Europäisches Parlament
2019-2024

Plenarsitzungsdokument

B9-0260/2023

22.5.2023

ENTWURF EINER EMPFEHLUNG DES EUROPÄISCHEN PARLAMENTS AN DEN RAT UND DIE KOMMISSION

eingereicht gemäß Artikel 208 Absatz 12 der Geschäftsordnung

nach der Prüfung von behaupteten Verstößen gegen das Unionsrecht und Missständen bei der Anwendung desselben im Zusammenhang mit dem Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware (2023/2500(RSP))

Sophie in ‘t Veld
im Namen des Untersuchungsausschusses zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware

B9-0260/2023

Entwurf einer Empfehlung des Europäischen Parlaments an den Rat und die Kommission nach der Prüfung von behaupteten Verstößen gegen das Unionsrecht und Missständen bei der Anwendung desselben im Zusammenhang mit dem Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware (2023/2500(RSP))

Das Europäische Parlament,

– gestützt auf den Vertrag über die Europäische Union (EUV), insbesondere auf die Artikel 2, 4, 6 und 21,

– gestützt auf die Artikel 16, 223, 225 und 226 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV),

– unter Hinweis auf die Charta der Grundrechte der Europäischen Union (im Folgenden „Charta“), insbesondere die Artikel 7, 8, 11, 17, 21, 41, 42 und 47,

– unter Hinweis auf die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation[1] (Datenschutzrichtlinie für elektronische Kommunikation),

– unter Hinweis auf die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)[2],

– unter Hinweis auf die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates[3],

– unter Hinweis auf die Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates[4] (Richtlinie zur Bekämpfung der Cyberkriminalität),

– unter Hinweis auf die Verordnung (EU) 2021/821 des Europäischen Parlaments und des Rates vom 20. Mai 2021 über eine Unionsregelung für die Kontrolle der Ausfuhr, der Vermittlung, der technischen Unterstützung der Durchfuhr und der Verbringung betreffend Güter mit doppeltem Verwendungszweck[5] (Verordnung über Güter mit

[1] ABl. L 201 vom 31.7.2002, S. 37.
[2] ABl. L 119 vom 4.5.2016, S. 1.
[3] ABl. L 119 vom 4.5.2016, S. 89.
[4] ABl. L 218 vom 14.8.2013, S. 8.
[5] ABl. L 206 vom 11.6.2021, S. 1.

doppeltem Verwendungszweck),

– unter Hinweis auf den Beschluss (GASP) 2019/797 des Rates vom 17. Mai 2019 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen[6], in der durch den Beschluss (GASP) 2021/796 des Rates vom 17. Mai 2021 geänderten Fassung[7],

– gestützt auf den Akt zur Einführung allgemeiner unmittelbarer Wahlen der Mitglieder des Europäischen Parlaments[8],

– gestützt auf den Beschluss 95/167/EG, Euratom, EGKS des Europäischen Parlaments, des Rates und der Kommission vom 6. März 1995 über Einzelheiten der Ausübung des Untersuchungsrechts des Europäischen Parlaments[9],

– gestützt auf den Beschluss (EU) 2022/480 des Europäischen Parlaments vom 10. März 2022 über die Einsetzung, die Zuständigkeiten, die Mitgliederzahl und die Mandatszeit des Untersuchungsausschusses zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware und die Festlegung des Gegenstands der Untersuchung[10],

– unter Hinweis auf die Richtlinie (EU) 2018/843 des Europäischen Parlaments und Rates vom 30. Mai 2018 zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinien 2009/139/EG und 2013/36/EU[11] (Geldwäscherichtlinie),

– unter Hinweis auf den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates vom 16. September 2022 zur Schaffung eines gemeinsamen Rahmens für Mediendienste im Binnenmarkt (Europäisches Medienfreiheitsgesetz) und zur Änderung der Richtlinie 2010/13/EU (COM(2022)0457),

