European Parliament
2019-2024

Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware

B9-0000/2023

4.1.2023

EUROPEAN PARLIAMENT DRAFT RECOMMENDATION TO THE COUNCIL AND THE COMMISSION

pursuant to Rule 208(12) of the Rules of Procedure

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

Sophie in ‘t Veld
on behalf of the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware

B9-0000/2023

European Parliament draft 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[1] (2023/2500(RSP))

The European Parliament,

– having regard to the Treaty on European Union (TEU) and in particular Articles 2, 4, 6 and 21 thereof,

– having regard to Articles 16, 223, 225 and 226 of the Treaty on the Functioning of the European Union (TFEU),

– having regard to the Charter of Fundamental Rights of the European Union (the 'Charter'), and in particular Articles 7, 8, 11, 17, 21 and 47 thereof,

– 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],

– 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[5],

– 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[6]

[1] The draft report is based on the document where the rapporteur set out her findings. Any person named in the course of the inquiry to whom this might prove prejudicial has the right to be heard by the Committee. The Secretariat may be reached at pega-secretariat@europarl.europa.eu.
[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.
[5] OJ L 206, 11.6.2021, p. 1.
[6] OJ L 129 I, 17.5.2019, p. 13.

as amended by Council Decision (CFSP) 2021/796 of 17 May 2021[7],

– having regard to the Act concerning the election of the Members of the European Parliament by direct universal suffrage[8],

– 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[9],

– having regard to the Charter of the United Nations and the United Nations Guiding Principles on Business and Human Rights[10],

– 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 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[11] and to its recommendations regarding the strengthening of IT security in the EU's institutions, bodies and agencies,

– having regard to the Venice Commission report concerning the democratic oversight of the security services[12] and the Opinion on the Act of 15 January 2016 Amending the Police Act and Certain Other Acts[13],

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

A. whereas it has been revealed that government bodies in several countries, both Member States and third countries, have used Pegasus and other brands of surveillance spyware against journalists, politicians, law enforcement officials, diplomats, lawyers, business people, civil society actors and other actors, for political and even criminal purposes; whereas such practices are extremely alarming and underscore the risk of abuse of surveillance technologies to undermine human rights and democracy;

B. whereas in the early days of mobile communication, eavesdropping was conducted through the interception of calls and, later, of text messages in their plain format;

C. whereas the arrival of encrypted mobile communication applications led to the emergence of the spyware industry exploring existing vulnerabilities in smartphones' operative systems to install software used to import spyware into the phone, including through 'zero-click', enabling the extraction of data before encryption;

[7] OJ L 174 I, 18.5.2021, p. 1.
[8] OJ L 278, 8.10.1976, p. 5.
[9] OJ L 113, 19.5.1995, p. 1.
[10] https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.
[11] OJ C 378, 9.11.2017, p. 104.
[12] https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)010-e.
[13] https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)012-e.

D. whereas the use of spyware surveillance should remain the exception and always subject to an effective and meaningful *ex ante* judicial authorisation by an impartial and independent judicial authority, which must ensure that the measure is necessary and proportionate and strictly limited to cases affecting national security, terrorism and serious crime;

E. whereas any spyware surveillance must be scrutinised by an independent *ex post* oversight authority, which must ensure that any authorised surveillance is carried out in compliance with fundamental rights and in accordance with the conditions set out by the Court of Justice of the European Union (CJEU), the European Court of Human Rights (ECtHR) and the Venice Commission and must be able to terminate the surveillance if it is not;

F. whereas spyware surveillance failing to meet the requirements set out in Union law and the jurisprudence of the CJEU and the ECtHR would entail a violation of the values enshrined in Article 2 TEU and the fundamental rights enshrined in the Charter and, in particular, Articles 7, 8, 11, 17, 21 and 47 thereof that recognise the specific rights, freedoms and principles set out in it, such as respect for private and family life, the protection of personal data, freedom of expression and information, right to property, right to non-discrimination, as well as the right to effective remedy and fair trial;

G. whereas the rights of targeted persons are laid down in the Charter of Fundamental Rights and international conventions, notably the right to privacy and the right to a fair trial, and in Union rules on the rights of suspects and accused;

H. whereas it results from the testimonies of victims that even if legal remedy and civil rights may exist on paper, they mostly become void in the face of obstruction by government bodies, the absence of implementation of the right to be informed for victims and the administrative burden to prove the status as victim;

I. whereas the Polish government has weakened and eliminated institutional and legal safeguards including proper oversight and scrutiny procedures, effectively leaving victims without any meaningful remedy; whereas the Pegasus surveillance spyware has been illegally deployed to spy on journalists, politicians, prosecutors and civil society actors for political purposes;

J. whereas the Hungarian government has weakened and eliminated institutional and legal safeguards including proper oversight and scrutiny procedures, effectively leaving victims without any meaningful remedy; whereas the Pegasus surveillance spyware has been illegally deployed to spy on journalists, politicians, prosecutors and civil society actors for political purposes;

K. whereas Greek Members of Parliament, opposition as well as Nea Demokratia (ND) MPs, ND party loyalists and journalists have been targeted with Predator spyware, the use of which is illegal under Greek law; whereas many of the persons targeted were also under official surveillance by the EYP Greek secret service; whereas the Greek government denies having purchased or used Predator, but it is highly probable that Predator has been used by or on behalf of persons very close to the Prime Minister’s office; whereas the Greek government admitted it has granted export licences to Intellexa for the sale of the Predator spyware to repressive governments; whereas the

government has responded to the scandal with legislative amendments that further reduce the rights of the target to be informed after surveillance has taken place;

