European Parliament
2019-2024

TEXTS ADOPTED

P9_TA(2023)0244

Investigation of the use of Pegasus and equivalent surveillance spyware (Recommendation)

European Parliament recommendation of 15 June 2023 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))

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, 41, 42 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)[1] ('e-Privacy Directive'),

– 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)[2],

– 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[3],

---

1 OJ L 201, 31.7.2002, p. 37.
2 OJ L 119, 4.5.2016, p. 1.
3 OJ L 119, 4.5.2016, p. 89.

– having regard to Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA[1] ('Cybercrime Directive'),

– 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[2] ('Dual-Use Regulation'),

– 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[3] as amended by Council Decision (CFSP) 2021/796 of 17 May 2021[4],

– having regard to the Act concerning the election of the Members of the European Parliament by direct universal suffrage[5],

– having regard to Decision 95/167/EC, Euratom, ECSC 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[6],

– having regard to 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[7],

– having regard to Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/139/EC and 2013/36/EU[8] ('Anti-Money Laundering Directive'),

– having regard to the proposal for a regulation of the European Parliament and the Council of 16 September 2022 establishing a common framework for media services in the internal market (European Media Freedom Act) and amending Directive 2010/13/EU (COM(2022)0457),

– having regard to Article 12 of the Universal Declaration of Human Rights,

– having regard to the judgment of the Court of Justice of the European Union (CJEU) in case C-37/20[9] on the anti-money-laundering directive on the provision whereby the information on the beneficial ownership of companies incorporated within the territory of the Member States is accessible in all cases to any member of the general public is

---

1 OJ L 218, 14.8.2013, p. 8.
2 OJ L 206, 11.6.2021, p. 1.
3 OJ L 129 I, 17.5.2019, p. 13.
4 OJ L 174 I, 18.5.2021, p. 1.
5 OJ L 278, 8.10.1976, p. 5.
6 OJ L 113, 19.5.1995, p. 1.
7 OJ L 98, 25.3.2022, p. 72.
8 OJ L 156, 19.6.2018, p. 43.
9 Judgment of the Court (Grand Chamber) of 22 November 2022, C-37/20, *WM* and *Sovim SA* v *Luxembourg Business Registers*, ECLI:EU:C:2022:912.

ruled invalid,

– having regard to Article 17 of the International Covenant on Civil and Political Rights,

– having regard to the Charter of the United Nations and the United Nations Guiding Principles on Business and Human Rights[1],

– having regard to the statement of UN High Commissioner for Human Rights Michelle Bachelet of 19 July 2022 entitled 'Use of spyware to surveil journalists and human rights defenders',

– having regard to the comment of Council of Europe Commissioner for Human Rights Dunja Mijatovic of 27 January 2023 entitled 'Highly intrusive spyware threatens the essence of human rights'[2],

– having regard to the European Data Protection Supervisor's (EDPS) Preliminary Remarks on Modern Spyware of 15 February 2022[3],

– having regard to the European Convention for the Protection of Human Rights and Fundamental Freedoms, and in particular Articles 8, 10, 13, 14 and 17 thereof and the protocols to that Convention,

– having regard to Europol's 2021 Serious and Organised Crime Threat Assessment (SOCTA) entitled 'A Corrupting Influence: the Infiltration and Undermining of Europe's Economy and Society by Organised Crime',

– having regard to the 2017 European Union Agency for Fundamental Rights (FRA) report entitled 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU', and to the updates presented on 28 February 2023 to the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA),

– 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[4] and in particular to the recommendations contained therein on strengthening IT security in the EU's institutions, bodies and agencies,

– having regard to EDPS opinion 24/2022 of 11 November 2022 on the European Media Freedom Act,

– having regard to the glossary on malware and spyware drawn up by the European Union Agency for Cybersecurity (ENISA),

– having regard to the European Ombudsman's Decision on how the European

---

1 https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

2 https://www.coe.int/en/web/commissioner/-/highly-intrusive-spyware-threatens-the-essence-of-human-rights

3 https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf

4 OJ C 378, 9.11.2017, p. 104.

Commission assessed the human rights impact before providing support to African countries to develop surveillance capabilities (case 1904/2021/MHZ),

– having regard to the statement 2 February 2023 by Ms Irene Kahn, UN Special Rapporteur on freedom of opinion and expression and Mr Fernand de Varennes, UN Special Rapporteur on minority issues demanding an investigation into the alleged spying programme targeting Catalan leaders[1],

– having regard to the report on by the European Commission for Democracy through Law (Venice Commission) on the democratic oversight of the security services[2] and to its opinion entitled 'Poland - Opinion on the Act of 15 January 2016 amending the Police Act and Certain Other Acts'[3],

– having regard to the report of the Committee of Inquiry to investigate the use of the Pegasus and equivalent surveillance spyware (A9-0189/2023),

– having regard to Rule 208(12) of its Rules of Procedure,

A. whereas, thanks to the efforts of CitizenLab and Amnesty Tech and numerous investigative journalists, it has been revealed that government bodies in several countries, both EU Member States and non-EU countries, have used Pegasus and equivalent 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 demonstrate the risk of abuse of surveillance technologies to undermine fundamental human rights, democracy and electoral processes;

B. whereas whenever the term 'spyware' is mentioned in the report, it means 'Pegasus and equivalent surveillance spyware' as defined in Parliament's Decision to set up the PEGA Committee;

C. whereas it has been observed that state actors have deliberately used spyware in a misleading manner by using spyware that can disguise itself as legitimate program, file or content ('Trojan horse'), such as fake messages from public institutions; whereas in some cases public authorities have used phone operators to transmit malicious content to the targeted person's device; whereas spyware can be deployed by exploiting zero-day vulnerabilities without the interaction of the target with infected content, can remove all traces of its presence after uninstallation and can anonymise the link between remote operators and server;

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

E. whereas the emergence of encrypted mobile communication applications led to the emergence of the spyware industry exploiting existing vulnerabilities in smartphone

---

1 https://www.ohchr.org/en/press-releases/2023/02/spain-un-experts-demand-investigation-alleged-spying-programme-targeting

2 https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)010-e

3 https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)012-e

operating systems to install software that imports spyware into the phone, including through ‘zero-click’ infections without the user’s knowledge or any action by the user, enabling the extraction of data before encryption; whereas such zero-click spyware, by its very design, makes effective and meaningful scrutiny of its use very difficult;

F. whereas knowledge about vulnerabilities in software systems is traded directly between parties, or is facilitated by brokers; whereas this trade includes non-state actors and criminal organisations;

G. whereas the acquisition, trading and hoarding of zero-day vulnerabilities fundamentally undermines the integrity and security of communications and cyber security of EU citizens;

H. whereas spyware surveillance should remain the exception and always require effective, binding and meaningful prior judicial authorisation by an impartial and independent judicial authority, which must ensure that the measure is necessary, proportionate and strictly limited to cases affecting national security or involving terrorism and serious crime; whereas surveillance techniques are liable to be abused in environments without effective checks and balances;

I. 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 CJEU, the European Court of Human Rights (ECtHR) and the Venice Commission; whereas this ex post oversight authority should order the termination of surveillance immediately if it is found to be incompatible with the above-mentioned rights and conditions;