– unter Hinweis auf Artikel 12 der Allgemeinen Erklärung der Menschenrechte,

– unter Hinweis auf das Urteil des Gerichtshofs der Europäischen Union (EuGH) in der Rechtssache C-37/20[12] über die Geldwäscherichtlinie, das besagt, dass die Bestimmung, nach der die Angaben über die wirtschaftlichen Eigentümer von im Hoheitsgebiet der Mitgliedstaaten eingetragenen Gesellschaften in allen Fällen für alle Mitglieder der Öffentlichkeit zugänglich sein müssen, ungültig ist;

– unter Hinweis auf Artikel 17 des Internationalen Pakts über bürgerliche und politische Rechte,

– unter Hinweis auf die Charta der Vereinten Nationen und die Leitprinzipien der

[6] ABl. L 129 I vom 17.5.2019, S. 13.
[7] ABl. L 174 I vom 18.5.2021, S. 1.
[8] ABl. L 278 vom 8.10.1976, S. 5.
[9] ABl. L 113 vom 19.5.1995, S. 1.
[10] ABl. L 98 vom 25.3.2022, S. 72.
[11] ABl. L 156 vom 19.6.2018, S. 43.
[12] Urteil des Gerichts (Große Kammer) vom 22. November 2022, C-37/20, *WM* und *Sovim SA*/*Luxemburg Business Registers*, EU:C:2022:912.

Vereinten Nationen für Wirtschaft und Menschenrechte[13],

– unter Hinweis auf die Erklärung der Hohen Kommissarin der Vereinten Nationen für Menschenrechte, Michelle Bachelet, vom 19. Juli 2022 mit dem Titel „Use of spyware to surveil journalists and human rights defenders“,

– unter Hinweis auf die Erklärung der Menschenrechtskommissarin des Europarats, Dunja Mijatovic, vom 27. Januar 2023 mit dem Titel „Highly intrusive spyware threatens the essence of human rights“[14],

– unter Hinweis auf die einleitenden Bemerkungen des europäischen Datenschutzbeauftragten (EDSB) zu moderner Spähsoftware vom 15. Februar 2022[15],

– unter Hinweis auf die Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten, insbesondere ihre Artikel 8, 10, 13, 14 und 17, und die Protokolle zu dieser Konvention,

– unter Hinweis auf die Bewertung der Bedrohungslage im Bereich der schweren und organisierten Kriminalität (SOCTA) von Europol aus dem Jahr 2021 mit dem Titel „A Corrupting Influence: the Infiltration and Undermining of Europe’s Economy and Society by Organised Crime“,

– unter Hinweis auf den Bericht der Agentur der Europäischen Union für Grundrechte (FRA) von 2017 mit dem Titel „Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU“ und auf die Aktualisierungen, die dem Untersuchungsausschuss zur Untersuchung des Einsatzes von Pegasus und gleichwertiger Überwachungs- und Spähsoftware (PEGA) am 28. Februar 2023 vorgelegt wurden,

– unter Hinweis auf seine Entschließung vom 12. März 2014 zu dem Überwachungsprogramm der Nationalen Sicherheitsagentur der Vereinigten Staaten, den Überwachungsbehörden in mehreren Mitgliedstaaten und den entsprechenden Auswirkungen auf die Grundrechte der EU-Bürger und die transatlantische Zusammenarbeit im Bereich Justiz und Inneres[16] und insbesondere auf die darin enthaltenen Empfehlungen im Hinblick auf die Stärkung der IT-Sicherheit in den Organen, Einrichtungen und sonstigen Stellen der Union,

– unter Hinweis auf die Stellungnahme 24/2022 des EDSB vom 11. November 2022 zum europäischen Medienfreiheitsgesetz,

– unter Hinweis auf das von der Agentur der Europäischen Union für Cybersicherheit (ENISA) erarbeitete Glossar zu Schad- und Spähsoftware,

