Recommendation to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware

2023/2500(RSP) - 15/06/2023 - Text adopted by Parliament, single reading

The European Parliament adopted by 411 votes to 97, with 37 abstentions, a recommendation to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware.

Parliament highlighted the undeniable importance of the protection of privacy, the right to dignity, private and family life, freedom of expression and information, freedom of assembly and association, and the right to a fair trial. It stressed that breaches of these fundamental rights and freedoms are key in terms of respect for the common legal principles set out in the Treaties and that democracy itself is at stake, as the use of spyware on politicians, civil society and journalists has a chilling effect and severely affects the right to peaceful assembly, freedom of expression and public participation.

The resolution strongly condemned the use of spyware by Member State governments and members of government authorities or state institutions for the purpose of monitoring, blackmailing, intimidating, manipulating and discrediting opposition members, critics and civil society, eliminating democratic scrutiny and the free press, manipulating elections and undermining the rule of law by targeting judges, prosecutors and lawyers for political purposes.

Lack of response to attacks

Parliament noted the fundamental inadequacy of the current Union governance structure to respond to attacks on democracy, fundamental rights and the rule of law from within the Union, and the lack of action taken by many Member States. It is also concerned at the apparent reticence to investigate spyware abuse, both in cases where the suspect is a Member State or a non-EU country government body.

The legal framework of some Member States does not provide precise, effective and comprehensive safeguards on the ordering and execution of and the potential redress mechanisms against surveillance measures.

Parliament regretted the failure of Member State governments, the Council and the Commission to fully cooperate with the inquiry and to share all relevant and meaningful information, in order to help the committee of inquiry to fulfil its tasks, as stated in its mandate. They concluded that neither the Member States, nor the Council, nor the Commission seemed to be at all interested in maximising their efforts to fully investigate the spyware abuse, thus knowingly protecting Union governments which violate human rights within and outside of the Union.

Contraventions and maladministration in the implementation of Union law have taken place in Poland, Hungary, Greece, Spain and Cyprus

Parliament called on Hungary and Poland to comply with European Court of Human Rights judgements and restore judicial independence and oversight bodies. The two countries should also ensure independent and specific judicial authorisation before deploying spyware, launch credible investigations into abuse cases, and guarantee that citizens have access to meaningful legal remedies.

The Greek government is asked 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.

Noting that Cyprus has served as an export hub for spyware, Parliament stated that it should repeal all export licences not aligned with EU legislation. Spanish authorities should ensure full, fair and effective investigations, especially into the 47 cases where it is unclear who authorised the deployment of spyware. The Spanish authorities should also ensure that targeted people have real legal remedies, according to the recommendation.

Rules to prevent abuse

While fighting serious crime and terrorism is critically important for Member States, the protection of fundamental rights and democracy is essential. Parliament stressed that the use of spyware by Member States must be proportionate, must not be arbitrary, and surveillance must only be authorised in narrowly, pre-determined circumstances.

Owing to the transnational and EU dimension of the use of spyware, coordinated and transparent scrutiny at EU level is necessary to ensure not only the protection of EU citizens but also the validity of evidence gathered by way of spyware in cross-border cases, and that there is a clear need for common EU standards regulating the use of spyware by Member State bodies.

The recommendation stressed that spyware may only be placed on the market for sale to and use by public authorities, based on a closed list, whose instructions include investigations of crimes or the protection of national security for which the use of spyware may be authorised.

Security agencies should only use spyware when all recommendations laid out by the Fundamental Rights Agency have been implemented.

Parliament concluded that when a Member State has purchased spyware, the acquisition must be auditable by an independent, impartial audit body with appropriate clearance. The Commission is urged to conduct a full-blown inquiry into all allegations and suspicions of the use of spyware against its officials, and report to Parliament and to the responsible law enforcement authorities where necessary.

International cooperation to protect citizens

Parliament called for a joint EU-US spyware strategy, including a joint whitelist and/or blacklist of spyware vendors whose tools have been abused or are at risk of being abused to maliciously target government officials, journalists and civil society, and who operate against the security and foreign policy of the Union, by foreign governments with poor human rights records, (not) authorised to sell to public authorities, common criteria for vendors to be included on either list, arrangements for common EU-US reporting on the industry, common scrutiny, common due diligence obligations for vendors and the criminalisation of the sale of spyware to non-state actors.

e-Privacy

The recommendation called for the protection of all electronic communications, content and metadata against the abuse of personal data and private communications by private companies and government authorities. Parliament pointed out that digital safety-by-design tools such as end-to-end encryption should not be weakened.

The Commission should assess the Member States' implementation of the e-Privacy Directive across the EU, and to start infringement procedures where violations occur.

EU Tech Lab

The Commission is called on to initiate, without delay, the creation of an independently run European interdisciplinary research institute, with a focus on research and development at the nexus of information and communication technology, fundamental rights and security. The lab should be set up in close cooperation with the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU) and ENISA. Adequate funding should be secured and the Commission is recommended to put forward a certification scheme for the analysis and authentication of forensic material.

Legislative action

The Commission should promptly come forward with legislative proposals on the basis of this recommendation.