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

K. whereas the rights of targeted persons are laid down in the Charter and international conventions, in particular the right to privacy and the right to a fair trial, as well as in Union rules on the rights of suspects and accused; whereas these rights have been confirmed by CJEU and ECtHR case-law;

L. whereas the impact of targeted surveillance on women can be particularly grievous, as authorities may use the increased social scrutiny women are under to weaponise private and intimate data extracted through spyware for defamation campaigns;

M. whereas it is clear from the testimonies of persons targeted that even if legal remedy and civil rights exist on paper, they mostly become void in the face of obstruction by government bodies, the absence or non-implementation of the right of persons targeted to be informed and the administrative obstacle of individuals having to prove they have been targeted; whereas even in systems with quick and open procedures, the nature of

spyware makes it very hard to prove authorship and the nature and extent to which an individual has been targeted;

N. whereas courts have not accepted the forensic evidence of independent experts but only evidence based on examination of the authorities, security or law enforcement that are allegedly behind an attack; whereas this leaves targets in a paradoxical situation with no viable option for proving a spyware infection;

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

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

Q. whereas it has been officially confirmed that a Member of the European Parliament(MEP) for Greece and a Greek journalist have been both wiretapped by the Greek National Intelligence Service (EYP) and targeted with Predator spyware; whereas a former US-Greek employee at Meta was simultaneously wiretapped by the EYP and targeted with Predator spyware, the use of which is illegal under Greek law; whereas according to media reports, opposition and government party MPs in Greece, party activists and journalists have allegedly also been targeted with Predator spyware or conventional wiretapping by the EYP or both; 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, such as Madagascar and Sudan; whereas the government has responded to the scandal with legislative amendments that further reduce the rights of targets to be informed after surveillance has taken place and is further hampering the work of independent authorities;

R. whereas revelations identified two categories of spyware target in Spain; whereas the first includes the Prime Minister and the Minister of Defence , the Minister of the Interior and other high officials; whereas the second category are part of what is referred to as ‘CatalanGate’ by the Citizen Lab organisation, and includes 65 targeted persons, including political figures from the regional Government of Catalonia, Members of the pro-Catalan independence movement, MEPs, lawyers, academics and civil society actors; whereas in May 2022 the Spanish authorities admitted to targeting 18 persons with court authorisation, though they have so far not disclosed the warrants or any other information, invoking national security when accounting for the use of spyware surveillance in Spain; whereas 47 other persons have also been allegedly targeted, but not received any information other than from Citizen Lab;

S. whereas no allegations of spyware infections have been confirmed in Cyprus; whereas Cyprus is an important European export hub for the surveillance industry and an attractive location for companies selling surveillance technologies;

T. whereas there are strong indications that the governments of Morocco and Rwanda, among others, have targeted high profile Union citizens with spyware, including the President of France, the Prime Minister, the Minister of Defence and the Minister of the Interior of Spain, the then Prime Minister of Belgium, the former President of the Commission and former Prime Minister of Italy, and Carine Kanimba, the daughter of Paul Rusesabagina;

U. whereas it can be safely assumed that all Member States have purchased or used one or more spyware systems; whereas most governments in the European Union will refrain from illegitimate use of spyware, but the risk of abuse is very plausible in the absence of a solid legal framework including safeguards and oversight, and in light of technical challenges in detecting and tracing infections;

V. whereas most Member State governments and Member State parliaments have not provided the European Parliament with meaningful information about their legal frameworks governing the use of spyware beyond what was already publicly known, despite an obligation to do so pursuant to Article 3(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;

W. whereas Article 4(3) TEU reads 'pursuant to the principle of sincere cooperation, the Union and the Member States shall, in full mutual respect, assist each other in carrying out tasks which flow from the Treaties';

X. whereas several key figures from the spyware industry have acquired Maltese citizenship, which facilitates their operations within and from the Union;

Y. whereas many spyware developers and 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; QuaDream in Cyprus; Amesys and Nexa Technologies in France; Tykelab and RCS Lab in Italy; and FinFisher (now defunct) in Germany;

Z. whereas the European Union does not participate in the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies; whereas all Member States except Cyprus participate in the Wassenaar Arrangement, although Cyprus submitted a request to join the Wassenaar Arrangement a long time ago; whereas Cyprus is bound by the Dual-Use Regulation;

AA. whereas Israel's export regime[1] applies in principle to all Israeli citizens, even when operating from the EU; whereas Israel is does not participate in the Wassenaar Arrangement but claims to apply its standards nevertheless;

AB. whereas the export of spyware from the Union to non-EU countries is regulated in the Dual-use Regulation, which was revised in 2021; whereas the Commission published its

---

[1] Defense Export Control Law 5766-2007, Israeli Ministry of Defence.

first implementation report in September 2022[1];

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

AD. 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; whereas 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, which have been accused of using Pegasus spyware against journalists, human rights defenders, civil society and politicians by Amnesty International and Forbidden Stories; whereas it is unknown if export licences were granted for the export of spyware to all these countries; whereas former FinFisher executives have been charged by the public prosecutor's office in Munich for exporting surveillance technology to Turkey without an export licence;

AE. whereas the number of attendees at arms fairs and ISSWorld who were marketing spyware capabilities demonstrates the predominance 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 diverse origins of spyware producers; whereas the fair is also attended by a wide range of European public authorities, including local police forces;

AF. whereas Article 4 (2) TEU provides that national security remains the sole responsibility of each the Member State;

AG. whereas, however, the CJEU has ruled (case 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';

AH. whereas the CJEU has ruled (case C-203/15) that 'Article 15(1) of 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), 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

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A434%3AFIN&qid=1662029750223.

Charter, 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';

AI. whereas the CJEU has ruled (case C-203/15) that 'Article 15(1) of Directive 2002/58/EC, as amended by Directive 2009/136/EC, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, 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';

AJ. whereas the case-law of the ECtHR makes clear that all surveillance must occur in accordance with the law, serve a legitimate aim and be necessary and proportionate: whereas, moreover, the legal framework must provide precise, effective and comprehensive safeguards on the ordering, execution and potential redress opportunities against surveillance measures, which must be subject to adequate judicial review and effective oversight[1];

AK. 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; whereas all Member States are parties to this Convention;

AL. whereas important aspects of the 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, fall within the scope of EU law;

AM. whereas the Charter lays down the conditions for the limitation of the exercise of fundamental rights, requiring that 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 when spyware is used, the level of interference with the right to privacy can be so severe that the individual is in fact deprived of it and the use cannot always be considered proportionate, irrespective of whether the measure can be deemed necessary to achieve the legitimate objectives of a democratic state;

AN. 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 such restrictions place national laws on spyware within the scope of the e-Privacy Directive in a similar way to national data retention laws; whereas frequent deployment of intrusive spyware technology would not be compatible

---

1 https://www.echr.coe.int/documents/fs_mass_surveillance_eng.pdf

with the Union legal order;

AO. whereas under international law a state has the right to investigate potential crimes only within its jurisdiction and has to resort to the assistance of other states where the investigation has to be carried out in other states unless there is a basis for conducting investigations in other jurisdictions under an international agreement or in in Union law, in the case of Member States;

