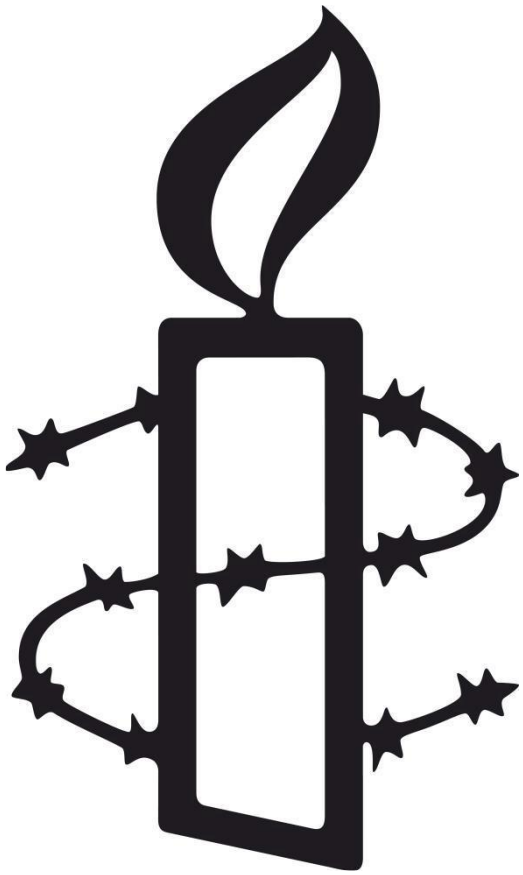
IMPACT OF DIGITAL AND AI-ASSISTED SURVEILLANCE ON ASSEMBLY AND ASSOCIATION RIGHTS, INCLUDING CHILLING EFFECTS

SUBMISSION TO THE SPECIAL RAPPORTEUR ON FREEDOM OF PEACEFUL ASSEMBLY AND OF ASSOCIATION



AMNESTY INTERNATIONAL

CONTENTS

Amnesty International submits this analysis in response to the call for contributions with a view to informing the report of the Special Rapporteur for the 62nd session of the Human Rights Council. It is not an exhaustive account of Amnesty International's research, but focuses on questions 1-2, 4, and 6-8.

1. INTRODUCTION

Amnesty International submits this analysis in response to the call for contributions[1] with a view to informing the report of the Special Rapporteur for the 62nd session of the Human Rights Council. It is not an exhaustive account of Amnesty International's research, but focuses on questions 1-2, 4, and 6-8.

2. TYPES OF SURVEILLANCE (QUESTION 1)

For years, civil society has warned that states are enjoying a "golden age of surveillance," as more and more of our online and offline lives are accessible to a growing array of new tools designed to track us. Amnesty International has documented numerous types of technology whose use impacts on human rights, notably the rights to freedom of peaceful assembly and of association.

The use of facial recognition technology (FRT) – which is fundamentally incompatible with human rights (see 6, below) is becoming worryingly commonplace. Amnesty International has documented abuses linked to FRT in The Occupied Palestinian Territories, Hyderabad, New York City, and Argentina. In France, authorities proposed a system of AI-powered video surveillance in the run-up to the Paris Olympics.[2] FRT has also been used by police in Denmark,[3] while in The Netherlands, the under-regulated use of cameras at peaceful protests, and the accompanying lack of transparency, have created chilling effects around the exercise of protest rights.[4] In Hungary (see section 6, below), legal changes allowing the use of FRT to target, *inter alia*, Pride marches, is a grave concern.

The use and abuse of these tools have particularly harmful impacts on marginalized communities. Migrants, in particular, are too often exempted from regulatory protections (such as the migration exemption in the EU's AI Act), and treated as "testing grounds" for controversial technologies, including biometric identification technologies.[5] The precarious status of migrants can lead to their being targeted for their protected protest rights, including through the use of surveillance and social media monitoring software, as Amnesty International highlighted in the United States.[6]

The use of spyware – much of which is fundamentally incompatible with human rights – as well as other forms of mass and targeted digital surveillance, continue to be a grave threat to protestors and HRDs in general (see section 6, below). Amnesty International has also documented the abuse of digital forensics tools, such as Cellebrite's UFED, to extract phone data from people exercising their right to protest, including its use to surreptitiously install spyware.[7]