L. whereas revelations showed two categories of spyware targets in Spain; whereas the first includes the Prime Minister and the Minister of Defence that are believed to be spied upon by Morocco; whereas the second concerns some 65 victims referred to as 'CatalanGate' including Catalan parliamentarians, Members of Parliament, lawyers and civil society actors; whereas the Spanish authorities admitted in May 2020 to targeting 18 of those 65 victims with court authorisation, however, they have refrained from providing further information, invoking national security;

M. whereas there are allegations of the Cyprus government party spying on critics, but so far no spyware infections have been detected; whereas Cyprus is an important European export hub for the surveillance industry and an attractive location for companies selling surveillance technologies;

N. whereas there are strong indications of among others the governments of Morocco and Ruanda targeting Union citizens with spyware, including the President of France, the Prime Minister and Defence Minister of Spain, the then Prime Minister of Belgium, the former President of the Commission and former Prime Minister of Italy, and the daughter of Paul Rusesabagina;

O. whereas it can be safely assumed that all Member States have purchased or used one or more spyware systems; whereas most governments will refrain from illegitimate use of spyware, but in the absence of a solid legal framework including safeguards and oversight, the risk of abuse is very high;

P. whereas the Member State governments and Member State parliaments have not provided Parliament with meaningful information about the legal frameworks governing the use of spyware in their Member States beyond what was already publicly known, despite an obligation to do so pursuant to Article 3, paragraph 4 of the Decision of the European Parliament, the Council and the Commission of 6 March 1995 on the detailed provisions governing the exercise of the European Parliament's right of inquiry; whereas it is difficult to assess the enforcement of Union legislation and the safeguards, oversight, and means of redress which prevents the adequate protection of citizen's fundamental rights;

Q. whereas several key figures from the spyware industry have acquired Maltese citizenship in order to be able to operate freely within and from the Union;

R. whereas different spyware vendors are or have been registered in one or more Member States; whereas examples include NSO Group with corporate presence in Luxembourg, Cyprus, the Netherlands and Bulgaria, the parent company of Intellexa, Thalestris Limited, in Ireland, Greece, Switzerland and Cyprus, DSIRF in Austria, Amesys and Nexa Technologies in France, Tykelab and RCS Lab in Italy, and FinFisher (now defunct) in Germany;

S. whereas all Member States but Cyprus are participating in the Wassenaar Arrangement for controlling conventional arms and dual-use goods and technologies;

T. whereas Israel's export regime[14] applies in principle to all Israeli citizens, even when operating from the EU; whereas Israel is not a participating country in the Wassenaar Arrangement but claims to apply its standards nevertheless;

U. whereas the export of spyware from the Union to third countries is regulated in the Dual-use Regulation, which was revised in 2021; whereas the Commission issued a first implementation report in September 2022[15];

V. whereas spyware producers exporting to third countries establish themselves within the Union to gain respectability while trading in spyware to totalitarian regimes; whereas exports from the Union to totalitarian regimes or non-state actors are taking place, in violation of the EU export rules on surveillance technologies;

W. whereas Amesys and Nexa Technologies are currently being prosecuted in France for exporting surveillance technology to Libya, Egypt, and Saudi Arabia; whereas Intellexa companies based in Greece reportedly exported their products to Bangladesh, Sudan, Madagascar and at least one Arab country, FinFisher's software is being used by dozens of countries all over the world, including Angola, Bahrain, Bangladesh, Egypt, Ethiopia, Gabon, Jordan, Kazakhstan, Myanmar, Oman, Qatar, Saudi Arabia, Turkey and Morocco's intelligence services have been accused of using Pegasus spyware against journalists and politicians by Amnesty and Forbidden Stories; whereas it is unknown if export licences were granted for the export of spyware to all these countries;

X. whereas the number of attendees at arms fairs and ISSWorld marketing spyware capabilities demonstrates the prevalence of third country providers of spyware and related products and services, a significant number of which are headquartered in Israel (e.g. NSO Group, Wintego, Quadream and Cellebrite), and reveals prominent producers in India (ClearTrail), the United Kingdom (BAe Systems and Black Cube) and the United Arab Emirates (DarkMatter), while the United States Entity List blacklisting spyware producers located in Israel (NSO Group and Candiru), Russia (Positive Technologies) and Singapore (Computer Security Initiative Consultancy PTE LTD.) further highlights the diversity of origin among spyware producers; whereas the fair is also attended by a wide range of European public authorities, including local police forces;

Y. whereas Member States claim that matters relating to national security fall outside of the Treaties as Article 4 (2) TEU provides that national security remains the sole responsibility of the Member States;

Z. whereas however, the CJEU has ruled (C-623/17) that 'although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law';

AA. whereas the CJEU has ruled (C-203/15) that 'Article 15(1) of Directive 2002/58/EC of

[14] Defense Export Control Law 5766-2007, Israeli Ministry of Defence.
[15] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A434%3AFIN&qid=1662029750223.