AP. whereas the infection of a device with spyware and the subsequent collection of data takes place through the servers of mobile service providers; whereas as free roaming within the Union has resulted in persons sometimes having mobile contracts from other Member States than the one where they reside, there is currently no legal basis in Union law for the collection of data in the other Member State through the use of spyware;

AQ. whereas David Kaye, the former UN Special Rapporteur on the promotion and protection of the right to freedom of expression[1] and Irene Khan, current UN Special Rapporteur on the promotion and protection of the right to freedom of expression[2], have called for an immediate moratorium on the use, transfer and sale of surveillance tools until rigorous human rights safeguards are put in place to regulate practices and guarantee that Governments and non-state actors use these tools in legitimate ways;

AR. Whereas there are cases where spyware companies, in particular Intellexa, have not only sold the interception and extraction technology itself, but also the entire service, also referred to as 'hacking as a service' or 'active cyberintelligence', offering a package of surveillance and interception technology methods, as well as training for staff and technical, operational and methodological support; whereas this service could allow the company to be in control of the entire surveillance operation and aggregate the surveillance data; whereas this practice is almost impossible for the relevant authorities to oversee and control; whereas this makes it difficult to adhere to principles of proportionality, necessity, legitimacy, legality and adequacy; whereas this service is not permitted by Israel's defence export agency (DECA); whereas Cyprus has been used to bypass existing limitations under Israeli law in order to provide hacking as a service;

AS. whereas Member States must comply with Directive 2014/24/EU and Directive 2009/81/EC on public and defence procurement, respectively; whereas they must adequately justify derogations under Article 346(1)(b) TFEU, as Directive 2009/81/EC explicitly takes into account the sensitive characteristics of defence procurement and comply with the WTO Agreement on Government Procurement, as amended 30 March 2012[3] if party to it;

AT. whereas the EDPS has underlined that Member States have to respect the European Convention on Human Rights and the jurisprudence of the ECtHR, which sets limits to surveillance activities for national security; whereas, furthermore, when used for law enforcement purposes, surveillance has to comply with EU law and in particular Charter

---

1 'Surveillance and human rights', report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/41/35, 2019**.**

2 Office of the UN High Commissioner for Human Rights, 'Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech'.

3 https://www.wto.org/english/tratop_e/gproc_e/gpa_1994_e.htm.

and EU directives such as the ePrivacy Directive and the Law Enforcement Directive;

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

AV. whereas in the Horizon 2020 programme, Israel is ranked third among Associated Countries for overall participation in the programme; whereas the Horizon Europe Agreement with Israel has an overall budget for 2021-27 of EUR 95,5 billion[1]; whereas some funds have been made available to Israeli military and security companies through these European programmes[2];

AW. whereas the main legislative instrument for Union development policies is Regulation (EU) 2021/947[3] ('Global Europe Regulation') and Union funding may be provided through the types of financing provided for by the Financial Regulation; whereas assistance can 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 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, in particular in an increasingly digital world where more and more of our activities take place online;

2. Takes the firm position 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 in other sources, and notes 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;

3. Strongly condemns 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;

4. Points out that this illegitimate use of spyware by national and non-EU governments directly and indirectly affects the Union's institutions and the decision making process,

---

1 https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/israel-joins-horizon-europe-research-and-innovation-programme-2021-12-06_en.

2 https://webgate.ec.europa.eu/dashboard/extensions/CountryProfile/CountryProfile.html?Country=Israel
https://elbitsystems.com/products/comercial-aviation/innovation-rd/.

3 Regulation (EU) 2021/947 of the European Parliament and of the Council of 9 June 2021 establishing the Neighbourhood, Development and International Cooperation Instrument – Global Europe, amending and repealing Decision No 466/2014/EU of the European Parliament and of the Council and repealing Regulation (EU) 2017/1601 of the European Parliament and of the Council and Council Regulation (EC, Euratom) No 480/2009 (OJ L 209, 14.6.2021, p. 1).

thereby 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, fundamental rights and the rule of law from within the Union, and the lack of action taken by many Member States; notes that when they are threatened in one Member State, the entire Union is put at risk;

6. Stresses that digital standards governing technological developments in the Union must respect fundamental rights;

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

8. Expresses concern, furthermore, about the illegitimate use of, and illicit trade in spyware by Member States, which, taken together, transform the Union into a destination for the spyware industry;

9. Expresses concern about the targeting of high-profile personalities, human rights defenders and journalists in the Union with spyware, by non-EU countries;

10. Is equally 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; notes the very slow progress and lack of transparency in the judicial investigations into spyware abuse against government leaders and ministers of EU Member States and the Commission, as well as against civil society members, journalists or political opponents;

11. Notes that 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; notes that such measures must serve a legitimate aim, and be necessary and proportionate;

12. Regrets 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; acknowledges that some of this information may be subject to strict legal requirements of secrecy and confidentiality; considers the collective reply by the Council wholly inadequate and contrary to the principle of sincere cooperation as enshrined in Article 4(3) TEU;

13. Concludes 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;

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

15. Calls on Poland to:

(a) urge the Public Prosecutor-General to launch inquiries into the abuse of spyware;

(b) urgently restore sufficient institutional and legal safeguards, including effective, binding *ex ante* and *ex post* scrutiny, as well as independent oversight mechanisms, including judicial review of surveillance activities; stresses that in the context of effective *ex ante* scrutiny, the request to the court for operational surveillance, as well as the court order for such surveillance, should contain a clear justification and indication of the technical means to be used for the surveillance, and that in the context of effective *ex post* scrutiny, an obligation to inform the person subject to surveillance of the fact, duration, scope and manner of the processing of the data obtained during the operational surveillance should be established;

(c) introduce consistent legislation protecting citizens, regardless of whether the operational surveillance is carried out by the public prosecution service, the secret services or any other state body;

(d) comply with the ruling of the Constitutional Tribunal on the 1990 Police Act;

(e) comply with the opinion of the Venice Commission on the 2016 Police Act;

(f) comply with the various judgments of the ECtHR, such as the judgment in 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 persons targeted, as well as the judgment in the *Klass and others* v. *Germany* case in 1978, which outlines that surveillance must be of sufficient importance to necessitate such an invasion of privacy;

(g) comply with all the CJEU and ECtHR rulings related to the independence of judiciary and the primacy of EU law;

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

(i) restore the full independence of the judiciary and respect the statutory powers of all relevant oversight bodies, such as the Ombudsman, the President of the Personal Data Protection Office and the Supreme Audit Office, to ensure all oversight bodies receive full cooperation and access to information and to provide full information to all persons targeted;

(j) urgently put in place the random allocation of cases to the judges of the courts for every application that is submitted, even during the weekend and outside of normal business hours, in order to avoid the selection of ‘friendly judges’ by the secret services, and ensure the transparency of such a system by, inter alia, making the algorithm on the basis of which a judge is randomly allocated to a case publicly available;

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

(l) urgently clarify the situation surrounding the misuse of spyware in Poland, so as not to cast any doubt on the integrity of the upcoming elections;