– unter Hinweis auf den Beschluss der europäischen Bürgerbeauftragten zu der Art, wie

[13] https://www.auswaertiges-amt.de/blob/266624/b51c16faf1b3424d7efa060e8aaa8130/un-leitprinzipien-de-data.pdf
[14] https://www.coe.int/en/web/commissioner/-/highly-intrusive-spyware-threatens-the-essence-of-human-rights
[15] https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf
[16] ABl. C 378 vom 9.11.2017, S. 104.

die Kommission die Auswirkungen auf Menschenrechte vor der Unterstützung für afrikanische Länder bei der Entwicklung von Überwachungsmöglichkeiten bewertet hat (Fall 1904/2021/MHZ),

– unter Hinweis auf die Erklärung von Irene Kahn, Sonderberichterstatterin der Vereinten Nationen für Meinungsfreiheit, und Fernand de Varennes, Sonderberichterstatter der Vereinten Nationen zu Minderheitenfragen, vom 2. Februar 2023, in der sie eine Untersuchung der mutmaßlichen Angriffe auf katalanische Führungspersonen mit Spähprogrammen fordern[17],

– unter Hinweis auf den Bericht der Europäischen Kommission für Demokratie durch Recht (Venedig-Kommission) betreffend die demokratische Aufsicht der Sicherheitsdienste[18] und ihr Gutachten über das Gesetz vom 15. Januar 2016 zur Änderung des Polizeigesetzes und bestimmter anderer Gesetze in Polen[19],

– unter Hinweis auf den Bericht des Untersuchungsausschusses zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware (A9-0189/2023),

– gestützt auf Artikel 208 Absatz 12 seiner Geschäftsordnung,

A. in der Erwägung, dass dank der Bemühungen von CitizenLab, Amnesty Tech und zahlreichen investigativen Journalisten aufgedeckt wurde, dass staatliche Stellen in mehreren Ländern, sowohl in Mitgliedstaaten als auch in Drittländern, Pegasus und ähnliche Überwachungs- und Spähsoftware gegen Journalisten, Politiker, Strafverfolgungsbeamte, Diplomaten, Rechtsanwälte, Geschäftsleute, Akteure der Zivilgesellschaft und andere Akteure zu politischen und sogar kriminellen Zwecken eingesetzt haben; in der Erwägung, dass solche Praktiken äußerst besorgniserregend sind und durch sie die Gefahr des Missbrauchs von Überwachungstechnologien zur Untergrabung von grundlegenden Menschenrechten, Demokratie und Wahlprozessen deutlich wird;

B. in der Erwägung, dass unter jeder Erwähnung des Begriffs „Spähsoftware“ in diesem Bericht „Pegasus und gleichwertige Überwachungs- und Spähsoftware“ im Sinne des Beschlusses des Parlaments zur Einsetzung des PEGA-Ausschusses zu verstehen ist;

C. in der Erwägung, dass beobachtet wurde, dass staatliche Akteure Spähsoftware bewusst in irreführender Weise eingesetzt haben, indem sie Spähsoftware verwendet haben, die sich als legitimes Programm, legitime Datei oder legitimer Inhalt tarnen kann („Trojaner“), z. B. gefälschte Nachrichten von öffentlichen Einrichtungen; in der Erwägung, dass staatliche Behörden in einigen Fällen Telefonanbieter benutzt haben, um bösartige Inhalte auf das Gerät der Zielperson zu übertragen; in der Erwägung, dass Spähsoftware durch die Ausnutzung von Zero-Day-Schwachstellen eingesetzt werden kann, ohne dass die Zielperson mit den infizierten Inhalten in Berührung kommt, und dass sie nach der Deinstallation alle Spuren ihres Vorhandenseins beseitigen und die

[17] https://www.ohchr.org/en/press-releases/2023/02/spain-un-experts-demand-investigation-alleged-spying-programme-targeting
[18] https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)010-e
[19] https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)012-e

