Investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware

2022/2077(INI) - 23/05/2023 - Committee report tabled for plenary, single reading

The Committee of Inquiry into the use of Pegasus and equivalent surveillance spyware adopted the report by Sophia IN 'T VELD (Renew, NL) on the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware.

In July 2021, the Pegasus Project, a collective of investigative journalists, NGOs and researchers, published a report based on a list in its possession of around 50 000 telephone numbers that may have been targeted using Pegasus spyware. Pegasus spyware has been widely used by both authoritarian and democratic governments around the world, with or without judicial oversight, to target journalists, lawyers, judges, activists, politicians and state officials. This raises concerns at various levels of the EU legal order with respect to data protection and privacy, freedom of expression, freedom of the press, freedom of association, redress mechanisms, legal remedy and fair trial, and democratic processes and institutions.

In response to this growing scandal, the European Parliament decided on 10 March 2022 to set up a committee of inquiry.

For the purposes of the inquiry, the PEGA Committee has used a broad approach as to what constitutes spyware, namely surveillance spyware that is installed on mobile devices by exploiting IT vulnerabilities.

Some Member States have deployed spyware and refused to comment on it by invoking national security, which, according to Article 4(2) of the Treaty on European Union (TEU), "remains the exclusive competence of each EU Member State". However, **the case law of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECHR)** makes it clear that national security considerations must be reconciled with the fundamental rights and democratic norms embedded in EU law. **The lack of a clear definition of national security** and the excessively broad interpretation of its scope by national authorities make it difficult to understand the justifications for the use of spyware.

Since the revelations of Pegasus Project, the United States has taken a number of steps to investigate and regulate these practices. In the EU, very few measures have been taken to date. Members believe that **clear rules must be adopted** to regulate the use and marketing of spyware, preferably in partnership with other countries such as the United States.

Europe's business

Although it is not officially confirmed, it can be assumed that all EU Member States have purchased one or more commercial spyware products. One company alone, NSO Group, has sold its products to twenty-two end-users in no fewer than fourteen Member States, among which are Poland, Hungary, Spain, The Netherlands and Belgium. In at least four Member States, **Poland, Hungary, Greece, and Spain**, there has been illegitimate use of spyware, and there are suspicions about its use in Cyprus. Two Member

States, Cyprus and Bulgaria, serve as the export hub for spyware. One Member State, Ireland, offers favourable fiscal arrangements to a large spyware vendor, and one Member State, Luxemburg, is a banking hub for many players in the spyware industry.

Members condemned major violations of EU law in Poland and Hungary, where the respective governments have dismantled independent oversight mechanisms.

They also expressed concern about the use of spyware in Greece and Spain.

EU's capacity to respond

The report noted that some governments have used powerful, highly invasive and intrusive spyware against EU citizens, abusing their right to use surveillance where there is a risk to national security. This jeopardises democracy, the rule of law and citizens' fundamental rights.

The EU has **few means of countering these threats** and is ill-equipped to fight potential criminal activities by national authorities, even if they harm the EU itself.

Members pointed out that the Commission considers that addressing transgressions of EU law is the sole responsibility of national authorities. When faced with flagrant violations of the rule of law and fundamental rights, this stance – which has no basis in the EU Treaties – becomes very problematic. Although subsidiarity and division of competences are a pillar of EU law, **these should not lead to impunity for governments** targeting EU citizens with spyware for political purposes.

In response to the spyware scandal, the Commission initially wrote letters seeking clarification from the governments of Poland, Hungary, Spain, Greece, Cyprus and France. It would appear, however, that the Commission's warning was not followed up by further action. While it is true that the Commission has no powers to act in the area of national security, **'national security' should not be interpreted as an unlimited carve out from European laws and Treaties** and become an area of lawlessness. It is up to the Member States, however, to 'demonstrate that national security would be compromised in the case at issue'.

On 21 December 2022, the Commission sent a general letter to all Member States to "map the situation in the Member States". The Commission asked specific questions concerning, among other things, the purpose of using spyware, the authorities authorised to deploy it, the national definition of national security, legislation governing the processing of data for national security purposes, safeguards, prior authorisation by a court or an independent administrative authority, oversight and notifications.

On 28 March 2023, Commissioner Reynders told the PEGA that a large majority of the Member States had replied, but that the Commission was still in the process of collecting the Member State responses to this mapping exercise, and that it would 'carefully assess' the replies. Based on this mapping exercise, the **Commission will reflect on its options regarding the use of spyware in Member States**. However, no specific end date is envisaged for the Commission's assessment, 'given the evolving and sensitive nature of the assessment'. The Commission also mentioned that it would follow the findings of PEGA very closely.

Members considered that Parliament, the Commission and the Council have **the power and the duty to legislate, regulate and enforce**, and they must do so with vigour and ambition, putting the defence of EU democracy above short-term political considerations.

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.