(m) properly implement and enforce Directive (EU) 2016/680 (the Law Enforcement Directive), and ensure that the data protection authority has the power of supervision over the processing of personal data by, inter alia, authorities such as the Central Anti-Corruption Bureau and the Internal Security Agency;

(n) implement the Whistleblower Directive;

(o) refrain from adopting provisions in new laws on electronic communications that contravene the European Convention on Human Rights (ECHR);

(p) ensure the availability of effective legal remedies for the citizens of Poland affected by the implementation of laws contravening the Constitution of Poland and the ECHR;

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

(r) guarantee the independent constitutional review of laws in Poland;

(s) restore the independence of the role of the Public Prosecutor-General from the Minister of Justice in order to guarantee that investigations into alleged breaches of fundamental rights are free from political considerations;

16. Urges the Commission to assess the compatibility of the Polish 2018 Act on the protection of personal data processed in connection with the prevention and combating of crime with the EU Law Enforcement Directive and, if necessary, to start an infringement procedure;

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

18. Calls on Hungary to:

(a) urgently restore sufficient institutional and legal safeguards, including effective, binding *ex ante* and *ex post* scrutiny, as well as independent oversight mechanisms; including judicial review of surveillance activities; stresses that in the context of effective *ex ante* scrutiny, the request to the court for operational surveillance, as well as the court order for such surveillance, should contain a clear justification and indication of the technical means to be used for the surveillance, and that in the context of effective *ex post* scrutiny, an obligation to inform the person subject to surveillance of the fact, duration, scope and manner of the processing of the data obtained during the operational surveillance should be established;

(b) comply with the various judgments of the ECtHR, such as the judgment in 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 persons targeted, as well as the judgement in the *Klass and others* v. *Germany* case in 1978, which outlines that surveillance

must be of sufficient importance to necessitate such an invasion of privacy, as well as the requirement for the notification of surveillance subjects;

(c) comply with all the CJEU and ECtHR rulings related to the independence of judiciary and the primacy of EU law;

(d) reinstate independent oversight bodies in line with the judgment of the ECtHR in the case of Hüttl v. Hungary, wherein the court states that the National Authority for Data Protection and Freedom of Information (NAIH) is 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;

(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 receive full cooperation and access to information and to provide full information to all persons targeted;

(f) 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;

(g) implement the Whistleblower Directive;

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

(i) refrain from adopting provisions in new laws on electronic communications that contravene the ECHR;

(j) ensure the availability of effective legal remedies for the citizens of Hungary affected by the implementation of laws contravening the Constitution of Hungary and the ECHR;

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

20. 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 without hindrance, investigate all allegations of the use of spyware;

(d) urgently withdraw Amendment 826/145 to Law 2472/1997, which abolished the ability of the Hellenic Authority for Communication Security and Privacy (ADAE) to notify citizens of the lifting of the confidentiality of communications; amend Law 5002/2022 in order to restore the right of persons targeted to

immediate information, on request, as soon as the surveillance has been completed, and correct other provisions that weaken safeguards, scrutiny and accountability;

(e) restore full independence of the judiciary and all relevant oversight bodies, such as the Ombudsman and the Data Protection Authorities, and fully respect the independence of the ADAE, to ensure all oversight and supervision bodies receive full cooperation and access to information and to provide full information to all persons targeted;

(f) ensure that the ADAE can set up an electronic archive to be able to perform its task;

(g) urgently clarify the situation surrounding the misuse of spyware in Greece, so as not to cast any doubt on the integrity of the upcoming elections;

(h) reverse the legislative amendment of 2019 that placed the National Intelligence Service (EYP) under the direct control of the Prime Minister; put in place constitutional guarantees and allow parliamentary scrutiny of its operations, without the pretext of the confidentiality of information;

(i) ensure the independence of the National Transparency Authority (EAD) leadership;

(j) ensure the judiciary has all the necessary means and support for the investigation following the alleged abuse of spyware, and seize the physical evidence of proxies, broker companies and spyware vendors that are linked to the spyware infections;

(k) invite Europol to immediately join the investigations;

(l) refrain from political interference in the work of Chief Prosecutor;

21. Concludes that overall, the regulatory framework in Spain is in line with the requirements set by the Treaties; points out, however, that some reforms are needed, and the implementation in practice must be fully in line with fundamental rights and ensure the protection of public participation;

22. Calls, therefore, on Spain to:

(a) conduct a full, fair and effective investigation, in which full clarity is provided on all alleged cases of the use of spyware, including the 47 cases for which it remains unclear whether or not the individuals concerned were targeted by the Spanish National Intelligence Agency (CNI) with a court order, or whether another authority had received court orders to legally target them, as well as on the use of spyware against the Prime Minister and members of the government, and to present the findings as broadly as possible, in line with the applicable laws;

(b) provide adequate access for the persons targeted to the judicial authorisation issued by the Supreme Court to the CNI to target 18 persons;

(c) cooperate with the courts to ensure that individuals targeted with spyware have

access to real and meaningful legal remedy, and that judicial inquiries are concluded without delay in an impartial and thorough manner, for which sufficient resources should be allocated;

(d) start the reform of the legal framework of the CNI, as announced in May 2022;

(e) invite Europol, which could contribute with technical expertise, to join the investigations;

23. Concludes that there is evidence of maladministration in the implementation of the EU Dual-Use Regulation in Cyprus which requires close scrutiny;

24. Calls on Cyprus to:

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

(b) thoroughly assess the shipment of spyware material within the EU's internal market between Member States and map the different Israeli companies or companies owned and run by Israeli citizens that are registered in Cyprus and that are involved in such activities;

(c) release the report of the special investigator on the 'Spyware Van' case, as requested by the committee during its official mission to Cyprus;

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

25. Is of the view that the situation in some other Member States also gives 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 some Member States such as Cyprus and Bulgaria to become an export hub for spyware to repressive regimes around the world;

26. Is of the opinion that the failure or refusal of some national authorities to ensure proper protection for the citizens of the Union, including regulatory gaps and proper legal instruments, 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 right of citizens to live in a safe environment where human dignity, private life, personal data and property are respected, as required by Directive 2012/29/EU, according to which every victim of crime has a right to receive support and protection in accordance with their individual needs;

27. Concludes that serious shortcomings in the implementation of Union law have taken place when the Commission and the European External Action Service (EEAS) provided support to non-EU countries, including but not limited to, 10 such countries in the Sahel, to enable them to develop surveillance capabilities[1];

---

[1] Decision in case 1904/2021/MHZ, available at https://www.ombudsman.europa.eu/en/decision/en/163491.