Verbindung zwischen den entfernten Betreibern und dem Server anonymisieren kann;

D. in der Erwägung, dass in den Anfängen der Mobilkommunikation das Abhören durch die Überwachung von Anrufen und später von Textnachrichten in einfachem Format erfolgte;

E. in der Erwägung, dass das Aufkommen von Anwendungen für verschlüsselte mobile Kommunikation zum Entstehen der Spähsoftware-Branche geführt hat, wobei bestehende Schwachstellen in den Betriebssystemen von Smartphones ausgenutzt werden, um Software zu installieren, mit der Spähsoftware in das Telefon importiert werden kann, die die Extraktion von Daten vor der Verschlüsselung ermöglicht, auch durch „Zero-Click"-Infektionen ohne Wissen oder Handeln des Nutzers; in der Erwägung, dass solche „Zero-Click"-Spähsoftware durch ihre Gestaltung die wirksame und sinnvolle Kontrolle ihrer Verwendung sehr schwierig macht;

F. in der Erwägung, dass die Kenntnis von Schwachstellen in Softwaresystemen direkt zwischen Parteien gehandelt wird oder dies durch Makler erleichtert wird; in der Erwägung, dass dieser Handel nichtstaatliche Akteure und kriminelle Organisationen umfasst;

G. in der Erwägung, dass der Erwerb von, der Handel mit und das Horten von Zero-Day-Schwachstellen die Integrität und Sicherheit der Kommunikation und die Cybersicherheit der Unionsbürgerinnen und -bürger grundlegend untergraben;

H. in der Erwägung, dass Überwachung durch Spähsoftware die Ausnahme bleiben sollte und immer einer wirksamen, verbindlichen und aussagekräftigen richterlichen Vorabgenehmigung durch eine unparteiische und unabhängige Justizbehörde unterliegen sollte, die sicherstellen muss, dass die Maßnahme notwendig und verhältnismäßig ist und streng auf Fälle beschränkt bleibt, die die nationale Sicherheit, Terrorismus und schwere Straftaten betreffen; in der Erwägung, dass Überwachungstechniken in Umgebungen ohne wirksame Kontrollen und Gegenkontrollen missbraucht werden können;

I. in der Erwägung, dass jede Überwachung durch Spähsoftware nachträglich von einer unabhängigen Aufsichtsbehörde überprüft werden muss, die sicherstellen muss, dass jede genehmigte Überwachung im Einklang mit den Grundrechten und den vom EuGH, dem Europäischen Gerichtshof für Menschenrechte (EGMR) und der Venedig-Kommission festgelegten Bedingungen durchgeführt wird; in der Erwägung, dass diese nachträglich überprüfende Aufsichtsbehörde umgehend die Beendigung der Überwachung anordnen sollte, wenn sich herausstellt, dass sie nicht mit den oben genannten Rechten und Bedingungen im Einklang steht;

J. in der Erwägung, dass eine Überwachung durch Spähsoftware, die nicht den Anforderungen des Unionsrechts und der Rechtsprechung des EuGH und des EGMR entspricht, eine Verletzung der in Artikel 2 EUV verankerten Werte und der in der Charta verankerten Grundrechte darstellt, insbesondere in Bezug auf Artikel 7, 8, 11, 17, 21 und 47 der Charta, in denen spezifische Rechte, Freiheiten und Grundsätze anerkannt werden, wie die Achtung des Privat- und Familienlebens, der Schutz personenbezogener Daten, die Meinungs- und Informationsfreiheit, das Recht auf Eigentum, das Recht auf Nichtdiskriminierung sowie das Recht auf einen wirksamen

Rechtsbehelf und ein faires Verfahren und die Unschuldsvermutung;