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), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication';

AB. whereas the CJEU has ruled (C-203/15) that 'Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union';

AC. whereas the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), recently modernised as Convention 108+, applies to processing of personal data for State (national) security purposes, including defence and all Member States are parties to this convention;

AD. whereas use of surveillance spyware for the prevention, investigation, detection or prosecution of criminal offences and the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, falls within the scope of EU law;

AE. whereas the Charter lays down the conditions for the limitation of the exercise of fundamental rights: it must be provided for by law, respect the essence of the rights and freedoms concerned, be subject to the principle of proportionality, and only be imposed if it is necessary and genuinely meets objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others; whereas in the case of the use of spyware the level of interference with the right to privacy is so severe that the individual is in fact deprived of it and the use cannot be considered proportionate, irrespective of whether the measure can be deemed necessary to achieve the legitimate objectives of a democratic state;

AF. whereas the e-Privacy Directive provides that Member States must ensure the confidentiality of communications; whereas the deployment of surveillance tools constitutes a restriction of the right to protection of terminal equipment afforded by the e-Privacy Directive; whereas this would place national laws on spyware within the scope of the e-Privacy Directive similar to national data retention laws; whereas regular deployment of intrusive spyware technology would not be compatible with the Union legal order;

AG. whereas a state under international law only has the right to investigate potential crimes

within its jurisdiction and has to resort to the assistance of other states where the investigation has to take place in other states unless there is a basis for conducting investigations in the other jurisdiction due to an international agreement, or in the case of Member States, in Union law;

AH. whereas the infection of a device with spyware and the subsequent collection of data takes place through the servers of the mobile service provider, and as the free roaming within the Union has resulted in persons more often having mobile contracts from other Member States than the one in which they live, a legal base for the collection of data in the other Member State through the use of spyware is currently absent in Union law;

AI. whereas Member States must comply with Directive 2014/24/EU and Directive 2009/81/EC on public and defence procurement, respectively, adequately justify derogation under Article 346(1)(b) of the TFEU, as the 2009 Directive explicitly takes into account the sensitive characteristics of defence procurement and observe the WTO Agreement on Government Procurement, as amended 30 March 2012[16] (GPA) if party to it;

AJ. whereas it has been reported that large financial institutions have tried to incite spyware producers to refrain from applying appropriate human rights standards and due diligence and continue selling spyware to totalitarian regimes;

AK. whereas Israel participates in Union research programmes since 2000; whereas funds have been made available to Israeli military and security companies through these European Programmes;

AL. whereas the main legislative instrument within the Union development policies is Regulation (EU) 2021/947 - the 'Global Europe Regulation'[17], and Union funding may be provided through the types of financing envisaged by the Financial Regulation, even to the extent that assistance could be suspended in the event of degradation in democracy, human rights or the rule of law in third countries;

1. Highlights the undeniable importance of protection of privacy and the right to dignity and private life in an increasingly digital world where more and more of our activities take place online;

2. Takes the firm position that breaches of the right to dignity, privacy and private life is not only a question of respect for the common legal principles set out in the Treaties and in other sources but a fundamental question of whether future human life will be free and democratic or controlled by digital processes;

3. Strongly condemns the use of spyware by Member State governments or members of government for the purpose of monitoring, blackmailing, intimidating, manipulating and discrediting opposition and critics, eliminating democratic scrutiny and free press, and manipulating elections;

4. Points out that this illegitimate use of spyware by national governments directly and

[16] https://www.wto.org/english/tratop_e/gproc_e/gpa_1994_e.htm.
[17] https://eur-lex.europa.eu/eli/reg/2021/947/oj#ntc11-L_2021209EN.01000101-E0011.

indirectly affects the Union institutions and the decision making process, thus undermining the integrity of European Union democracy;

5. Notes with grave concern the fundamental inadequacy of the current Union governance structure to respond to attacks on democracy from within the Union;

6. Takes the firm position that the export of spyware from the Union to dictatorships and oppressive regimes with poor human-right records where such tools are used against human rights activists, journalist and government critics is a severe violation of fundamental rights enshrined in the Charter and a gross violation on Union export rules;

7. Is of the opinion that contraventions, or maladministration in the implementation of Union law with regard to the use of, and trade in spyware, have taken place in Poland, Hungary, Greece, Spain and Cyprus;

8. Expresses furthermore concern about the use of, and trade in spyware by other Member States, who collectively nurture the Union as a safe haven for the spyware industry, often in violation of Union laws and standards;

9. Is furthermore of the view that government parties of third countries have targeted high profile personalities in the Union with spyware;

10. Is equally concerned at the apparent reticence to investigate the spyware attacks, both if the suspect is a Union or third country government body; notes the very slow progress and lack of transparency in the judicial investigations into spyware attacks on government leaders and ministers of EU Member States;

11. Condemns the refusal of Member State governments, the Council and the Commission, to fully cooperate with the inquiry and to share all relevant and meaningful information; considers the collective reply by the Council wholly inadequate and contrary to the principle of loyal cooperation;

12. Concludes that no Member State, nor the Council, nor the Commission has any desire to shed light on the spyware scandal, thus knowingly protecting Union governments who violate human rights within and outside of the Union;

13. Concludes that contraventions and maladministration in the implementation of Union law have taken place in Poland;

14. Calls on Poland to:

    (a) urgently restore sufficient institutional and legal safeguards, including effective *ex ante* and *ex post* scrutiny as well as independent oversight mechanisms;