28. Takes the position that the trade in and use of spyware needs to be regulated strictly; recognises, however, that the legislative process may take time, while abuse must be stopped immediately; calls for the adoption of conditions for the legal use, sale, acquisition and transfer of spyware; insists that, for the continued use of spyware, Member States shall fulfil all of the following conditions by 31 December 2023:

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

    (b) they prove 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;

    (c) they enter into an explicit commitment to involve Europol, pursuant to Articles 4, 5 and 6 of the Europol Regulation, in investigations into allegations of illegitimate use of spyware; and that

    (d) all export licences that are not fully in line with the Dual-Use Regulation are repealed;

29. Considers that the fulfilment of these conditions must be assessed by the Commission by 30 November 2023; considers, further, that the findings of the assessment shall be published in a public report;

30. Stresses that while fighting serious crime and terrorism, and acknowledging that the ability to do so is critically important for Member States, the protection of fundamental rights and democracy is essential; stresses, further, 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; considers that effective *ex ante* mechanisms to ensure judicial oversight are critical to protecting individual freedoms; reaffirms that individual rights cannot be put at risk by permitting unfettered access to surveillance; underlines that the ability of the judiciary to perform meaningful and effective *ex post* oversight in the area of requests for surveillance for national security is also important, to ensure that the disproportionate use of spyware by governments can be challenged;

31. Underlines that the use of spyware for law enforcement should be directly regulated through measures based on Chapter 4 of Title 5 TFEU on Judicial cooperation in criminal matters; emphasises that the configuration of spyware that is imported into the EU and otherwise placed on the market should be regulated by way of a measure based on Article 114 TFEU; notes that the use of spyware for national security purposes may only be indirectly regulated through, for example, fundamental rights and rules relating to data protection;

32. Considers that 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 on the basis of Chapter 4 of Title 5 TFEU regulating the use of spyware by Member State bodies, drawing from standards laid down by the CJEU, ECtHR, the Venice

Commission and the Fundamental Rights Agency[1]; considers that such EU standards should cover at least the following elements:

(a) the envisaged use of spyware should be authorised only in exceptional and specific cases in order to protect national security and be subject to an effective, binding and meaningful *ex ante* judicial authorisation by an impartial and independent judicial authority or other independent democratic oversight body, 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 for every device accessed 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; Member State authorities should, furthermore, only target individual end-user devices or accounts and refrain from hacking internet and technology service providers, in order to avoid affecting non-targeted users;

(c) the authorisation for the use of spyware may only be granted in exceptional cases with respect to investigations into a limited and closed list of clearly and precisely defined serious crimes that represent a genuine threat to national security, and spyware may only be used towards persons in relation to whom there are sufficient indications that they have committed or are planning to commit such serious criminal offences;

(d) data which is protected by privileges or immunities referring to categories of persons (such as politicians, doctors, etc.) or specifically protected relationships (such as lawyer-client privilege) or rules on the determination and limitation of criminal liability relating to the freedom of the press and the freedom of expression in other media, must not be sought through spyware unless there are sufficient grounds, established under judicial oversight, confirming involvement in criminal activities or national security matters, which should be subject to a common framework;

(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 the event of suspicions of abuse;

(g) national scrutiny bodies should report to the Member States, and the Member States should thereafter notify the Commission of this information on a regular basis; the Commission should use this information in its annual rule of law report

[1] Fundamental Rights Agency, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Volume II Summary*, 2017, https://fra.europa.eu/en/publication/2017/surveillance-intelligence-services-fundamental-rights-safeguards-and-remedies-eu.

to allow the comparison of spyware use in the Member States;

(h) the right of notification for the targeted person: after the surveillance has ended, the authorities should notify the person 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, the data obtained, information on how that data has been used and by which actors, the date of deletion of the data and the right and practical arrangements for seeking administrative and judicial remedies before the competent authorities; notes that this notification should be sent without undue delay, unless an independent judicial authority grants delay of notification, in the event that immediate notification would seriously jeopardise the purpose of the surveillance;

(i) the right of notification for non-targeted persons whose data were accessed: after the period for which the surveillance had been authorised has ended, the authorities should notify the persons whose right to privacy has been severely interfered with through the use of spyware but were not the target of the operation; the authorities should notify this person of the fact that their data was accessed by the authorities, provide information regarding the date and duration of the surveillance, the warrant issued for the surveillance operation, the data obtained, information on how that data has been used and by which actors, and the date of deletion of the data; notes that this notification should be sent without undue delay, unless an independent judicial authority grants delay of notification, in the event that immediate notification would seriously jeopardise the purpose of the surveillance;

(j) effective, binding and independent *ex post* oversight over the use of spyware, the bodies responsible for which must have all required means and powers to exercise a meaningful oversight and be coupled with parliamentary oversight based on cross-party membership with appropriate clearance and with full access to sufficient information to ascertain that the surveillance was lawfully and proportionally conducted, and parliamentary oversight of sensitive confidential information should be facilitated through the necessary infrastructure, processes and security clearances; regardless of the definition or demarcation of the concept of national security, national oversight bodies must be competent for the full scope of national security;

(k) fundamental principles of due process and judicial oversight must be central to the regime surrounding surveillance spyware;

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

(m) 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, as well as the 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; in cases where abuses have been verified, adequate sanctions of either a criminal or an administrative nature, according to the relevant national law in the Member States, should apply;

(n) the improvement of free of charge access of persons targeted to technological expertise at this stage, since the increased availability and affordability of technological processes, such as forensic analysis, would allow persons targeted to present stronger cases in court and would improve the representation of persons targeted in court through technological capacity building of legal representation and the judiciary to better advise persons targeted, identify violations, improve the oversight of and accountability for spyware abuse;

(o) the reinforcement of the rights of the defence and the right to a fair trial by ensuring that those accused of crimes are allowed and able to check the accuracy, authenticity, reliability and even the legality of the evidence used against them and therefore rejecting any blanket application of national defence secrecy rules;

(p) during surveillance, the authorities should delete all data that is irrelevant to the authorised investigation and after the surveillance and the investigation for which the authorisation was granted has ended, the 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;

(q) relevant information that is obtained by spyware should only be accessible to authorised authorities and solely for the purpose of an operation; this access should be limited to a particular period of time, as specified in the judicial process;

(r) minimum standards for rights of individuals in criminal proceedings on the admissibility of evidence collected with the help of spyware need to be established; the possibility of false or manipulated information produced as a result of the deployment of spyware (impersonation) needs to be included in criminal procedural law;

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

(t) a marker needs to be included in the surveillance software so that oversight bodies can unambiguously identify the deployer in the event of suspicion of abuse; the mandatory signature for each spyware deployment should consist of an individual label for the acting authority, the type of spyware used and an anonymised case number;

33. Calls on the Member States to undertake public consultations with stakeholders, secure transparency of the legislative process and include EU standards and safeguards when drafting new legislation on the use and sale of spyware;

34. Emphasises that only spyware that is designed so that it enables and facilitates the functionality of spyware according to the legislative framework as set out in paragraph 32 may be placed on the internal market, developed or used in the Union; affirms that

such a regulation on the placing on the market of spyware that provides for 'rule-of-law-by-design' based on Article 114 TFEU should grant Union citizens a high level of protection; considers it unjustifiable that, while the Dual-Use Regulation has provided citizens of non-EU countries protection against spyware exports from the EU since 2021, no equivalent protection is offered to EU citizens;

35. Considers that only interception and extraction technology may be sold by companies in the EU and acquired by Member States, and not 'hacking as a service', which includes the supply of technical, operational and methodological support of surveillance technology, and allows the provider access to a disproportionate amount of data that is incompatible with principles of proportionality, necessity, legitimacy, legality and adequacy; calls on the Commission to propose a legislative proposal in this regard;

