Human Rights Organizations Call for Robust Implementation of New EU Export Control Rules and Investigation of EU member states' role in Pegasus affair

September 2021

---

accessnow

AMNESTY INTERNATIONAL

RSF REPORTERS WITHOUT BORDERS

CPJ COMMITTEE TO PROTECT JOURNALISTS

HUMAN RIGHTS WATCH

Human Rights Organizations Call for Robust Implementation of New EU Export Control Rules and Investigation of EU member states' role in Pegasus affair

As new EU export controls come into force on 9 September with the recast Dual-Use Regulation[1], we, the undersigned organizations, call upon the European Commission as well as all 27 EU member states to follow up on their promise of creating a transparent market in cyber-surveillance technologies that is bound by effective human rights safeguards with immediate action.

The Pegasus Project's[2] revelations about the extent of human rights abuses committed and individuals targeted with the spyware in connection with their work as human rights defenders and journalists highlight the urgent need for effective international regulation of the sale, export, servicing, and use of digital technologies. The revelations highlight failures on many levels to prevent serious human rights violations through appropriate corporate due diligence, appropriate export controls and domestic safeguards in police and intelligence laws. But they also point to significant gaps in the EU's regulatory framework: The targeting of independent journalists in Hungary with NSO Group's Pegasus spyware and the potential targeting of lawyers and an opposition politician, gives rise to credible allegations that the government of Hungary, an EU member state, used phone surveillance technology. Together with the company's claims[3] that it held export licenses from Cyprus[4] and Bulgaria, and the lack of transparency around these licenses, these cases raise serious doubts about the EU's regulatory regime and respect for human rights.

We therefore call upon the European Commission to investigate the alleged abuse of digital surveillance technology by Hungarian authorities as well as whether any other EU member states have engaged in such abuses, and to determine and disclose whether any EU member states' authorities have granted licences for the export of NSO's Pegasus spyware**.** We place special emphasis on our call for a global moratorium on the sale, transfer, and use of digital surveillance technology until adequate human rights safeguards are in place, supported by more than 150 human rights organizations[5] as well as leading UN experts[6]. Long-term international policy reform is necessary, and until a binding legal framework is in place, this out-of-control trade should be halted.

In addition to these urgent actions, the Commission and all 27 member states should take steps to ensure effective implementation of the Recast Dual Use Regulation and to work toward further international reform.

---

[1] 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) PE/54/2020/REV/2

[2] Forbidden Stories 2021. Pegasus Project (last accessed on 6 September 2021)

[3] NSO Group 2021. Transparency and Responsibility Report (last accessed on 6 September 2021)

[4] Questions have been raised in the past about possible export licences granted by Cypriot authorities, e.g. by MEP Eva Kaili in October 2020, to which the Executive Vice-President Dombrovskis responded in January 2021. A current parliamentary priority question by MEP Sophia in t'Veld remains unanswered as of 6 September 2021

[5] Amnesty Int. et al. 2021. Joint open letter by civil society organizations and independent experts calling on states to implement an immediate moratorium on the sale, transfer and use of surveillance technology

[6] OHCHR 2021. Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech

Recommendations to the Commission regarding the implementation of the 2021 Dual Use Regulation

Ensure transparency of exports: The new Regulation establishes that the Commission shall publish an annual public report to the Parliament and Council detailing per member state the number of applications received for each type of surveillance technology, the issuing Member State and the destinations concerned. If implemented properly, this could prove the most important development within this reform toward a market in which companies are held accountable for their sales and in which civil society, researchers, and journalists can track exports and alert the authorities if further sales might pose serious risks to human rights. We remain concerned that the opacity in this industry, including around the possible issuing of NSO licenses from EU member states‘ authorities, enables the evasion of oversight and accountability, as has allegedly been the case so far in the matter of NSO’s European licences. Neither the companies nor states concerned should be allowed to withhold critical information under the pretext of business secrets or national security concerns. We highly recommend a more ambitious transparency regime including preferably monthly reports to counteract the risks attached to emerging technologies and a fast-moving market. These reports should at a minimum include the number of license applications per item, the exporter name, a description of the end user, destination, and intended use, government agency involved, the value of the license, and whether the license was granted or denied and why. Furthermore, transparency reporting should include information on companies’ processes to ensure proper implementation of their due diligence obligations to identify, prevent, and mitigate potential and actual negative impact on human rights.

Provide clarity on what is to be included in the definition of cyber-surveillance technology: The effectiveness of the new Regulation depends on a sufficiently broad interpretation of the term “cyber-surveillance technology”. We strongly recommend that the Commission ensure without delay that systems specially designed to perform biometric identification of natural persons for security purposes are subject to control within the EU control list and within the Wassenaar Arrangement in a transparent and consultative process and interpret these items to constitute “cyber-surveillance”

Ensure continuous information exchange with civil society experts: Effective implementation of the new regulation requires meaningful engagement with civil society, whose expertise is needed to identify potential human rights risks associated with the export of surveillance technology, informing the interpretation of the definition of “cyber-surveillance technology“, and other key components of the regulation. To date, the EU and member states‘ engagement with civil society has been mixed and on balance has not been sufficient, especially in the face of competing interests from the private sector.

Recommendations to EU member states going beyond the EU Dual-Use Regulation:

- Conduct an independent, impartial and transparent investigation into all alleged cases of targeted surveillance abuse;

- Ensure that there are effective mechanisms, including under member states' domestic laws, to investigate human rights violations involving surveillance technologies, and to hold those responsible to account;
- In light of the evident inadequacy of the Wassenaar arrangement, which EU export controls build on, and its limited membership, states should implement a binding legal framework, in consultation with relevant civil society stakeholders, to govern the export of surveillance technology with a focus on the prevention of human rights abuses. The export control regime should impose verifiable due diligence obligations for companies concerning potential and actual harm to human rights. It should include an effective reporting mechanism to ensure transparency and accountability toward the public, researchers, civil society, the media, and shareholders. The new framework ought to install an effective catch-all mechanism that would enable state authorities to intervene even where an emerging technology is not yet listed as a controlled good in order to keep pace with a fast-moving market; and
- Develop international standards on law enforcement, intelligence, and security force oversight that include domestic safeguards against disproportionate and arbitrary infringements of the rights to privacy and freedom of expression, including press freedom.

Signatories

Access Now

Amnesty International

Committee to Protect Journalists

Human Rights Watch

Reporters Without Borders (RSF)