    (b) comply with the ruling of the Constitutional Tribunal on the 1990 Police act;

    (c) comply with the opinion of the Venice Commission on the 2016 Police act;

    (d) comply with the various judgements of the ECtHR, like the judgement of the *Roman Zakharov v. Russia* case in 2015 that underlines the necessity for strict surveillance criteria, proper judicial authorisation and oversight, the immediate

destruction of irrelevant data, judicial scrutiny over urgency procedures and a requirement for the notification of victims as well as the judgement in the *Klass and others v. Germany* case in 1978 that outlines that surveillance must be of sufficient importance to necessitate such an invasion of privacy;

(e) withdraw Article 168a of the rewritten Act Amending the Code of Criminal Procedure of 2016;

(f) restore full independence of the judiciary and all relevant oversight bodies, such as the Ombudsman and the Data Protection Authorities, to ensure all oversight bodies get full cooperation and access to information and to provide full information to all victims;

(g) urgently install the random allocation of cases to the judges of the courts for every application that is submitted, even on the weekend and outside of normal business hours to avoid the selection of 'friendly judges' by the secret services;

(h) reinstate the traditional system of parliamentary oversight wherein the opposition party takes on the Chairmanship of the Parliamentary Oversight Committee for the Special Services (KSS);

(i) urge the Polish prosecutor to launch inquiries into the abuse of spyware;

(j) implement the Whistleblowers Directive;

(k) invite Europol to investigate all cases of alleged abuse of spyware;

15. Concludes that contraventions and maladministration in the implementation of Union law have taken place in Hungary;

16. Calls on Hungary to:

(a) urgently restore sufficient institutional and legal safeguards, including effective *ex ante* and *ex post* scrutiny as well as independent oversight mechanisms;

(b) comply with the various judgements of the ECtHR, like the judgement in the *Klass and others v. Germany* case in 1978 that outlines the requirement for the notification of surveillance subjects;

(c) reinstate independent oversight bodies in line with the judgement of the ECtHR in the case of *Hüttl v. Hungary* wherein the court states that the NAIH are incapable of conducting independent oversight of the use of spyware given that the secret services are entitled to deny access to certain documents on the basis of secrecy;

(d) restore full independence of the judiciary and all relevant oversight bodies, such as the Ombudsman and the Data Protection Authorities, to ensure all oversight bodies get full cooperation and access to information and to provide full information to all victims;

(e) reinstate independent employees into leading roles in oversight bodies such as

the Constitutional Court, the Supreme Court, the Court of Auditors, the prosecution service, the National Bank of Hungary and the National Election Committee;

(f) invite Europol to investigate all cases of alleged abuse of spyware;

17. Concludes that contraventions and maladministration in the implementation of Union law have taken place in Greece;

18. Calls on Greece to:

(a) urgently restore and strengthen the institutional and legal safeguards, including effective *ex ante* and *ex post* scrutiny as well as independent oversight mechanisms;

(b) urgently repeal all export licences that are not fully in line with the Dual-Use Regulation and investigate the allegations of illegal exports, among others to Sudan;

(c) ensure that the authorities can freely and unhindered investigate all allegations of the use of spyware;

(d) urgently withdraw Amendment 826/145 of Law 2472/1997, which abolished the ability of the ADAE to notify citizens of the lifting of the confidentiality of communications;

(e) restore full independence of the judiciary and all relevant oversight bodies, such as the Ombudsman and the Data Protection Authorities, to ensure all oversight bodies get full cooperation and access to information and to provide full information to all victims;

(f) reverse the legislative amendment of 2019 that placed the EYP under the direct control of the Prime Minister;

(g) urgently implement the Whistleblowers Directive;

(h) ensure the independence of the EAD leadership;

(i) urgently launch a police investigation following the alleged abuse of spyware and seize physical evidence of proxies, broker companies and spyware vendors that are linked to the spyware infections;

(j) invite Europol to immediately join the investigations;

19. Concludes that although the regulatory framework in Spain seems to be in line with the requirements set by the Treaties and by judgements by the CJEU and the ECtHR, the factual implementation raises questions, as Members of Parliament have been targeted and that lawyers, politicians, activists and journalists were targeted when there was no criminal charge or evident imminent threat to national security;

20. Calls on the government of Spain to:

(a) provide full clarity on all alleged cases of the use of spyware

(b) ensure real and meaningful legal remedy for all victims, and for judicial inquiries to be concluded without delay;

(c) urgently resolve the ongoing crisis in the judiciary;

21. Concludes that contraventions and maladministration in the implementation of Union law are likely to have taken place in Cyprus;

22. Calls on the government of Cyprus to:

(a) thoroughly assess all export licences issued for spyware and repeal them where appropriate;

(b) release the report of the special investigator on the 'Spyware Van' case;

(c) fully investigate, with the assistance of Europol, all allegations of illegitimate use of spyware, notably on journalists, lawyers and civil society actors;

23. Is of the view that the situation in other Member States is also reason for concern, in particular given the presence of a lucrative and expanding spyware industry benefiting from the good reputation, the single market and free movement of the Union, enabling Member States like Cyprus and Bulgaria to become an export hub for spyware to undemocratic regimes around the world;