K. in der Erwägung, dass die Rechte der betroffenen Personen in der Charta und in internationalen Übereinkommen – insbesondere das Recht auf Privatsphäre und das Recht auf ein faires Verfahren – sowie in den Unionsvorschriften über die Rechte von Verdächtigen und Beschuldigten verankert sind; in der Erwägung, dass diese Rechte durch die Rechtsprechung des EuGH und des EGMR bestätigt wurden;

L. in der Erwägung, dass die Auswirkungen einer gezielten Überwachung auf Frauen besonders schwerwiegend sein können, da die Behörden die verstärkte soziale Kontrolle, der Frauen ausgesetzt sind, dazu nutzen können, private und intime Daten, die durch Spähsoftware extrahiert wurden, für Verleumdungskampagnen zu verwenden;

M. in der Erwägung, dass aus den Aussagen der ins Visier genommenen Personen eindeutig hervorgeht, dass Rechtsbehelfe und Bürgerrechte zwar auf dem Papier bestehen mögen, aber angesichts der Behinderung durch staatliche Stellen, des Fehlens bzw. der fehlenden Umsetzung des Rechts der betroffenen Personen auf Information und der administrativen Hindernisse für Einzelpersonen, die nachweisen müssen, dass sie ins Visier genommen wurden, zumeist unwirksam sind; in der Erwägung, dass es selbst in Systemen mit schnellen und offenen Verfahren aufgrund des Wesens von Spähsoftware sehr schwierig ist, den Urheber und die Art und das Ausmaß, in denen eine Person ins Visier genommen wurde, nachzuweisen;

N. in der Erwägung, dass die Gerichte die forensischen Beweise unabhängiger Sachverständiger nicht akzeptieren, sondern nur Beweise, die auf einer Untersuchung der Behörden, der Sicherheits- oder der Strafverfolgungsdienste beruhen, die angeblich hinter einem Angriff stehen; in der Erwägung, dass sich die Zielpersonen dadurch in einer paradoxen Situation befinden und keine praktikable Möglichkeit haben, eine Infektion durch Spähsoftware nachzuweisen;

O. in der Erwägung, dass die polnische Regierung institutionelle und rechtliche Schutzmechanismen, einschließlich angemessener Aufsichts- und Kontrollverfahren, geschwächt und abgeschafft hat, sodass den ins Visier genommenen Personen keine wirksamen Rechtsmittel zur Verfügung stehen; in der Erwägung, dass die Überwachungs- und Spähsoftware Pegasus zu politischen Zwecken illegal eingesetzt wurde, um Journalisten, Oppositionspolitiker, Anwälte, Staatsanwälte und Akteure der Zivilgesellschaft auszuspähen;

P. in der Erwägung, dass die ungarische Regierung institutionelle und rechtliche Schutzmechanismen, einschließlich angemessener Aufsichts- und Kontrollverfahren, geschwächt und abgeschafft hat, sodass den ins Visier genommenen Personen keine wirksamen Rechtsmittel zur Verfügung stehen; in der Erwägung, dass die Überwachungs- und Spähsoftware Pegasus zu politischen Zwecken illegal eingesetzt wurde, um Journalisten, Oppositionspolitiker, Anwälte, Staatsanwälte und Akteure der Zivilgesellschaft auszuspähen;

Q. in der Erwägung, dass offiziell bestätigt wurde, dass ein Mitglied des Europäischen Parlaments (MdEP) für Griechenland und ein griechischer Journalist vom griechischen nationalen Nachrichtendienst (EYP) sowohl abgehört als auch mit Predator-Spähsoftware ins Visier genommen wurden; in der Erwägung, dass ein ehemaliger US-