3. HUMAN RIGHTS IMPACTS OF SURVEILLANCE (QUESTION 2)

Argentina - Argentina has recently adopted a series of measures that raise serious human rights concerns, framed in an increasingly repressive approach toward protest and public dissent. The government has

[1] https://www.ohchr.org/en/calls-for-input/2025/call-input-hrc62-thematic-report-impact-digital-and-ai-assisted-surveillance

[2] "French plans for AI surveillance during Olympics are dangerous," Agnes Callamard, Al Jazeera, 10 March 2023, https://www.aljazeera.com/opinions/2023/3/10/french-plans-for-ai-surveillance-during-olympics-are-dangerous; Amnesty International, France: Intrusive Olympics surveillance technologies could usher in a dystopian future, 20 March 2023, https://www.amnesty.org/en/latest/news/2023/03/france-intrusive-olympics-surveillance-technologies-could-usher-in-a-dystopian-future/; Amnesty International, France: Allowing mass surveillance at Olympics undermines EU efforts to regulate AI, 23 march 2023, https://www.amnesty.org/en/latest/news/2023/03/france-allowing-mass-surveillance-at-olympics-undermines-eu-efforts-to-regulate-ai/

[3] Justitia, Justitia udgiver åbent brev: Nedsæt en privatlivskommission og stop hastebehandling af PET-loven, https://justitia-int.org/justitia-udgiver-aabent-brev-nedsaet-en-privatlivskommission-og-stop-hastebehandling-af-pet-loven/

[4] Amnesty International, The Netherlands: Recording dissent: Camera surveillance at peaceful protests in the Netherlands, 16 October 2024, EUR 35/8469/2024, https://www.amnesty.org/en/documents/eur35/8469/2024/en/

[5] EDRi, Technological Testing Grounds Migration Management Experiments and Reflections from the Ground Up, https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf; Amnesty International,

The Digital Border: Migration, Technology and Inequality, 21 May 2024, POL 40/7772/2024, https://www.amnesty.org/en/documents/pol40/7772/2024/en/

[6] 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/

[7] Amnesty International, Serbia: "A Digital Prison": Surveillance and the suppression of civil society in Serbia, 16 December 2024, EUR 70/8813/2024, https://www.amnesty.org/en/documents/eur70/8813/2024/en/

authorized the use of artificial intelligence, cyber patrolling, and predictive algorithms in policing tasks. These measures, combined with the "anti-protest protocol" (Resolution 943/2023), have created an environment in which digital and physical surveillance converge to monitor, deter, and criminalize freedoms of peaceful assembly and of association. The state's ability to track online speech, identify participants in demonstrations, and store this information in opaque databases poses direct risks to freedom of expression, association, and assembly.[8]

In Serbia, Amnesty International research found that protestors were subject to unlawful surveillance using spyware (See 6, below), as well as subject to unlawful device searches using digital forensics tools provided by the company Cellebrite, as part of a broader crackdown on activism that saw activists subject to smear campaigns and criminal proceedings.[9]

In the United States, technology that included social media surveillance capabilities and other big data analytics, provided by the companies Palantir and Babel X has been used to target pro-Palestinian rights protestors and others in irregular migration status for deportation, creating chilling effects on human rights.[10]

4. SURVEILLANCE CHILLING EFFECTS (QUESTION 4)

Chilling effects are intimately tied to abuses of surveillance technologies and the lack of comprehensive safeguards to prevent such abuses (see section 6, below).

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.[11] It is well-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]."[12]

Amnesty International's research bears this out.[13] 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.[14] 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 contact with family and friends even in exile.[15]

[8] https://www.instagram.com/p/DLF2izFv1E8/?img_index=2; https://x.com/amnistiaar/status/1935076558147924136

[9] Amnesty International, Serbia: "A Digital Prison": Surveillance and the suppression of civil society in Serbia, 16 December 2024, EUR 70/8813/2024, https://www.amnesty.org/en/documents/eur70/8813/2024/en/

[10] 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/

[11] Daragh Murray, Pete Fussey, Kuda Hove, Wairagala Wakabi, Paul Kimumwe, Otto Saki, Amy Stevens, "The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe," *Journal of Human Rights Practice*, Volume 16, Issue 1, February 2024, Pages 397-412, https://doi.org/10.1093/jhuman/huad020

[12] European Court of Human Rights, Zakharov v. Russia Application no. 47143/06, para. 171.