24. Is of the opinion that the failure or refusal of national authorities to ensure the proper protection for the citizens of the Union, demonstrates with all necessary clarity that action at Union level is indispensable to ensure that the letter of the Treaties is upheld and that Union legislation is respected, so that the rights of citizens to human dignity, private life, personal data and property is respected;

25. Concludes that contraventions and maladministration in the implementation of Union law has been committed by the Commission and the European External Action Service (EEAS) when providing support to third countries, including but not limited to 10 such countries in the Sahel, to enable them to develop surveillance capabilities;

26. Calls on the Commission and the EEAS to:

(a) immediately halt any support to third countries aimed at to enabling them to develop surveillance capabilities or that otherwise facilitate such development;

(b) develop an appropriate human and fundamental rights impact assessment procedure that fully takes into account Article 51 of the Charter of Fundamental Rights;

(c) present the human and fundamental rights impact assessment procedure to Parliament and the Council;

(d) carry out the human and fundamental rights impact assessment;

(e) discontinue any support to third countries aimed at to enabling them to develop surveillance capabilities or that otherwise facilitate such development if the respect for human and fundamental rights, including rule of law, protection for democratic principles, politicians, human rights defenders and journalists cannot be guaranteed;

27. Takes the position that the trade in, and use of spyware needs to be regulated strictly; recognising however, that the legislative process will take considerable time, calls for the immediate adoption of a conditional moratorium on the sale, acquisition, transfer and use of spyware, that must be lifted on a country-by-country basis if the following conditions have been met:

(a) all cases of alleged abuse of spyware are fully investigated and resolved without delay by the appropriate law enforcement, prosecutorial and judicial authorities; and

(b) proof that the framework governing the use of spyware is in line with the standards laid down by the Venice Commission and relevant case-law by the CJEU and ECtHR; and

(c) the explicit commitment to grant any request by Europol pursuant to Art 6(1a) of the Europol Regulation relating to investigations into allegations of illegitimate use of spyware; and

(d) repealing all export licences that are not fully in line with both the letter and the spirit of the Dual-Use Regulation;

28. Considers that the fulfilment of the conditions must be assessed by the Commission;

29. Considers that there is a clear need for common EU standards regulating the use of spyware by Member State bodies, drawing from standards laid down by the CJEU, ECtHR and the Venice Commission; considers that such EU standards should cover at least the following elements:

(a) the envisaged use of spyware must be subject to an effective and meaningful *ex ante* judicial authorisation by an impartial and independent judicial authority, having access to all relevant information, demonstrating the necessity and proportionality of the envisaged measure;

(b) the targeting with spyware should only last as long as is strictly necessary, the judicial authorisation beforehand should define the precise scope and duration and the hacking may only be extended when further judicial authorisation is granted for another specified duration, given the nature of spyware and the possibility of retroactive surveillance;

(c) the authorisation for the use of spyware may only be granted with respect to investigations into a limited and closed list of crimes, and spyware may only be used towards persons in relation to which there is sufficient indications that they have committed or are planning to commit such crimes;

(d) there should be a non-exhaustive but binding list of privileged and sensitive professions, such as lawyers, journalists, politicians, and doctors that may not be targeted by spyware;

(e) specific rules must be drawn up for surveillance with spyware technology given that it allows for unlimited retroactive access to messages, files and metadata;

(f) Member States should publish, as a minimum, the number of requests for surveillance approved and rejected, and the type and purpose of the investigation and anonymously register each investigation in a national register with a unique identifier so that it can be investigated in case of suspicions of abuse;

(g) the right of notification for the targeted citizen: after the surveillance has ended, the authorities should notify the citizen of the fact that they were subject to the use of spyware by the authorities, including information regarding the date and duration of the surveillance, the warrant issued for the surveillance operation, data obtained, information on how that data has been used and by which actors as well as the date of deletion of the data; notes that such notification should be done without undue delay, unless an independent judicial authority grants delay of notification, in which case immediate notification would seriously jeopardise the purpose of the surveillance;

(h) an effective and independent *ex post* oversight over the use of spyware which must have all required means and powers to exercise a meaningful oversight and be coupled with a parliamentary oversight based on cross-party membership and full access to information;

(i) a meaningful legal remedy for direct and indirect targets and that individuals who claim to be adversely affected by surveillance should have access to redress through an independent body; calls, therefore, for the introduction of a duty of notification for state authorities, including appropriate timeframes for notification, whereby delivery occurs once the security threat has passed;

(j) legal remedies must be effective in both law and fact and that they must be known and accessible; stresses that such remedies require swift, thorough and impartial investigation by an independent oversight body and that this body should have access, expertise and technical capabilities to handle all relevant data to be able to determine whether the security assessment made by the authorities of an individual is reliable and proportionate;

(k) the need to improve victims' free of charge access to technological expertise at this stage, since increased availability and affordability of technological processes, such as forensic analysis, would allow victims to present stronger cases in court;

(l) during surveillance, authorities should delete all irrelevant data and after the surveillance and the investigation for which the authorisation was granted has ended, authorities should delete the data as well as any related documents, such

as notes that were taken during that period, such deletion must be recorded, and be auditable;

(m) Member States must notify each other in case of surveillance of citizens or residents of another Member State or of a mobile number of a carrier in another Member State;