griechischer Mitarbeiter bei Meta gleichzeitig vom EYP abgehört und mit Predator-Spähsoftware, deren Verwendung nach griechischem Recht illegal ist, ins Visier genommen wurde; in der Erwägung, dass Medienberichten zufolge Abgeordnete der Opposition und der Regierungspartei in Griechenland, Parteiaktivisten und Journalisten mutmaßlich auch durch Predator-Spähsoftware oder konventionelles Abhören durch den EYP oder beides ausgespäht genommen wurden; in der Erwägung, dass die griechische Regierung bestreitet, Predator gekauft oder eingesetzt zu haben, es aber sehr wahrscheinlich ist, dass Predator von oder im Auftrag von Personen eingesetzt wurde, die dem Büro des Ministerpräsidenten sehr nahe stehen; in der Erwägung, dass die griechische Regierung zugegeben hat, dass sie Intellexa Ausfuhrlizenzen für den Verkauf der Spähsoftware Predator an repressive Regierungen wie die von Madagaskar und Sudan erteilt hat; in der Erwägung, dass die Regierung auf den Skandal mit Gesetzesänderungen reagiert hat, die das Recht von betroffenen Personen, nach einer Überwachung informiert zu werden, weiter einschränken und die Arbeit unabhängiger Behörden weiter behindern;

R. in der Erwägung, dass Enthüllungen zwei Kategorien von Spähzielen in Spanien ergeben haben; in der Erwägung, dass die erste Kategorie den Ministerpräsidenten und die Verteidigungsministerin, den Innenminister und andere hohe Amtsträger umfasst; in der Erwägung, dass die zweite Kategorie Teil dessen ist, was von der Organisation „Citizen Lab“ als „CatalanGate“ bezeichnet wird, und 65 Zielpersonen umfasst, darunter politische Persönlichkeiten der Regionalregierung von Katalonien, Mitglieder der katalanischen unabhängigkeitsbefürwortenden Bewegung, MdEP, Rechtsanwälte, Wissenschaftler und Akteure der Zivilgesellschaft; in der Erwägung, dass die spanischen Behörden im Mai 2022 eingeräumt haben, 18 Personen mit richterlicher Genehmigung ins Visier genommen zu haben, obwohl sie bislang weder die Anordnungen noch andere Informationen offengelegt haben und sich, wenn sie Rechenschaft für die Überwachung mit Spähsoftware in Spanien ablegen sollen, auf die nationale Sicherheit berufen; in der Erwägung, dass 47 weitere Personen angeblich ins Visier genommen wurden, dass darüber aber keine anderen Informationen als die von Citizen Lab vorliegen;

S. in der Erwägung, dass Behauptungen über Infektionen mit Spähsoftware in Zypern nicht bestätig wurden; in der Erwägung, dass Zypern ein wichtiges europäisches Ausfuhrzentrum für die Überwachungsindustrie und ein attraktiver Standort für Unternehmen ist, die Überwachungstechnologien verkaufen;

T. in der Erwägung, dass es deutliche Hinweise darauf gibt, dass unter anderem die Regierungen von Marokko und Ruanda hochrangige Unionsbürgerinnen und -bürger mit Spähsoftware ausspioniert haben, darunter den französischen Staatspräsidenten, den Ministerpräsidenten, die Verteidigungsministerin und den Innenminister Spaniens, den damaligen belgischen Premierminister, den ehemaligen Kommissionspräsidenten und ehemaligen italienischen Ministerpräsidenten sowie Carine Kanimba, die Tochter von Paul Rusesabagina;

U. in der Erwägung, dass mit Sicherheit davon ausgegangen werden kann, dass alle Mitgliedstaaten ein oder mehrere Spähsysteme erworben oder verwendet haben; in der Erwägung, dass die meisten Regierungen in der Europäischen Union von der unrechtmäßigen Verwendung von Spähsoftware absehen werden, dass aber in

Ermangelung eines soliden Rechtsrahmens mit Schutzmaßnahmen und Überwachung sowie angesichts der technischen Herausforderungen bei der Erkennung und Verfolgung von Infektionen die Gefahr des Missbrauchs sehr plausibel ist;

