

EP Recommendation on Lessons Learned from Misused Spyware

Thomas Wahl



News

On 15 June 2023, the plenary of the European Parliament adopted a [recommendation that outlines reforms to curb spyware abuse](#). The recommendation backs the conclusions of the one-year investigations by the "[Committee of Inquiry](#) to investigate the use of Pegasus and equivalent surveillance spyware" (PEGA).

The PEGA Committee was set up by the EP in March 2022 (→ [euCRIM 1/2022, 13](#)) after it became known that the Pegasus software (developed by the Israeli cyber-arms company NSO Group) was being used in over 50 countries to surveil journalists, human rights activists, lawyers, and politicians. The Committee was mandated to investigate alleged infringement or maladministration in application of EU law in relation to the use of Pegasus and equivalent spyware surveillance software. In particular, it gathered information on the extent to which Member States or third countries are using intrusive surveillance thus violating the rights and freedoms enshrined in the Charter of Fundamental Rights of the EU.

In the final EP recommendation, appeals were made to all EU institutions and Member States. In particular, MEPs stated that the illicit use of spyware has put "democracy itself at stake". They called for credible investigations, legislative changes and better enforcement of existing rules to tackle abuse. The recommendation also contains explicit calls on Poland, Hungary, Greece, Spain and Cyprus, whose governments were involved in the misuse, to scrutinize contraventions and maladministration.

Furthermore, the EP called for strict regulations of the trade in and use of spyware and sets conditions for the Member States on the continued use of the software. In particular, the use of spyware by law enforcement should only be authorised in exceptional cases for a pre-defined purpose and a limited time. Data falling under lawyer-client privilege or belonging to politicians, doctors or the media should be sheltered from surveillance (unless there is evidence of criminal activity). In addition, the enforcement of existing legal standards must be improved and the concept of "national security" must be defined in order to avoid abusive justification of spying.

With regard to the external policy dimension, MEPs demand, *inter alia*, an in-depth review of spyware export licences, stronger enforcement of the EU's export control rules, and a joint EU-US spyware strategy.

In order to raise awareness and accountability in the EU, MEPs propose the creation of an independently run European interdisciplinary research institute (EU Tech Lab). This institute should be tasked with discovering and exposing the unlawful use of software for illicit surveillance purposes, providing accessible and free legal and technological support, performing forensic analytical research for judicial investigations and reporting regularly on the use and misuse of spyware in the EU.

AUTHOR

Thomas Wahl

Senior Researcher
Max Planck Institute for the
Study of Crime, Security and
Law

ISSN: 1862-6947
<https://euCRIM.eu>



The recommendation has been submitted to the European Commission with the request to initiate legislative proposals on the based of this recommendation.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and “criministrative” law.

All news items are freely accessible at: <https://eucrim.eu/news/>

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.

The project is co-financed by the Union Anti-Fraud Programme (UAFB), managed by the European Anti-Fraud Office (OLAF).



**Co-funded by
the European Union**