[13] 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/

[14] 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/

[15] 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

5. SURVEILLANCE AND VULNERABLE/MARGINALIZED GROUPS (QUESTION 6)

In The Philippines, the two successive governments of President Duterte and President Marcos Jr. have weaponized digital tools, misinformation and a flawed anti-terrorism law to create a climate of fear and intimidation amongst young human rights defenders.[16] The central element in this coordinated campaign of state violence is the practice of "red-tagging", through which leading political figures and state security actors have vilified human rights defenders, student activists, teachers, journalists and others as "Communist rebels" and "terrorists", inciting hatred and violence, and leading to widespread chilling effects.[17]

In Thailand, women and LGBTI activists have been unlawfully targeted with digital surveillance, including Pegasus spyware and online harassment, by state and non-state actors, in an effort to silence them, in an example of how Tech-facilitated Gender Based Violence (TfGBV) can be used to punish activists for their protected exercise of their protest rights, leading to serious mental health consequences and other chilling effects.[18]

6. NECESSARY SAFEGUARDS, REGULATION AND RED LINES (QUESTION 7)

The presence of robust and comprehensive human rights safeguards is a necessary pre-condition for the use of any surveillance technologies, but importantly – not a sufficient one. It is also crucial to emphasize that in order to be effective, safeguards must be comprehensive. By definition, safeguards which are not capable of preventing all abuses will continue to allow some, and abuses of surveillance technologies in particular, proliferate where loopholes exist that allow them.

For this reason, Amnesty International has long called for a moratorium on the sale, transfer or use of all spyware until such time as a comprehensive system of human rights safeguards is in place capable of preventing abuses.[19] This call is supported by numerous other civil society groups,[20] as well as an ever-expanding list of international legal experts and authorities.[21]

When it comes to AI-powered surveillance technologies, it is important that safeguards be put in place throughout the lifecycle of AI products, and not focus only on the procurement or deployment phase.[22] Regulations must not adopt blanket or disproportionate exemptions based on policing, national security, military or other grounds. Regulations must avoid blanket exemption that prevents AI regulation from being applied to the research and development phases of the AI lifecycle and must ensure that technical and human rights safeguards apply to exported AI technologies. Deployers must publish detailed human rights

[16] Amnesty International, Philippines: "I turned my fear into courage": Red-tagging and state violence against young human rights defenders in the Philippines, 14 October 2024, ASA 35/8574/2024, https://www.amnesty.org/en/documents/asa35/8574/2024/en/

[17] Amnesty International, Philippines: Left to Their Own Devices Report, 4 April 2025, ASA 35/9187/2025, https://www.amnesty.org/en/documents/asa35/9187/2025/en/

[18] Amnesty International, Thailand: "Being ourselves is too dangerous": Digital violence and the silencing of women and LGBTI activists in Thailand, 16 May 2024, ASA 39/7955/2024, https://www.amnesty.org/en/documents/asa39/7955/2024/en/

[19] Amnesty International, Towards a Global Moratorium on Targeted Surveillance Technology, https://www.amnesty.org/en/wp-content/uploads/2022/11/POL4061542022ENGLISH.pdf

[20] EDRi, EDRi joins coalition demanding that states implement a moratorium on the sale, transfer & use of surveillance technology; Access Now, No to spyware: media, civil society demand ban on tech used for human rights abuses; Human Rights Watch, Unchecked Spyware Industry Enables Abuses Governments Should Halt Trade in Surveillance Technology, https://www.hrw.org/news/2021/07/30/unchecked-spyware-industry-enables-abuses

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

[22] 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; Amnesty International, David Nolan, Hajira Maryam & Michael Kleinman, The Urgent but Difficult Task of Regulating Artificial Intelligence, 16 January 2024, https://www.amnesty.org/en/latest/campaigns/2024/01/the-urgent-but-difficult-task-of-regulating-artificial-intelligence/

impact assessments before each deployment. Regulation must ensure transparency and accountability mechanisms that empower affected communities to realize the right to remedy in practice.