V. in der Erwägung, dass die Regierungen und Parlamente der meisten Mitgliedstaaten dem Europäischen Parlament keine aussagekräftigen Informationen über die rechtlichen Rahmenbedingungen für die Verwendung von Spähsoftware zur Verfügung gestellt haben, die über das hinausgehen, was bereits öffentlich bekannt war, obwohl sie gemäß Artikel 3 Absatz 4 des Beschlusses des Europäischen Parlaments, des Rates und der Kommission vom 6. März 1995 über die Einzelheiten der Ausübung des Untersuchungsrechts des Europäischen Parlaments dazu verpflichtet sind; in der Erwägung, dass es schwierig ist, die Durchsetzung der Rechtsvorschriften der Union und die Garantien, die Aufsicht und die Rechtsmittel zu bewerten, was einen angemessenen Schutz der Grundrechte der Bürgerinnen und Bürger verhindert;

W. in der Erwägung, dass es in Artikel 4 Absatz 3 EUV heißt: „Nach dem Grundsatz der loyalen Zusammenarbeit achten und unterstützen sich die Union und die Mitgliedstaaten gegenseitig bei der Erfüllung der Aufgaben, die sich aus den Verträgen ergeben“;

X. in der Erwägung, dass mehrere wichtige Personen aus der Spähsoftware-Branche die maltesische Staatsangehörigkeit erlangt haben, was ihre Tätigkeiten innerhalb der Union und von der Union aus erleichtert;

Y. in der Erwägung, dass viele Entwickler und Anbieter von Spähsoftware in einem oder mehreren Mitgliedstaaten eingetragen sind oder waren; in der Erwägung, dass die NSO Group mit Unternehmen in Luxemburg, Zypern, den Niederlanden und Bulgarien, die Muttergesellschaft von Intellexa, Thalestris Limited, in Irland, Griechenland, der Schweiz und Zypern, DSIRF in Österreich, Amesys und Nexa Technologies in Frankreich, Tykelab und RCS Lab in Italien und FinFisher (inzwischen aufgelöst) in Deutschland Beispiele dafür sind;

Z. in der Erwägung, dass die Europäische Union nicht am Wassenaar-Arrangement über Ausfuhrkontrollen für konventionelle Waffen sowie Güter und Technologien mit doppeltem Verwendungszweck teilnimmt; in der Erwägung, dass alle Mitgliedstaaten außer Zypern am Wassenaar-Arrangement teilnehmen, obwohl Zypern vor langer Zeit einen Antrag auf Beitritt zum Wassenaar-Arrangement gestellt hat; in der Erwägung, dass Zypern an die Verordnung über Güter mit doppeltem Verwendungszweck gebunden ist;

AA. in der Erwägung, dass die israelische Ausfuhrregelung[20] grundsätzlich für alle israelischen Staatsbürgerinnen und -bürger gilt, auch wenn sie von der EU aus tätig sind; in der Erwägung, dass Israel kein Teilnehmerland des Wassenaar-Arrangements ist, aber behauptet, dessen Standards dennoch anzuwenden;

AB. in der Erwägung, dass die Ausfuhr von Spähsoftware aus der Union in Drittländer durch die Verordnung über Güter mit doppeltem Verwendungszweck geregelt wird, die 2021 überarbeitet wurde; in der Erwägung, dass die Kommission im September 2022 ihren

[20] Verteidigungsausfuhrkontrollgesetz 5766-2007, israelisches Verteidigungsministerium.

ersten Durchführungsbericht veröffentlicht hat[21];

AC. in der Erwägung, dass sich einige Hersteller von Spähsoftware, die in Drittländer ausführen, in der Union niederlassen, um Ansehen zu gewinnen, während sie mit repressiven Regimes Handel mit Spähsoftware treiben; in der Erwägung, dass Ausfuhren aus der Union an repressive Regime oder nichtstaatliche Akteure stattfinden, was einen Verstoß gegen die EU-Ausfuhrbestimmungen darstellt;

