DECISIONS

DECISION (EU) 2022/480 OF THE EUROPEAN PARLIAMENT

of 10 March 2022

on setting up a committee of inquiry to investigate the use of the Pegasus and equivalent surveillance spyware, and defining the subject of the inquiry, as well as the responsibilities, numerical strength and term of office of the committee

The European Parliament,

— having regard to the request presented by 290 Members for a committee of inquiry to be set up to look into and investigate alleged contraventions, or maladministration in implementation of Union law as regards the use of the Pegasus and equivalent surveillance spyware that is installed on mobile devices by exploiting IT vulnerabilities ('equivalent surveillance spyware'),

— having regard to the proposal from the Conference of Presidents,

— having regard to Article 226 of the Treaty on the Functioning of the European Union (TFEU),

— having regard to Decision 95/167/EC, Euratom, ECSC of the European Parliament, the Council and the Commission of 19 April 1995 on the detailed provisions governing the exercise of the European Parliament's right of inquiry ([1]),

— having regard to the European Union's attachment to the values and principles of liberty, democracy and respect for human rights and fundamental freedoms and of the rule of law as outlined in the preamble to the Treaty on European Union (TEU) and notably in Articles 2, 6 and 21 of that Treaty,

— having regard to Article 4(2) TEU, which reaffirms Member States' exclusive competence in maintaining law and order and safeguarding national security,

— having regard to Articles 16 and 223 TFEU,

— having regard to the Charter of Fundamental Rights of the European Union (the 'Charter'), and in particular Articles 7, 8, 11, 21 and 47 thereof, that recognise the specific rights, freedoms and principles set out in it, such as respect for private and family life and the protection of personal data, freedom of expression and information, right to non-discrimination, as well as the right to effective remedy and fair trial, and which fully apply to Member States when they are implementing Union law, and Article 52(1) thereof that allows for certain limitation on the exercise of fundamental rights and freedoms,

— having regard to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) ([2]),

— having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ([3]),

— having regard to Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA ([4]),

([1]) OJ L 113, 19.5.1995, p. 1.
([2]) OJ L 201, 31.7.2002, p. 37.
([3]) OJ L 119, 4.5.2016, p. 1.
([4]) OJ L 119, 4.5.2016, p. 89.

— having regard to Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States ([5]) as amended by Council Decision (CFSP) 2021/796 of 17 May 2021 ([6]),

— having regard to 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 ([7]),

— having regard to the Act concerning the election of the members of the European Parliament by direct universal suffrage ([8]),

— having regard to the European Convention for the Protection of Human Rights and Fundamental Freedoms, and in particular Articles 8, 9, 13 and 17 thereof, and the Protocols to that Convention,

— having regard to the United Nations Guiding Principles on Business and Human Rights ([9]),

— having regard to its resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs ([10]) and to its recommendations regarding the strengthening of IT security in the EU's institutions, bodies and agencies,

— having regard to Rule 208 of its Rules of Procedure,

A. whereas there have been recent revelations that several countries, including Member States, have used the Pegasus surveillance spyware against journalists, politicians, law enforcement officials, diplomats, lawyers, business people, civil society actors and other actors, and that such practices are extremely alarming and appear to confirm the dangers of the misuse of surveillance technology to undermine human rights and democracy;

1. Decides to set up a committee of inquiry to investigate alleged contraventions, or maladministration in the implementation, of Union law as regards the use of the Pegasus and equivalent surveillance spyware, without prejudice to the jurisdiction of national or Union courts;

2. Decides that the committee of inquiry shall:

— investigate the scope of alleged contraventions, or maladministration in the implementation, of Union law, resulting from the use of the Pegasus and equivalent surveillance spyware, collect information on the extent to which Member States, including but not limited to Hungary and Poland, or third countries use intrusive surveillance in a way that violates the rights and freedoms enshrined in the Charter, as well as assess the level of risk this poses to the values enshrined in Article 2 TEU, such as democracy, the rule of law and respect for human rights;

— for the performance of its duties, collect and analyse information to ascertain:

— the use and the functioning of the Pegasus and equivalent surveillance spyware and its alleged negative impact on fundamental rights under the Charter, in cases where Member States were implementing Union law;

— the existing legal framework in which Member States have acquired and used the Pegasus and equivalent surveillance spyware;