36. Stresses 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; considers that security agencies should only use spyware when all recommendations laid out by the Fundamental Rights Agency have been implemented[1];

37. Highlights the obligation to use a version of spyware that is designed in such a way that it minimises the access to all data stored on a device, but should be designed in such a way that it limits access to data to the minimum of what is strictly necessary for the purpose of the authorised investigation;

38. Concludes that when a Member State has purchased spyware, the acquisition must be auditable by an independent, impartial audit body with appropriate clearance;

39. Stresses that all entities placing spyware on the internal market should comply with strict due diligence requirements, and companies applying in a public procurement process to be suppliers should undergo a vetting process which includes the company's response to human rights violations committed with their software and whether the technology relies on data gathered in undemocratic and abusive surveillance practices; underlines that the competent national supervisory authorities should report to the Commission on an annual basis on compliance;

40. Stresses that companies offering surveillance technologies or services to state actors should disclose to the competent national supervisory authorities the nature of the export licences;

41. Underlines that Member States should establish a cooling-off period, temporarily preventing former employees of governmental bodies or agencies from working for spyware companies;

Need for boundaries to national security

42. Is concerned about cases of the unjustified invocation of 'national security' to justify the deployment and use of spyware and to ensure absolute secrecy and lack of accountability; welcomes the Commission statement, in line with the CJEU's

---

1 https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2-summary_en.pdf.

jurisprudence[1] that a mere reference to national security cannot be interpreted as being an unlimited carve out from the application of EU law and should require a clear justification, and calls on the Commission to follow up on that statement in the cases where there are indications of abuse; considers that in a democratic transparent society that abides by the rule of law, such limitations in the name of national security will be the exception rather than the rule;

43. Considers that the notion of national security must be contrasted with the more restricted scope vis-à-vis internal security, whereby the latter has a broader scope, including the prevention of risks to citizens, and, in particular, the enforcement of criminal law;

44. Regrets the difficulties stemming from the lack of a common legal definition of national security laying down criteria to determine what legal regime may apply in matters of national security, as well as of a clear demarcation of the area where such a special regime may apply;

45. Considers that the use of spyware constitutes a limitation of fundamental rights; further considers that where a concept is used in a legal context, entailing the transfer of rights and the imposition of obligations (and, in particular, limitations of the fundamental rights of individuals), the concept needs to be clear and foreseeable to all persons affected by it; recalls that the Charter provides that any limitation to fundamental rights according to Article 52(1) must be set out in law; considers, therefore, that it is necessary for 'national security' to be clearly defined; underlines that regardless of the precise demarcation, the domain of national security must be subject to independent, binding and effective oversight in its entirety;

46. Stresses that if the authorities invoke national security grounds as a justification for using spyware, they should, in addition to the framework laid down in paragraph 29, demonstrate compliance with EU law, including adherence to the principles of proportionality, necessity, legitimacy, legality and adequacy; highlights that the justification should be easily accessible and made available to a national scrutiny body for assessment;

47. Reiterates, in this context, that all Member States signed Convention 108+, which lays down standards and obligations for the protection of individuals concerning the processing of personal data, including for national security purposes; points out that Convention 108+ is a binding European framework dealing with the processing of data by intelligence and security services; urges all Member States to ratify this convention without delay, to already implement its standards in national law and to act accordingly over national security;

48. Emphasises that exceptions and restrictions to a limited number of provisions of the

---

[1] Judgment of 6 October 2020, Case C-623/17, *Privacy International* v *Secretary of State for Foreign and Commonwealth Affairs and Others*, ECLI:EU:C:2020:790, paragraph 44 and Judgments of 6 October 2020, Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others* v *Premier ministre and Others*, ECLI:EU:C:2020:791, paragraph 99: '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'.

convention are only permitted when they are in accordance with the requirements referred to in Article 11 of the convention, meaning that when implementing Convention 108+, each specific exception and restriction must be provided for by law, must respect the essence of the fundamental rights and freedoms, and must justify that it 'constitutes a necessary and proportionate measure in a democratic society' for one of the legitimate grounds listed in Article 11[1] and that such exceptions and restrictions must not interfere with the 'independent and effective review and supervision under the domestic legislation of the respective Party';

49. Further notes that Convention 108+ stresses that the oversight 'shall have powers of investigation and intervention'; considers that effective review and supervision implies binding powers where the impact on fundamental rights is the greatest, particularly in the accessing, analysis and storage phases of processing personal data;

50. Considers that the lack of binding powers of oversight bodies within the domain of national security is incompatible with the criterion laid down in Convention 108+ that this 'constitutes a necessary and proportionate measure in a democratic society';

51. Points out that Convention 108+ allows for a very limited number of exceptions with regard to its Article 15 but it does not allow such exceptions, notably regarding paragraph 2 [awareness-raising duties], paragraph 3 [consultation on legislative and administrative measures], paragraph 4 [requests and complaints by individuals], paragraph 5 [independence and impartiality], paragraph 6 [necessary resources for the effective performance of tasks], paragraph 7 [periodic reporting], paragraph 8 [confidentiality], paragraph 9 [possibility of appeal] and paragraph 10 [no power regarding bodies when acting in their judicial capacity];

Better implementation and enforcement of existing legislation

52. 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 too often improperly implemented and/or enforced: the Anti-Money Laundering Directive, the Law Enforcement Directive, procurement rules, the 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 1 August 2023 at the latest;

53. Considers the proper implementation and strict enforcement of the Union legal framework on data protection, particularly the Law Enforcement Directive, the General Data Protection Regulation and the e-Privacy Directive, to be crucial; considers equally important the full implementation of the relevant CJEU judgments, which is still lacking in several Member States; recalls that the Commission has a central role in enforcing EU law and ensuring its uniform application throughout the Union, and should make

---

[1] This assessment is provided for in the case law of the ECtHR that lays the burden of proof with the State/Legislator. Relevant ECtHR case law includes: *Roman Zakharov* v. *Russia* (Application No. 47143/06), 4 December 2015; *Szabó and Vissy* v. *Hungary* (Application No. 37138/14), 12 January 2016; *Big Brother Watch and Others* v. *the United Kingdom* (application nos. 58170/13, 62322/14 and 24969/15), 25 May 2021 and *Centrum för rättvisa* v. *Sweden* (application no. 35252/08), 25 May 2021.

use of all tools available, including infringement procedures in cases of persistent non-compliance;

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

55. Calls for Cyprus and Israel to become participating states of the Wassenaar Arrangement; reminds the Member States that all efforts must be made to enable Cyprus and Israel to join the Wassenaar Arrangement;

56. 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;

57. Stresses that in the light of the spyware revelations, the Commission and the Member States should conduct an in-depth investigation into the export licences granted for the use of spyware under the Dual-Use Regulation and the Commission should share the results of this assessment with Parliament;

58. Underlines the need for the traceability of and accountability for spyware exports and recalls that EU companies should only be able to export spyware that demonstrates sufficient traceability properties to ensure that responsibility can always be attributed;

59. 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;

60. Calls on the Commission to ensure sufficient staff capacity for the units responsible for the oversight and enforcement of the Dual-Use Regulation;

