Joint Statement: Pegasus in the European Parliament, the EU Must Act Now

On 3 July 2026, a forensic analysis by the Citizen Lab revealed that Stelios Kouloglou, former Member of the European Parliament and investigative journalist, was targeted and infected with Pegasus spyware, developed by NSO Group, on or around 21 October 2022, and again on 6 and 7 March 2023. At the time, Kouloglou was serving as a substitute Member of the Parliament's Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA Committee).

This revelation is especially alarming because of the specific institutional context in which the targeting occurred. A member of the very committee mandated to investigate spyware abuse in Europe was targeted during key moments of that inquiry, which raises grave concerns about the integrity of parliamentary oversight, the protection of independent institutions in line with separation of powers, and the ability of elected representatives to scrutinise state surveillance without intimidation or interference as part of a legitimate exercise of their duties.

While the Citizen Lab did not attribute the spyware attack to a particular government, they noted that there is no indication that the government of Greece, despite being connected to widespread spyware abuses with Predator spyware, was responsible for these attacks, or has ever been a Pegasus customer. Instead, their analysis suggests that a Pegasus customer previously investigated by the Citizen Lab and Access Now may be responsible for at least one of the infections. That customer was caught using Pegasus to hack exiled activists and journalists from Russia and Belarus. We are not aware of any evidence suggesting that either Russia or Belarus has been a Pegasus customer.

Nearly three years after the PEGA Committee adopted its report and recommendations, the European Union has failed to deliver a meaningful, EU-wide response to the proliferation and abuse of commercial spyware. Since then, the EU and Member States have been involved in repeated scandals: besides the spyware use against exiled journalists and activists in Latvia, Lithuania, and Poland; there was also the targeting of the President of the European Parliament with Predator spyware; the use of Graphite spyware in Italy against humanitarian workers and journalists; EU public money flowing to spyware companies; as well as a lack of enforcement of the dual-use regulation resulting in continued exports of surveillance technology from the EU to countries with serious records of human rights violations.

These incidents all point to a structural failure to adequately and seriously respond to the spyware crisis in Europe. This latest revelation should be treated as a rule of law emergency, threatening the very foundations of our society.

Europe cannot continue moving from scandal to scandal without consequence. The targeting of a Member of the European Parliament involved in investigating spyware abuse should mark a turning point. The EU must act now to defend independent oversight, protect fundamental rights, and ensure that spyware abuse in Europe is met with accountability, not impunity. We therefore call on:

- DG ITEC to conduct a full, independent, and impartial investigation into the hacking of Stelios Kouloglou to determine those responsible, establish all the relevant facts that led to the attacks, and launch an independent assessment of the full scope of the targeting of parliamentarians involved in oversight activities;
- The European Commission to urgently and publicly respond to the PEGA Committee recommendations, reporting on any implementation of said recommendations, identifying the gaps that remain, and setting out a roadmap for addressing the spyware crisis in the Union without further delays;
- Member States to guarantee effective remedies for victims, including access to evidence, independent investigations, notification where surveillance has occurred, and accountability for both state users and corporate actors; the European Commission should closely monitor the situation in that regard, ensuring compliance with EU legal standards, and use its enforcement powers against infringing Member States;
- The European Commission to strengthen enforcement of the EU Dual-Use Regulation and ensure that the upcoming evaluation of the Regulation fully reflects the findings of the PEGA Committee and subsequent spyware revelations; includes a comprehensive fundamental rights impact assessment; and is conducted with meaningful participation of civil society;
- Ensure that EU funds do not support companies involved in the development, sale, or deployment of spyware.

Signatories

- Access Now
- Alternatif Bilişim
- Amnesty International
- Asociația pentru Tehnologie și Internet – ApTI
- Balkan Free Media Initiative
- Centre for Democracy and Technology Europe
- Chaos Computer Club
- Civil Liberties Union for Europe (Liberties)
- Committee to Protect Journalists
- Data Rights
- Danes je nov dan, Inštitut za druga vprašanja
- Digitale Gesellschaft (Germany)
- epicenter.works – for digital rights
- European Centre for Press and Media Freedom (ECPMF)
- European Digital Rights (EDRi)
- European Federation of Journalists (EFJ) / Fédération européenne des journalistes (FEJ)
- First Department Human Rights Project
- Homo Digitalis
- Human Constanta
- Initiative für Netzfreiheit
- Irídia - Centre for the Defence of Human Rights
- IT-Pol Denmark
- Media Diversity Institute
- Osservatorio Nessuno OdV
- Panoptykon Foundation
- Privacy International
- Privacy Network
- Red Line for Gulf (RL4G)
- Reporters Without Borders (RSF)
- RESIDENT.NGO
- SHARE Foundation
- South East Europe Media Organisation (SEEMO)
- SMEX (Lebanon)

- WHAT TO FIX
- 7amleh – The Arab Center for the Advancement of Social Media

- Aleksei Fokin — Independent Threat Intelligence Researcher, FDC Threat Intelligence
- Prof Fionnuala Ni Aolain, KC, University of Minnesota Law School, Former UN Special Rapporteur Counter-Terrorism on Human Rights and Counter Terrorism
- Dmitrii Zair-Bek, Threat Intelligence Expert & Human Rights Defender