— whether Member States' authorities have used the Pegasus and equivalent surveillance spyware for political, economic or other unjustified purposes to spy on journalists, politicians, law enforcement officials, diplomats, lawyers, business people, civil society actors or other actors, in violation of Union law and of the values enshrined in Article 2 TEU, or the rights enshrined in the Charter;

([5]) OJ L 129 I, 17.5.2019, p. 13.
([6]) OJ L 174 I, 18.5.2021, p. 1.
([7]) OJ L 206, 11.6.2021, p. 1.
([8]) OJ L 278, 8.10.1976, p. 5.
([9]) https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf
([10]) OJ C 378, 9.11.2017, p. 104.

— whether the use, in contravention of Union law, of the Pegasus and equivalent surveillance spyware had an adverse impact on democratic processes in the Member States concerning elections on local, national and European levels;

— the alleged contraventions or maladministration by Member States, resulting from the use of the Pegasus and equivalent surveillance spyware, of Directive 2002/58/EC, in particular regarding the principle of confidentiality of communications and the prohibition of listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data of persons;

— whether the use of the Pegasus and equivalent surveillance spyware by Member States have constituted, resulted in or revealed violations of Directive (EU) 2016/680 and Regulation (EU) 2016/679;

— whether the Commission had evidence of the use of the Pegasus and equivalent surveillance spyware against persons;

— whether the Member States have ensured sufficient institutional and legal safeguards to avoid the illegal use of spyware, and whether persons who suspect that their rights have been violated by the use of spyware have access to effective remedy;

— the alleged failure of Member States to act in respect of the involvement of entities in the EU in the development, dissemination, or financing of the Pegasus and equivalent surveillance spyware, including the supply chain in terms of technology and its exploitation, in so far as it is in breach of Union law, including Regulation (EU) 2021/821, and including where surveillance software marketed for a certain purpose (e.g. fight against terrorism) is used in another context;

— the role of the government of Israel and of other third countries in supplying the Pegasus and equivalent surveillance spyware to Member States;

— whether the use of the Pegasus or equivalent surveillance spyware by Member State authorities has resulted in the transfer of personal data to third countries, in particular but not limited to it, to the NSO Group, as well as to third countries' governments;

— whether the use of the Pegasus or equivalent surveillance spyware, directly or indirectly involving entities linked to the EU, contributed to illegal spying on journalists, politicians, law enforcement officials, diplomats, lawyers, business people, civil society actors or other actors in third countries and whether it led to human rights violations or abuses that are of serious concern as regards the objectives of the EU's common foreign and security policy, and whether such use was in contravention of the values enshrined in Article 21 TEU and in the Charter, also with due regard to the United Nations Guiding Principles on Business and Human Rights and other rights enshrined in international human rights law;

— whether there were sufficient grounds for the Council to adopt restrictive measures or sanctions in the framework of the EU common foreign and security policy against one or more third countries where a decision, adopted in accordance with Chapter 2 of Title V TEU provided for the interruption or reduction of economic or financial relation, in accordance with Article 215(1) TFEU;

— whether the use of the Pegasus or equivalent surveillance spyware by third countries had an impact on fundamental rights ensured under Union law and whether, there were sufficient grounds for the Council to reassess any international cooperation agreements in the Area of Freedom, Security and Justice concluded with third countries pursuant to Article 218 TFEU;

— make any recommendations that it deems necessary in this matter;

— make recommendations for protecting EU institutions and its Members and staff against such surveillance spyware;

3. Decides that the committee of inquiry shall submit its final report within 12 months of the adoption of this decision;
4. Decides that the committee of inquiry should take account in its work of any relevant developments within the remit of the committee that emerge during its term;
5. Underlines that in order to ensure good cooperation and information flow between the committee of inquiry and the relevant standing committees and sub-committees, the Chair and the Rapporteur of the committee of inquiry could be involved in relevant debates of the standing committees and sub-committees, and vice versa, in particular for hearings of the committee of inquiry;
6. Decides that any recommendations drawn up by the committee of inquiry should be referred to the relevant standing committees and subcommittees in their respective fields of competences as defined by Annex VI to the Rules of Procedure;
7. Decides that the committee of inquiry shall have 38 members;
8. Instructs its President to arrange for publication of this decision in the *Official Journal of the European Union*.