or social benefits.⁵⁹

The Commission and Member States must ensure that such technologies, the use of many of which is prohibited inside the EU under the AI Act, are not allowed to be exported from the EU.

Stronger Due Diligence

Corporate due diligence requirements must be made mandatory, in line with the United Nations Guiding Principles on Business and Human Rights, the OECD Due Diligence Guidance and the EU Corporate Sustainability and Due Diligence Directive.

This is especially important as regards the issue of non-listed cyber-surveillance technologies. While Article 5 (the so-called “catch-all clause”) creates the possibility for export authorities to notify

[ivSK?utm_source=social_share_send&utm_medium=member_desktop_web&rcm=ACoAAATLndUBZ-Kfrm9hgTvEEAMQOErak5ILzJY\).](https://www.investigate-europe.eu/posts/made-in-spain-surveillance-tech-banned-in-eu-booms-in-india)

⁵⁷ Investigate Europe, The Reporters' Collective and InfoLibre, in partnership with the Pulitzer Center's AI Accountability Network, Made in Spain: Surveillance tech banned in EU booms in India, 15 July 2026, <https://www.investigate-europe.eu/posts/made-in-spain-surveillance-tech-banned-in-eu-booms-in-india>

⁵⁸ Investigate Europe and infoLibre, El reconocimiento facial ‘made in Spain’ que España veta en sus estadios se exporta a América Latina, 2026, https://www.infolibre.es/investigacion/reconocimiento-facial-made-in-spain-espana-veta-estadios-exporta-america-latina_130_2227052.html; <https://www.busqueda.com.uy/informacion/el-reconocimiento-facial-made-in-spain-que-espana-veta-sus-estadios-se-exporta-uruguay-n5415319>

⁵⁹ UN Special Rapporteur on the on the rights to freedom of peaceful assembly and of association, *Unmasking the chilling effects of the digital surveillance ecosystem: the erosion of assembly and association rights*, 21 April 2026, UN Doc. A/HRC/62/45, para. 112(h)(i)(ii)-(iii), (calling on states to strictly prohibit: “Arbitrary, indiscriminate and mass surveillance used for law enforcement purposes, including biometric and AI applications, such as facial recognition technology, AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the Internet or CCTV footage, and AI systems for social scoring; (iii) The use of surveillance technologies and data collection for arbitrary and discriminatory predictive and profiling purposes, including predictive policing, and for purposes not warranted,”); Amnesty International, *Automating Suspicion: Risk Profiling as a Smokescreen for Structural Discrimination and Inequality*, 11 June 2026, <https://www.amnesty.org/en/documents/POL40/1096/2026/en/>; Amnesty International, *Recommendations to the Parliamentary Assembly and Committee of Ministers of the Council of Europe on the Draft Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law*, IOR 10/2024.5404, 11 April 2024, <https://www.amnesty.eu/wp-content/uploads/2024/04/Amnesty-International-Recs-draft-CoECAI-11042024.pdf>

companies of the need to subject non-listed items to export authorization, it does not mandate it. Rather, it places the obligation on companies to notify the authorities that their own products may be intended for use in connection with human rights abuses.

This assumption is premised on the idea that companies will voluntarily submit to export authorization without their due diligence processes being subject to rigorous oversight or reporting requirements. Nor is there evidence that Member States are making use of this provision. As a 2025 report from the Centre for Democracy & Technology Europe noted, “based on information collected through interviews with licensing officials, however, the use of the catch-all control appears to have been limited, with no reported cases of Member States notifying exporters of the requirement to obtain a license.”⁶⁰

As noted in other sections, the 2024 Commission Guidelines on Article 5 contain several positive elements. However, while these guidelines may be helpful in assisting exporters who seek to comply with the requirements of the Regulation, they are insufficient to prevent those who wish to evade scrutiny from doing so.

The Commission and Member States must ensure that human rights due diligence obligations on exporting companies are mandatory, ongoing and subject both to state oversight and scrutiny, as well as public, through the mandate to make due diligence findings public.

⁶⁰ Center for Democracy and Technology Europe, “From Export Control to Unknown Exports: How the EU’s Dual-Use regime falls short on tackling spyware,” December 2025, p. 18, <https://cdt.org/insights/cdt-europe-report-eu-export-controls-are-failing-to-address-the-spread-of-spyware/>