61. 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 use in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law; calls for the full implementation of human rights and due diligence checks in the licensing process and further improvements such as remedy for targets of human rights abuses and the transparent reporting of performed due diligence;

62. 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;

63. Stresses that, in a future amendment of the Dual-Use Regulation, the 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; and why the export licence was approved or denied; emphasises that these reports should be made public on a quarterly basis; calls for the setting up of a dedicated standing parliamentary

committee with access to classified information from the Commission, for the purpose of parliamentary oversight;

64. 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 non-EU countries, the Commission can decide to classify certain information in its annual report;

65. 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 the 'authentication' or authorisation controls of the device; electronic systems or equipment, designed either for the surveillance and monitoring of the electro-magnetic spectrum for military intelligence or security purpose; and Unmanned Aerial Vehicles capable of conducting surveillance;

66. 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

67. Calls 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;

68. Calls for the EU-US Trade and Technology Council to hold wide and open consultations with civil society for the development of the joint EU-US strategy and standards, including the joint whitelist and/or blacklist;

69. 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 regarding human rights standards and due diligence arrangements;

70. Notes that compared to the US, where NSO was quickly blacklisted and the US President signed an Executive Order, stating that it must not make operational use of commercial spyware that poses significant counterintelligence or security risks to the United States Government or significant risks of improper use by a foreign government

or foreign person, no sufficient action has been taken at EU level as regards the imports of spyware and the enforcement of the export rules;

71. Concludes that the Union export rules and their enforcement must be strengthened for the protection of human rights in non-EU countries and must be given the necessary tools to implement its provisions effectively; recalls 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 and set robust standards of transparency, traceability and accountability for the use of surveillance technology, which should culminate in an initiative at United Nations level;

Zero-day vulnerabilities

72. Calls for the regulation of the discovery, sharing, patching and exploitation of vulnerabilities, as well as disclosure procedures, thereby completing the basis set out by Directive (EU) 2022/2555[1] (NIS 2 Directive) and the proposal for the Cyber Resilience Act[2];

73. 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;

74. Calls on 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 to run bug bounty programmes;

75. Calls on the Commission to increase its support and funding for bug bounties and other projects aimed at searching for and patching security vulnerabilities, and to set up a coordinated approach to mandatory vulnerability disclosure among Member States;

76. Calls for a ban on the sale of vulnerabilities in a system for any purpose other than strengthening the security of that system , and an obligation to disclose the findings of all vulnerability research in a coordinated and responsible manner that promotes public safety and minimises the risk of exploitation of the vulnerability;

77. Calls on public and private entities to create a publicly available contact point where vulnerabilities can be reported in a coordinated and responsible manner, and for organisations that receive information about vulnerabilities in their system to act immediately to fix them; considers that, when a patch is available, organisations should be mandated to have the appropriate measures in place to ensure rapid and guaranteed deployment, as part of a coordinated and responsible disclosure process;

78. Considers that the Member States should allocate sufficient financial, technical and

---

1 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022, p. 80).

2 Proposal of 15 September 2022 for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (COM(2022)0454).

human resources to security research and patching vulnerabilities;

79. Calls on the Member States to develop a vulnerability equity processes, prescribed by law, which determine that, by default, vulnerabilities must be disclosed and not exploited, and that any decision to deviate from this must be an exception and assessed under the requirements for necessity and proportionality, including the consideration as to whether the infrastructure affected by the vulnerability is used by a large share of the population, and be subject to strict oversight by an independent supervising body, as well as to transparent procedures and decisions;

Telecom networks

80. Stresses that the licence of any service provider found to be facilitating unlawful access to national and/or international mobile signalling infrastructure across all generations (currently 2G to 5G) should be revoked;

81. Stresses that the processes through which new phone numbers from all over the world can be created by malicious actors should be better regulated to make illicit activity more difficult to hide;

82. Stresses the need for telecom providers to ensure that they have the capacity to detect potential misuse of access, control, or effective end use of signalling infrastructure gained by third parties through commercial or other agreements in the Member State that they operate in;

83. Calls on the Member States to ensure that competent national authorities, in accordance with the NIS 2 Directive's provisions, evaluate telecom providers' level of resilience to unauthorised intrusions;

84. Calls on telecom providers to take firm and demonstrable action to mitigate against the various forms of emulating without authorisation the origination of telecoms traffic by a network element in order to access the data or service that was meant for the legitimate user, and other activity involving the manipulation of the normal operations of mobile network elements and infrastructure for surveillance purposes by malicious actors, including state-level actors, as well as criminal groups;

85. Calls on the Member States to take action to ensure that non-EU state actors that do not respect fundamental rights do not have control or effective end use of strategic infrastructure, or influence over decisions related to strategic infrastructure within the Union, including telecommunications infrastructure;

86. Calls on all Member States to prioritise greater investment in the protection of critical infrastructure, such as national telecommunications systems, to address gaps in protection against privacy breaches, data leaks and unauthorised intrusions, in order to defend the fundamental rights of citizens;

87. Calls on the competent national authorities to actively promote strengthening the capabilities of providers, as well as response capabilities, to better support the identification of persons illegally targeted, notification and incident reporting, in order to provide ongoing, measurable assurance and mitigation of the exploitation of security gaps by non-EU and domestic malicious actors;

e-Privacy

88. 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 the abuse of surveillance technologies, that strengthens the fundamental right to privacy and provides for strong safeguards and effective enforcement; points out that the scope for lawful interception should not go beyond the e-Privacy Directive (2002/58/EC);

89 Calls 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; points out that digital safety-by-design tools such as end-to-end encryption should not be weakened;

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

The role of Europol

91. Notes that a letter from Europol to the Chair of the PEGA Committee of April 2023 informs the Committee that Europol has contacted Greece, Hungary, Bulgaria, Spain and Poland to ascertain whether there are any ongoing or envisaged criminal investigations or other inquiries under the applicable provisions of national law, which could be supported by Europol; stresses that offering assistance to Member States does not constitute the initiation, conduct or coordination of a criminal investigation as laid down in Article 6;

92. Calls on Europol to make full use of its newly acquired powers under Article 6 (1a) of Regulation (EU) 2022/991, enabling it to propose to the competent authorities of the Member States concerned to initiate, conduct or coordinate an investigation, where relevant; points out that under Article 6 it is up to the Member States to reject such a proposal;

93. Calls on all Member States to commit to the European Parliament and the Council to involve Europol in investigations into allegations of illegitimate use of spyware at national level, particularly when a proposal under Article 6 (1a) of Regulation (EU) 2022/991 has been made;

94. Calls on the Member States to set up a register within Europol of national law enforcement operations involving the use of spyware, 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;

95. Takes the view that a reflection must be launched about the role of Europol in case where national authorities fail or refuse to investigate and there are clear threats to the interests and security of the EU;

Union development policies

96. Calls on the Commission and the EEAS to implement more rigorous control mechanisms to ensure that Union development aid, including the donation of surveillance technology and training in the deployment of surveillance software, does not fund or facilitate tools and activities that could impinge on the principles of

democracy, good governance, the rule of law and respect for human rights, or that pose a threat to international security or the essential security of the Union and its Members; 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, including the possible temporary suspension of specific projects if an infringement of these principles is detected;