30. Emphasises that only spyware that is configured so that it enables and facilitates the functionality of spyware according to the legislative framework according to Article 82 TFEU and in particular supporting the different roles of the authorities involved may be placed on the internal market, developed or used in the Union;

31. Stresses that spyware may only be placed on the market for sale to and use by a closed list of public authorities whose instructions include investigations of crimes for which the use of spyware may be authorised;

32. Highlights the obligation to use a version of spyware that is programmed in such a way that it minimises the access to data, that the spyware should not have access to all data stored on a device, but should be programmed in such a way that it limits access to data to the minimum of what is strictly necessary;

33. Concludes that when a Member State has purchased spyware, the acquisition must be auditable to an independent, impartial audit body;

34. Stresses that all entities placing spyware on the internal market should comply with strict due diligence requirements, including vetting of potential clients and should report to the Commission on an annual basis on compliance;

Need for a definition of national security

35. Condemns the invocation of 'national security' as pretext for the abuse of spyware and for absolute secrecy and lack of accountability; welcomes the Commission statement that a mere reference to national security cannot be interpreted as being an unlimited carve out from the normal rules and calls on the Commission to follow up on that statement in the cases where there is manifest abuse;

36. Calls for a common legal definition of national security, laying down criteria to determine what legal regime applies in matters of national security as well as a clear demarcation of the area where such a special regime may apply;

37. Considers that the use of spyware constitutes a limitation of fundamental rights; recalls that the Charter of Fundamental Rights provides that any limitation to fundamental rights according to Article 52(1) must be set out in law; considers therefore that it is necessary to define 'national security';

Better enforcement of existing legislation

38. Underlines the shortcomings in national legal frameworks and the necessity for better enforcement of existing Union legislation to counterpose these deficiencies; identifies the following Union laws as relevant but improperly enforced: the Anti-Money

Laundering Directive, procurement rules, Dual-use Regulation, case-law (rulings on surveillance and national security), and the Whistleblower Directive; calls on the Commission to investigate and report on the shortcomings in implementation and enforcement and put forward a roadmap to correct them by summer 2023 at the latest;

39. Considers the strict implementation and enforcement of the Union legal framework on data protection, especially the Law Enforcement Directive, General Data Protection Regulation and e-Privacy Directive, a critical prerequisite; considers equally important the full implementation of the relevant CJEU judgements, which is still lacking in several Member States, in which the Commission has a central role in enforcing EU law and ensuring its uniform application throughout the Union;

40. Calls for the Wassenaar Arrangement to become a binding agreement on all its participants, with the aim of making it an international treaty;

41. Calls for Cyprus to become a participating state of the Wassenaar Arrangement, reminds the Council, the Member States and the Commission that all efforts must be made to enable Cyprus to join the Wassenaar Arrangement;

42. Stresses that the Wassenaar Arrangement should include a human rights framework that embeds the licensing of spyware technologies, assesses and reviews the compliance of companies producing spyware technologies and that participants should prohibit the purchase of surveillance technologies from states that are not part of the Arrangement;

43. Stresses that in light of the spyware revelations, the Commission should conduct an in-depth investigation of export licences granted for the use of spyware under the Dual-use Regulation;

44. Emphasises that the Commission needs to regularly check and properly enforce the Recast Dual-use Regulation to avoid ‘export regime shopping’ throughout the Union, as is currently the case in Bulgaria and Cyprus, and that the Commission should have adequate resources for this task;

45. Calls for amendments to the Dual-use Regulation to clarify in Article 15 that export permits of dual-use goods must not be given where goods are or may be intended for in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law;

46. Calls for changes to the Dual-use Regulation to ensure that transit is prohibited in cases where goods are or may be intended for internal repression and/or the commission of serious violations of human rights and international humanitarian law;

47. Stresses that, in a future amendment of the Dual-use Regulation, designated national authorities responsible for the approval and denial of export licences for dual-use items should provide detailed reports including information on the dual-use item in question; the number of licences applied for, the name of the exporting country, a description of the export company and whether this company is a subsidiary; a description of the end user and destination; the value of the export licence; why the export licence was approved or denied; emphasises that these reports should be made public on a quarterly basis; calls for the set up of a dedicated standing parliamentary committee with access

to classified information by the Commission, for the purpose of parliamentary oversight;

48. Stresses that, in a future amendment of the Dual-use Regulation, the exception to the requirement to provide information to the Commission on grounds of commercial sensitivity, defence and foreign policy or national security reasons must be abolished; considers instead that in order to prevent sensitive information becoming available to third countries, the Commission can decide to classify certain information in its annual report;

49. Stresses that the definition of cyber-surveillance items in the recast Dual-use Regulation cannot be given a restrictive interpretation but should include all technologies in this area, such as mobile telecommunications interception or jamming equipment; intrusion software; IP network communications surveillance systems or equipment; software specially designed or modified for monitoring or analysis by law enforcement; laser acoustic detection equipment; forensic tools which extract raw data from a computing or communications device and circumvent 'authentication' or authorisation controls of the device; electronic systems or equipment, designed either for surveillance and monitoring of the electro-magnetic spectrum for military intelligence or security purpose; and Unmanned Aerial Vehicles capable of conducting surveillance;

50. Calls for additional European legislation that requires corporate actors producing and/or exporting surveillance technologies to include human rights and due diligence frameworks in line with the UN Guiding Principles on Business and Human Rights (UNGPs);