It is also critical to emphasize that sector-specific safeguards must form part of a larger human rights regulatory framework that includes, *inter alia*, privacy and data protection laws, as well as corporate governance and due diligence laws, and strong protections for whistleblowers and for privacy-protecting technologies, such as encryption.[23] This is especially important where data, after being collected, may be repurposed or combined with other data in non-transparent ways which may create chilling effects, especially for marginalized communities who face specific risks.

6.1 COMMON REGULATORY FAILURES

States too often abuse national security and other grounds to create regulatory loopholes that lead to human rights abuses, as do abuse of trade secrecy and business confidentiality clauses.[24] These may be of a general nature, or related to specific issues, notably transparency requirements. The EU AI Act, for example, includes exceptions to transparency and accountability requirements for law enforcement, national security and migration and border control, including where states collaborate with private vendors.[25]

Failure to meaningfully consult with civil society may also lead to regulation that fails to uphold human rights standards.[26]

6.2 TECHNOLOGIES THAT MUST BE PROHIBITED AS INCOMPATIBLE WITH HUMAN RIGHTS

It is also important to emphasize that certain technologies – by their design – are fundamentally incompatible with International Human Rights Law, and that their production, transfer, and use must be prohibited. Examples of technologies which run afoul of this red line include:

HIGHLY INVASIVE SPYWARE

Highly invasive spyware refers to spyware that allows unlimited access to a device by default, and which cannot be limited in its functionality to only those functionalities that are necessary and proportionate to a specific use and target; or whose use is not verifiable and capable of being independently audited. These characteristics mean that this type of spyware, by design, cannot comply with the requirements of proportionality in its deployment (since by default it has access to the maximum amount of data possible) and undermines the requirements of oversight and accountability, as well as the right to remedy (since it deliberately obscures traces of its use and subverts the investigation of abusive uses.)

Amnesty International has documented numerous cases of abuse of this type of spyware, with examples including NSO's Pegasus software, and Intellexa's Predator.[27]

---

[23] Amnesty International, Encryption: a matter of human rights, 22 March 2016, POL 40/3682/2016, https://www.amnesty.org/en/documents/pol40/3682/2016/en/

[24] Amnesty International, Europe: Dangerously disproportionate: The ever-expanding national security state in Europe, 17 January 2017, EUR 01/5342/2017, https://www.amnesty.org/en/documents/eur01/5342/2017/en/; Amnesty International, India/Global: New technologies in automated social protection systems can threaten human rights, 29 April 2024, https://www.amnesty.org/en/latest/news/2024/04/india-global-new-technologies-in-automated-social-protection-systems-can-threaten-human-rights/

[25] Civil Society Joint Statement, EU's AI Act fails to set gold standard for human rights, https://www.amnesty.eu/news/eus-ai-act-fails-to-set-gold-standard-for-human-rights/

[26] Amnesty International, Human rights and justice must be at the heart of the upcoming Commission guidelines on the AI Act implementation, 16th January 2025, https://www.amnesty.eu/news/human-rights-and-justice-must-be-at-the-heart-of-the-upcoming-commission-guidelines-on-the-ai-act-implementation/ ("…we note the shortcomings of the Commission's consultation process: notably, the lack of advanced notice and a short time frame for submissions, no publication of the draft guidelines to enable more targeted and useful feedback, lack of accessible formats for feedback, strict character limits on complicated, and at times leading, questions which required elaborate answers…"

[27] Amnesty International, Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group's Tools, 22 June 2020, https://securitylab.amnesty.org/latest/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools/; Amnesty International, Kazakhstan: Four activists' mobile devices infected with Pegasus Spyware, 9 December 2021, https://securitylab.amnesty.org/latest/2021/12/kazakhstan-four-activists-mobile-devices-infected-with-pegasus-spyware/; Amnesty International, India: Damning new forensic investigation reveals repeated use of Pegasus spyware to target high-profile journalists, 28 December 2023, https://securitylab.amnesty.org/latest/2023/12/india-damning-new-forensic-investigation-reveals-repeated-use-of-pegasus-spyware-to-target-high-profile-

Amnesty International has urged courts[28] and other bodies to support the ban on highly invasive spyware, a call that is supported by the findings of the UN Special Rapporteur on Countering Terrorism[29] and the European Data Protection supervisor,[30] and more recently by the Special Rapporteurship for Freedom of Expression of the Inter-American Commission on Human Rights, who called on states to "Prohibit, through the appropriate regulatory authority, the acquisition, import, and use of commercial spyware technologies lacking technical safeguards to limit functions to specific, necessary, and proportionate surveillance objectives."[31]