97. Calls on the Commission and the EEAS to include in every human and fundamental rights impact assessment a monitoring procedure on the potential abuse of surveillance, which fully takes into account Article 51 of the Charter in the time frame of within one year [after the publication of the PEGA recommendations]; stresses that this procedure must be presented to Parliament and the Council and that this impact assessment must be carried out prior to any support to non-EU countries;

98. Calls on the EEAS to report on the abuse of spyware against human rights defenders in the EU Annual Report on Human Rights and Democracy;

Union financial regulations

99. 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;

100. Is concerned about the implications of the CJEU decision on Directive (EU) 2018/843 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing[1], whereby the information on the beneficial ownership of corporate and legal entities established in a national and publicly accessible Register of Beneficial Ownership (UBO) has been ruled invalid[2]; stresses that, taking the CJEU decision into account, the future directive should allow for as much public accessibility as possible, so that it becomes more difficult to hide purchases or sales of spyware through proxies and broker companies;

Follow-up to Parliament resolutions

101. Calls for the urgent follow-up to Parliament's 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 recommendations therein need to be carried out as a matter of urgency;

102. 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;

---

1 Judgment of 22 November 2022, Joined Cases C-37/20 and C-601/20, ECLI:EU:C:2022:912.

2 CJEU. Press Release No 188/22, Judgment of the Court in Joined Cases C-37/20 and C-601/20.

103. 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;

104. 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;

105. 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) develop criteria on enhanced transparency, built on the general principle of access to information and the so-called Tshwane Principles[1];

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

107. 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;

108. Calls on the Member States to develop cooperation among oversight bodies;

109. 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;

110. Recalls the provisions of the interinstitutional agreement between the European 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;

---

1 The Global Principles on National Security and the Right to Information, June 2013.

Union research programmes

111. Calls for the implementation of more rigorous and effective control mechanisms to ensure that Union research funds do not fund or facilitate tools, including spyware and surveillance tools, that infringe EU values; notes that assessments of compliance with Union law should contain specific control criteria to prevent such abuses; calls for the termination of Union research funds to entities that are or have been involved in the direct or indirect facilitation of human rights violations with surveillance tools;

112. Stresses that EU funding for research, such as the Horizon Europe agreements with non-EU countries, must not be used to contribute to the development of spyware and equivalent technologies;

EU Tech Lab

113. Calls on the Commission 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; stresses that this institute should work with experts, academia and civil society representatives, as well as be open to participation by Member States' experts and institutions;

114. Stresses that the institute would contribute to better awareness, attribution and accountability in and beyond Europe, as well as expand the European talent base and our understanding of how spyware vendors develop, maintain, sell and deliver their services to third parties;

115. Considers that the 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, including smartphone screenings for individuals who suspect that they have been targeted by spyware and the tools necessary for detecting spyware, performing forensic analytical research for judicial investigations and reporting regularly on the use and misuse of spyware in the EU, taking into account technological updates; considers that this report should be made available annually and transmitted to the Commission, Parliament, and the Council;

116. Recommends that the Commission set up the EU Tech Lab in close cooperation with the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU) and ENISA and that it consult the relevant experts when establishing the EU Tech Lab in order to learn from the best practices in the academic field;

117. Underlines the importance of ensuring adequate funding for the EU Tech Lab;

118. Recommends that the Commission put forward a certification scheme for the analysis and authentication of forensic material;

119. Calls on the Commission to support civil society capacity globally in order to strengthen resilience against spyware attacks and the provision of assistance and services to citizens;

The rule of law

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

121. Calls, therefore, on the Commission to ensure an effective implementation of its Rule of Law toolbox, particularly by:

    (a) putting in place a more comprehensive monitoring of the rule of law, including country-specific recommendations related to Member States' unlawful use of spyware in the Commission's Annual Rule of Law Report, assessing the responsiveness of state institutions to providing redress to persons targeted t, 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 launching 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 in the context of police and judicial cooperation in criminal matters;

Union litigation fund

122. Calls for the establishment, without undue delay, of a Union Litigation Fund to cover the actual litigation costs and enable the persons targeted by spyware to seek adequate redress, including damages for the illegal use of spyware against them, 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';

EU institutions

123. 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;

124. 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;

125. Calls on the Commission to set up a special taskforce, involving the national electoral commissions, dedicated to protection of the 2024 European elections across the Union; recalls that not only foreign but also internal interference poses a threat to the European electoral processes; stresses that in the event of the misuse of pervasive surveillance tools, such as Pegasus, the elections may be affected;

126. Notes that the PEGA Committee received a collective reply from the Council to the queries of the European Parliament to all individual Member States only on the eve of the publication of the draft report, approximately four months after the letters from Parliament; expresses dismay at the lack of action of the European Council and the

Council of Ministers, and calls for a dedicated European Council Summit, given the magnitude of the threat to democracy in Europe;

127. Calls on the Council of the EU to address developments related to the use of spyware and its impact on the values enshrined in Article 2 TEU during hearings organised under Article 7(1) TEU;

128. Calls on the Council to permanently invite the European Parliament to Council Security Committee meetings, as provided for in Article 17(2) of the Council Security Rules 2013;

129. Takes the position that Parliament should have full powers of inquiry, including better access to classified and non-classified information, the power to summon witnesses, to formally require witnesses to testify under oath and to provide requested information within specific deadlines; reiterates the Parliament's position in its proposal of 23 May 2012 for a regulation of the European Parliament on the detailed provisions governing the exercise of the European Parliament's right of inquiry and repealing Decision 95/167/EC, Euratom, ECSC of the European Parliament, the Council and the Commission[1]; calls on the Council to immediately take action on this proposal for a regulation to allow for a proper right of inquiry for the European Parliament;

130. Acknowledges Parliament's efforts in detecting spyware infections; considers, however, that the protection of staff should be strengthened, having regard to the privileges and immunities of those who have been spied on; recalls that any attack on a Member's political rights is an attack on the independence and sovereignty of the institution, as well as an attack on voters' rights;

131. Calls for Parliament's Bureau 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 by Parliament to the responsible law enforcement authorities; stresses that Parliament should provide legal and technical assistance in such cases;

132. Resolves to take the initiative to launch an interinstitutional conference, wherein Parliament, the Council and the Commission must aim for governance reforms that strengthen the Union's institutional capacity to respond adequately to attacks on democracy and the 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;

133. Calls for the swift adoption of the Commission proposal for a regulation of the European Parliament and of the Council laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (COM(2022)0122) and prompt implementation and strict enforcement thereafter, in order to reduce the risk of spyware infections of the devices and systems used by the EU institutions' staff and politicians;

134. Calls for the EU to sign up to Convention 108+;

135. Calls on the European Ombudsman to initiate discussions within the European Network

---

1 OJ C 264 E, 13.9.2013, p. 41.

of Ombudsmen on the impact of the misuse of pervasive surveillance on democratic processes and citizens' rights; calls on the network to develop recommendations on effective and meaningful redress across the EU;

Legislative action

136. Calls on the Commission to promptly come forward with legislative proposals on the basis of this recommendation;

°

° °

137. Instructs its President to forward this recommendation to the Member States, the Council, the Commission and to Europol.