International cooperation to protect citizens

51. Calls for a joint EU-US spyware strategy, including a joint white list and/or black list of spyware vendors (not) authorised to sell to public authorities, common criteria for vendors to be included in either list, arrangement 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;

52. Calls for the EU-US Trade and Technology Council to hold wide and open consultation with civil society for the development of the joint EU-US strategy and standards;

53. Calls for talks to be launched with other countries, in particular Israel, to establish a framework for spyware marketing and export licences, including rules on transparency, a list of eligible countries and due diligence arrangements;

54. Emphasises that compared to the US, where NSO was quickly black-listed and there are bipartisan initiatives for legislation on commercial spyware, no action has been taken in the Union as regards the imports of spyware and the enforcement of the exports rules is wholly inadequate;

55. Concludes that the Union export rules and their enforcement must be given sharp teeth for the protection of human rights of in third countries, and that the EU should seek to join forces with the US and other allies in regulating the trade in spyware and using their combined market power to force change;

Zero-day vulnerabilities

56. Calls for a regulation of the discovery, sharing, patching and exploitation of vulnerabilities, without prejudice to the NIS2 Directive and the proposal for the Cyber Resilience Act;

57. Considers that researchers must be able to research vulnerabilities, and share their results without civil and criminal liability under inter alia the Cybercrime Directive and the Copyright Directive;

58. Calls upon the major industry players to create incentives for researchers to participate in vulnerability research, by investing in vulnerability treatment plans, disclosure practices within the industry and with civil society and run bug bounty programmes;

59. Calls for a ban on commercial trade in vulnerabilities, and an obligation to disclose the findings of vulnerability research so they can be patched;

60. Calls upon organisations to create a publicly available contact point where vulnerabilities can be disclosed in a standardised way and for organisations that receive information about vulnerabilities in their system to act immediately to fix; calls for a maximum period to patch disclosed vulnerabilities after disclosure;

61. calls for a ban for public authorities to purchase, keep open or stockpile vulnerabilities, except only in limited, specified cases with clear vulnerability equity processes, set in law, with necessity/proportionality test for the decision to disclose or exceptionally withhold a vulnerability, and strict rules on delaying notification, subject to strict oversight by an independent supervising body;

Telecom networks

62. Stresses that, if any state actor has an access point to the SS7 network, the licence of the main operator through which the state actor has access, should be revoked;

63. Stresses that the current unlimited possibility for unknown individuals to buy any number for any country in the world available should be better regulated to make malicious activity more difficult to hide;

64. calls on Telecom providers to take firm and demonstrable action against spoofing;

e-Privacy

65. Calls for the rapid adoption of the e-Privacy Regulation in a way that fully reflects the case-law on the restrictions for national security and the need to prevent abuse of surveillance technologies, strengthens the fundamental right to privacy; points out that the scope for surveillance should not go beyond the e-Privacy Directive;

The role of Europol

66. Expresses its dismay at the refusal of Europol to make full use of its newly acquired powers under Regulation (EU) 2022/991, enabling it to propose to competent authorities of the Member States concerned to initiate, conduct or coordinate a criminal

investigation, especially when the national authorities are unable or unwilling to investigate, and in particular when there is a justified concern that evidence may be destroyed;

67. Calls on all Member States to commit to granting the proposals of Europol under the aforementioned article;

68. Calls on Europol to set up a register of law enforcement operations involving the use of spyware within Europol, wherein each operation should be identified with a code and for the use of spyware by governments to be included in the annual Internet Organised Crime Threat Assessment report by Europol;

69. Calls for the revision of the Europol Regulation, so that in exceptional cases Europol can also start a criminal investigation without Member State consent, in cases where the national authorities fail or refuse to investigate and there are clear threats to the interests and security of the EU;

Union development aid

70. Calls on the Commission to implement more rigorous control mechanisms to ensure that Union development aid does not fund or facilitate tools that could impinge on the principles of democracy, good governance, the rule of law and respect for human rights; notes that the Commission's assessments of compliance with Union law, in particular the Financial Regulation, should contain specific control criteria and enforcement mechanisms to prevent such abuses;

Union financial regulations

71. Highlights that respect for human rights by the financial sector must be enhanced; stresses that the UNGPs 10+ recommendations must be transposed into Union law and that the Due Diligence Directive should fully apply to the financial sector, to ensure respect for democracy, human rights and the rule of law in the financial sector;

Follow-up of Parliament resolutions

72. Calls for the urgent follow-up of Parliaments 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; stresses that the following recommendations need to be carried out as a matter of urgency;

73. Stresses that, despite the fact that oversight of intelligence services' activities should be based on both democratic legitimacy (strong legal framework, *ex ante* authorisation and *ex post* verification) and adequate technical capability and expertise, the majority of current EU and US oversight bodies dramatically lack both, in particular the technical capabilities;

74. Calls, as it did in the case of Echelon, on all national parliaments which have not yet done so to install meaningful oversight of intelligence activities by parliamentarians or expert bodies with legal powers to investigate; calls on the national parliaments to

ensure that such oversight committees/bodies have sufficient resources, technical expertise and legal means, including the right to conduct on-site visits, to be able to effectively control intelligence services;

75. Calls for the setting up of a High-Level Group to propose, in a transparent manner and in collaboration with parliaments, recommendations and further steps to be taken for enhanced democratic oversight, including parliamentary oversight, of intelligence services and increased oversight collaboration in the EU, in particular as regards its cross-border dimension;

