Press release

08-05-2023 - 19:36
20230505IPR84901

European Parliament

Spyware: MEPs sound alarm on threat to democracy and demand reforms

- Spyware was used to monitor, intimidate and discredit opponents, journalists and civil society
- Spyware should only be allowed when strict conditions are fulfilled
- Uniform definition of national security needed
- An EU Tech Lab could help with research, investigations and forensic analysis

EP spyware inquiry committee has adopted its final report and recommendations, condemning spyware abuses in several EU member states and setting out a way forward.

On Monday evening, the European Parliament's Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA) adopted its final report and recommendations following a year-long inquiry into the abuse of spyware in the EU. MEPs condemn spyware abuses that aim to intimidate political opposition, silence critical media and manipulate elections. They note that EU governance structures cannot effectively deal with such attacks and say reforms are needed.

Systemic issues in Poland and Hungary

MEPs condemn major violations of EU law in Poland and Hungary, where the respective governments have dismantled independent oversight mechanisms. For Hungary, MEPs argue that the use of spyware has been "part of a calculated and strategic campaign to destroy media freedom and freedom of expression by the government." In Poland, the use of Pegasus has been part of "a system for the surveillance of the opposition and critics of the government -- designed to keep the ruling majority and the government in power".

To remedy the situation, MEPs call on Hungary and Poland to comply with European Court of Human Rights judgements and restore judicial independence and oversight bodies. They should also ensure independent and specific judicial authorisation before the deployment of spyware and judicial review afterwards, launch credible investigations into abuse cases, and ensure citizens have access to proper legal redress.

Concerns over spyware use in Greece and Spain

On Greece, MEPs say spyware use "does not seem to be part of an integral authoritarian strategy, but rather a tool used on an ad hoc basis for political and financial gains". Even though Greece has "a fairly robust legal framework in principle", legislative amendments have weakened safeguards. As a result, spyware has been used against journalists, politicians and businesspersons, and exported to countries with poor human rights records.

MEPs call on the government to "urgently restore and strengthen the institutional and legal safeguards", repeal export licences that are not in line with EU export control legislation, and respect the independence of the Hellenic Authority for Communication Security and Privacy (ADAE). They also note Cyprus has played a major role as an export hub for spyware, and should repeal all export licences it has issued that are not in line with EU legislation.

On Spain, MEPs found that the country "has an independent justice system with sufficient safeguards", but some questions on spyware use remain. Noting that the government is already working to address shortcomings, MEPs call on authorities to ensure "full, fair and effective" investigations, especially into the 47 cases where it is unclear who authorised the deployment of spyware, and to make sure targets have real legal remedies.

Stronger regulation needed to prevent abuse

To stop illicit spyware practices immediately, MEPs consider spyware should only be used in member states where allegations of spyware abuse have been thoroughly investigated, national legislation is in line with recommendations of the Venice Commission and EU Court of Justice and European Court of Human Rights case law, Europol is involved in investigations, and export licences not in line with export control rules have been repealed. By December 2023, the Commission should assess whether these conditions have been fulfilled in a public report.

MEPs want EU rules on the use of spyware by law enforcement, which should only be authorised in exceptional cases for a pre-defined purpose and a limited time. They argue that data falling under lawyer-client privilege or belonging to politicians, doctors or the media should be shielded from surveillance, unless there is evidence of criminal activity. MEPs also propose mandatory notifications for targeted people and for non-targeted people whose data was accessed as part of someone else's surveillance, independent oversight after it has happened, meaningful legal remedies for targets, and standards for the admissibility of evidence collected using spyware.

MEPs also call for a common legal definition of the use of national security as grounds for surveillance, in order to prevent attempts to justify manifest abuses.

EU Tech Lab and a boost to vulnerability research

To help uncover illicit surveillance, MEPs propose the creation of an EU Tech Lab, an independent research institute with powers to investigate surveillance, provide legal and technological support including device screening, and perform forensic research. They also want new laws to regulate the discovery, sharing, resolution and exploitation of vulnerabilities.

Foreign policy dimension

On third countries and the EU's foreign policy instruments, MEPs would like to see an in-depth investigation of spyware export licences, stronger enforcement of the EU's export control rules, a joint EU-US spyware strategy, talks with Israel and other third countries to establish rules on spyware marketing and exportation, and ensuring EU development aid does not support acquisition and use of spyware.

Quotes

After the vote, Committee Chair Jeroen Lenaers (EPP, NL) said: "Our inquiry has made it clear that spyware has been used to violate fundamental rights and endanger democracy in several EU member states, Poland and Hungary being the most blatant cases. Spyware use must always be proportionate and authorised by an independent judiciary, which unfortunately is not the case in some parts of Europe. Stricter EU-level scrutiny is needed to ensure that spyware use is the exception, to investigate serious crimes, and not the norm. Because we acknowledge that it can – when used in a controlled manner – be an important tool to combat crimes like terrorism. Our committee has formulated a wide range of proposals to regulate the use of spyware, while respecting national security competences. Now the Commission and member states should do their part and transpose our recommendations into concrete legislation to protect the rights of citizens."

Rapporteur Sophie In 't Veld (Renew, NL) added: "Today, the committee of inquiry concludes its work. This does not mean that the work of this Parliament is finished. Not one victim of spyware abuse has been awarded justice. Not one government has really been held accountable. The member states and the European Commission should not sleep easy, because I intend to keep on this case until justice is being done. The unimpeded use of commercial spyware without proper judicial oversight poses a threat to European democracy, as long as there is no accountability. Digital tools have empowered us all in various ways, but they have made governments far more powerful. We have to close that gap."

On ***Tuesday 9 May from 14.30 CEST***, Mr Lenaers and Ms In 't Veld will hold a press conference in the Daphne Caruana Galizia press room in Strasbourg. The event will be streamed here, and journalists can connect to ask questions via Interactio.

Procedure and next steps

MEPs adopted a report, detailing the findings of the inquiry, with 30 votes in favour, 3 against, and 4 abstaining, and a text outlining recommendations for the future with 30 votes in favour, 5 against, and 2 abstaining. The latter text is expected to be voted by the full Parliament during the plenary session starting 12 June.

Further information

Draft texts and amendments tabled in committee
Studies ordered by the committee
The mandate of the committee of inquiry
Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware

Contacts

Janne OJAMO
Press Officer
(+32) 2 284 12 50 (BXL)
(+32) 470 89 21 92
janne.ojamo@europarl.europa.eu
pega-press@europarl.europa.eu
@EP_PegaInquiry