FACIAL RECOGNITION TECHNOLOGY

Facial recognition technology (FRT) for identification (also referred to as 1:n, or one-to-many) 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 peaceful assembly and association.[32]

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 human rights in other contexts, including the Occupied Palestinian Territories, and Hyderabad, India.[33] Authorities in France have also turned to mass video surveillance powered by AI around the Olympics,[34] while authorities in Hungary have introduced legislative changes to allow the use of FRT to target participants in the Pride marches.[35]

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

- biometric technologies 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, when used to determine whether people on the move present a 'risk' of unlawful activity or security threats,

journalists/; Amnesty International, Thailand: "Being ourselves is too dangerous": Digital violence and the silencing of women and LGBTI activists in Thailand, 16 May 2024, ASA 39/7955/2024, https://www.amnesty.org/en/documents/asa39/7955/2024/en/; Amnesty International, Serbia: Journalists targeted with Pegasus spyware, 27 March 2025, https://securitylab.amnesty.org/latest/2025/03/journalists-targeted-with-pegasus-spyware/; Amnesty International, Armenia/Azerbaijan: Pegasus spyware targeted Armenian public figures amid conflict, 25 May 2023, https://securitylab.amnesty.org/latest/2023/05/armenia-azerbaijan-pegasus-spyware-targeted-armenian-public-figures-amid-conflict-2/; 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/; Amnesty International, El Salvador: Amnesty International verifies use of Pegasus spyware for surveillance of journalists, 13 January 2022, https://securitylab.amnesty.org/latest/2022/01/el-salvador-pegasus-spyware-surveillance-journalists/; Amnesty International, The Pegasus Project: How Amnesty Tech uncovered the spyware scandal, 23 March 2022, https://www.amnesty.org/en/latest/news/2022/03/the-pegasus-project-how-amnesty-tech-uncovered-the-spyware-scandal-new-video/; Amnesty International, Case Study: The Predator Files, https://securitylab.amnesty.org/case-study-the-predator-files/

[28] Amnesty International, Poland: Written submissions filed to the European Court of Human Rights in the case of Krzysztof Brejza v. Poland and 8 Other Applications, 26 February 2025, https://securitylab.amnesty.org/latest/2025/02/poland-written-submissions-filed-to-the-european-court-of-human-rights-in-the-case-of-krzysztof-brejza-v-poland-and-8-other-applications/

[29] United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach, April 2023, https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf. See generally Paras. 125 – 127 ("Spyware which fails to display such features cannot, however otherwise tightly regulated, be capable of human rights compliance.")

[30] EDPS Preliminary Remarks on Modern Spyware, https://www.edps.europa.eu/data-protection/our-work/publications/papers/edps-preliminary-remarks-modern-spyware_en. See section 4 ("…the capability of spyware tools such as Pegasus to provide full and unrestricted control by the attacker of the target's phone, coupled with the fact that they leave very little, if any, digital traces, raises the question of to what extent the information gathered with their help could be used as evidence in a criminal procedure.")

[31] The Impact of Digital Surveillance on Freedom of Expression in the Americas, Special Rapporteurship for Freedom of Expression of the Inter-American Commission on Human Rights, September 2025, https://www.oas.org/en/iachr/expression/reports/VigilanciaRELECIDH.pdf

[32] Amnesty International, Ban the Scan, https://banthescan.amnesty.org/

[33] 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.

[34] "French plans for AI surveillance during Olympics are dangerous," Agnes Callamard, Al Jazeera, 10 March 2023, https://www.aljazeera.com/opinions/2023/3/10/french-plans-for-ai-surveillance-during-olympics-are-dangerous

[35] Amnesty International, Hungary: Pride ban is full-frontal attack on LGBTI people and must not be signed into law, 18 March 2025, https://www.amnesty.org/en/latest/news/2025/03/hungary-pride-ban-is-full-frontal-attack-on-lgbti-people-and-must-not-be-signed-into-law/; EDRi, The Commission must uphold the AI Act and fundamental freedoms in Hungary, https://edri.org/our-work/the-commission-must-uphold-the-ai-act-and-fundamental-freedoms-in-hungary/

- predictive analytic systems used to interdict, curtail and prevent migration,
- the use of AI in predictive policing (prediction of crimes by individual person(s) and/or in given spaces and/or times),
- the use of AI systems for social scoring,
- the export of AI systems that are incompatible with human rights.[36]

7. ROLES AND RESPONSIBILITIES OF DIFFERENT ACTORS (QUESTION 8)

The under- or in many cases unregulated production and trade in surveillance tech continues to fuel a surveillance crisis globally. Tech companies must be held accountable for failing to uphold their human rights responsibilities, and states must ensure that these companies are subject to regulation adequate to prevent abuses.