76. Considers this High-Level group should:

(a) define minimum European standards or guidelines on the *ex ante* and *ex post* oversight of the intelligence services on the basis of existing best practices and recommendations by international bodies, such as the UN and the Council of Europe, including the issue of oversight bodies being considered as a third party under the 'third party rule', or the principle of 'originator control', on the oversight and accountability of intelligence from foreign countries;

(b) set strict limits on the duration and scope of any surveillance ordered unless its continuation is duly justified by the authorising/oversight authority; recalls that the duration of any surveillance ordered should be proportionate and limited to its specific purpose;

(c) develop criteria on enhanced transparency, built on the general principle of access to information and the so-called Tshwane Principles[18];

77. Intends to organise a conference with national oversight bodies, whether parliamentary or independent;

78. Calls on the Member States to draw on best practices so as to improve access by their oversight bodies to information on intelligence activities (including classified information and information from other services) and establish the power to conduct on-site visits, a robust set of powers of interrogation, adequate resources and technical expertise, strict independence vis-à-vis their respective governments, and a reporting obligation to their respective parliaments;

79. Calls on the Member States to develop cooperation among oversight bodies, in particular within the European Network of National Intelligence Reviewers (ENNIR);

80. Calls on the Commission to present, a proposal for a Union security clearance procedure for all office holders in the Union, as the current system, which relies on the security clearance undertaken by the Member State of citizenship, provides for different requirements and lengths of procedures within national systems, thus leading to differing treatment of Members of Parliament and their staff depending on their nationality;

81. Recalls the provisions of the inter-institutional agreement between the European

[18] The Global Principles on National Security and the Right to Information, June 2013.

Parliament and the Council concerning the forwarding to and handling by Parliament of classified information held by the Council on matters other than those in the area of the common foreign and security policy, which should be used to improve oversight at EU level;

Union research programmes

82. Calls for the implementation of more rigorous control mechanisms to ensure that Union research funds do not fund or facilitate tools that infringe on EU values; notes that assessments of compliance with Union law should contain specific control criteria to prevent such abuses;

A Union Tech Lab

83. Calls on the Commission to initiate without delay the creation of an independent European interdisciplinary institute, with a focus on research and development at the nexus of information and communication technology, fundamental rights and security, which will also be tasked with discovering and exposing the unlawful use of software for illicit surveillance purposes;

Rule of law

84. Stresses that the impact of the illegitimate use of spyware is much more pronounced in Member States where authorities that would usually be tasked with investigating and providing redress to victims, are captured by the state and that where a rule of law crisis exists, the national authorities cannot be relied upon;

85. Calls therefore on the Commission to ensure a proactive implementation of its Rule of Law toolbox, particularly by:

(a) putting in place a more comprehensive monitoring of the Rule of Law, including assessing the responsiveness of State institutions to provide redress to victims of spyware, in particular to journalists, and by broadening the scope of its annual Rule of Law report and include all challenges to Democracy, the Rule of Law and Fundamental Rights as included in Article 2 TEU, as repeatedly asked for by Parliament;

(b) proactively pursuing and bundling infringement procedures against Member States for Rule of Law deficiencies such as threats to the independence of the judiciary and the effective functioning of the police and prosecutorial service; and

(c) broadening the Commission assessment for the purpose of the Rule of Law budget conditionality regime, in particular by looking at the impacts of the use of spyware on the accountability of public spending;

Union litigation fund

86. Calls for the establishment, without undue delay, of a Union Litigation Fund to cover the actual litigation costs and enable the victims of spyware to seek adequate redress in

line with the Preparatory Action adopted by Parliament in 2017, to create an ‘EU fund for financial support for litigating cases relating to violations of democracy, rule of law and fundamental rights’;

European Council, Council of ministers and Commission

87. Expresses concern over the lack of action by the Commission so far, and urges it to make full use of all its powers as guardian of the Treaties, and to conduct a comprehensive and in-depth investigation into the abuse of and trade in spyware in the Union;

88. Urges the Commission 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;

89. Notes that the PEGA Committee received a collective reply from the Council to the queries of the European Parliament to all individuals Member States only on the eve of the publication of the draft report, approximately 4 months after the letters of the EP; expresses dismay at the lack of action of the European Council and Council of ministers, and calls for a dedicated European Council Summit, given the magnitude of the threat to democracy in Europe;

90. Takes the position that Parliament should have full powers of inquiry, including the power to summon witnesses, to formally require witnesses to testify under oath and to provide requested information within specific deadlines;

91. Resolves to adopt a protocol for cases where members or staff of the House have become the direct or indirect target of spyware and underlines that all cases must be reported to the responsible law enforcement authorities;

92. resolves to take the initiative to launch an inter-institutional conference wherein Parliament, the Council and the Commission must aim for governance reforms that strengthen the Union institutional capacity to respond adequately to attacks on democracy and rule of law from the inside and to ensure that the Union has effective supranational methods for enforcing the Treaties and secondary law in the case of non-compliance by Member States;

Legislative action

93. Calls on the Commission to come forward with legislative proposals on the basis of this Recommendation;

°

° °

94. Instructs its President to forward this resolution to the Member States, the Council, the Commission and to Europol.