A lack of transparency, coupled with often deliberately complex and shifting corporate structures, makes it difficult, if not impossible, for HRDs, or the general public, to know which surveillance tools are being purchased or used against them.[37] This dynamic is facilitated by investors, including venture capital firms, failing to take account of their due diligence responsibilities, as well as states failing to regulate the surveillance industry, including by controlling dangerous exports.[38]

The lobbying influence of Big Tech companies is also a critical human rights concern. The market dominance of a handful of large companies creates dangers to numerous human rights, notably in the power of these companies to lobby against effective regulation that protects human rights.[39] In the EU, a push for "simplification" of digital rights regulations could threaten key rights protections, and follows a massive increase in lobbying by Big Tech firms.[40]

[36] 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

[37] Amnesty International, A Web of Surveillance: Unravelling a murky network of spyware exports to Indonesia, 1 May 2024, https://securitylab.amnesty.org/latest/2024/05/a-web-of-surveillance/; Amnesty International, 23 July 2021, Uncovering the Iceberg: The Digital Surveillance Crisis Wrought by States and the Private Sector, DOC 10/4491/2021, https://www.amnesty.org/en/documents/doc10/4491/2021/en/;

[38] Amnesty International, 21 October 202, Operating in the shadows: Investor risk from the private surveillance industry, DOC 10/4359/2021, https://www.amnesty.org/en/documents/doc10/4359/2021/en/; Amnesty International, Silicon Shadows: Venture Capital, Human Rights, and the Lack of Due Diligence, https://www.amnestyusa.org/reports/silicon-shadows-venture-capital-human-rights-and-the-lack-of-due-diligence/; Amnesty International, 21 September 2020, Out of Control: Failing EU Laws for Digital Surveillance Export, EUR 01/2556/2020, https://www.amnesty.org/en/documents/eur01/2556/2020/en/; Amnesty International, 9 September 2025, Pakistan: Shadows of Control: Censorship and mass surveillance in Pakistan, ASA 33/0206/2025, https://www.amnesty.org/en/documents/asa33/0206/2025/en/

[39] Amnesty International, 28 August 2025, Breaking up with Big Tech: A human rights-based argument for tackling Big Tech's market power, POL 30/0226/2025, https://www.amnesty.org/en/documents/POL30/0226/2025/en/;

[40] Joint statement: The EU must uphold hard-won protections for digital human rights, 13th November 2025, https://www.amnesty.eu/news/eu-must-uphold-protections-for-digital-human-rights/; Corporate Europe Observatory, Byte by byte: How Big Tech undermined the AI Act, 17 November 2023, https://corporateeurope.org/en/2023/11/byte-byte; Corporate Europe Observatory, Trojan horses: how European startups teamed up with Big Tech to gut the AI Act, 11 March, 2024, https://corporateeurope.org/en/2024/03/trojan-horses-how-european-startups-teamed-big-tech-gut-ai-act; Corporate Europe Observatory, Big Tech lobby budgets hit record levels, 29 October 2025, https://corporateeurope.org/en/2025/10/big-tech-lobby-budgets-hit-record-levels;

Amnesty International is a movement of 10 million people which mobilizes the humanity in everyone and campaigns for change so we can all enjoy our human rights. Our vision is of a world where those in power keep their promises, respect international law and are held to account. We are independent of any government, political ideology, economic interest or religion and are funded mainly by our membership and individual donations. We believe that acting in solidarity and compassion with people everywhere can change our societies for the better.

Contact

info@amnesty.org

amnesty.org

facebook.com/AmnestyGlobal

@Amnesty

Amnesty International
Peter Benenson House
1 Easton Street
London WC1X 0DW, UK

Index: IOR 40/0484/2025
Publication: **November 2025**
Original language: **English**