AD. in der Erwägung, dass Amesys und Nexa Technologies derzeit in Frankreich wegen der Ausfuhr von Überwachungstechnologie nach Libyen, Ägypten und Saudi-Arabien strafrechtlich verfolgt werden; in der Erwägung, dass die Intellexa-Unternehmen mit Sitz in Griechenland Berichten zufolge ihre Produkte nach Bangladesch, Sudan, Madagaskar und in mindestens ein arabisches Land ausgeführt haben; in der Erwägung, dass die Software von FinFisher in Dutzenden von Ländern auf der ganzen Welt eingesetzt wird, darunter Angola, Bahrain, Bangladesch, Ägypten, Äthiopien, Gabun, Jordanien, Kasachstan, Myanmar, Oman, Katar, Saudi-Arabien, die Türkei und Marokko, dessen Geheimdienst von Amnesty International und Forbidden Stories beschuldigt wird, die Spähsoftware Pegasus gegen Journalisten, Menschenrechtsverteidiger, die Zivilgesellschaft und Politiker einzusetzen; in der Erwägung, dass nicht bekannt ist, ob Ausfuhrgenehmigungen für die Ausfuhr von Spähsoftware in alle diese Länder erteilt wurden;

AE. in der Erwägung, dass durch die Zahl der Teilnehmer an Rüstungsmessen und an der ISSWorld, die Spähsoftware-Funktionen vermarkten, die Vorherrschaft der Anbieter von Spähsoftware und damit zusammenhängenden Produkten und Dienstleistungen aus Drittländern deutlich wird, von denen eine beträchtliche Zahl ihren Hauptsitz in Israel haben (z. B. NSO Group, Wintego, Quadream und Cellebrite), und offenbart wird, dass bekannte Hersteller in Indien (ClearTrail), dem Vereinigten Königreich (BAE Systems und Black Cube) und den Vereinigten Arabischen Emiraten (DarkMatter) zu finden sind, während durch die United States Entity List, in der Spähsoftware-Hersteller mit Sitz in Israel (NSO Group und Candiru), Russland (Positive Technologies) und Singapur (Computer Security Initiative Consultancy PTE LTD.) auf einer schwarzen Liste aufgeführt sind, die Vielfalt der Herkunft der Spähsoftware-Hersteller noch stärker verdeutlicht wird; in der Erwägung, dass die Messe auch von zahlreichen europäischen Behörden, einschließlich örtlicher Polizeibehörden, besucht wird;

AF. in der Erwägung, dass Artikel 4 Absatz 2 EUV vorsieht, dass die nationale Sicherheit in der alleinigen Zuständigkeit der Mitgliedstaaten verbleibt;

AG. in der Erwägung, dass der EuGH jedoch entschieden hat (Rechtssache C-623/17), dass „es zwar Sache der Mitgliedstaaten [ist], ihre wesentlichen Sicherheitsinteressen festzulegen und die geeigneten Maßnahmen zu ergreifen, um ihre innere und äußere Sicherheit zu gewährleisten, doch [...] die bloße Tatsache, dass eine nationale Maßnahme zum Schutz der nationalen Sicherheit getroffen wurde, nicht dazu führen [kann], dass das Unionsrecht unanwendbar ist und die Mitgliedstaaten von der erforderlichen Beachtung dieses Rechts entbunden werden“;

AH. in der Erwägung, dass der EuGH entschieden hat (Rechtssache C-203/15), dass „Art. 15

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

Abs. 1 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 geänderten Fassung [...] im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union dahin auszulegen [ist], dass er einer nationalen Regelung entgegensteht, die für Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsieht“;

AI. in der Erwägung, dass der EuGH entschieden hat (Rechtssache C-203/15), dass „Art. 15 Abs. 1 der Richtlinie 2002/58 in der durch die Richtlinie 2009/136 geänderten Fassung [...] im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta der Grundrechte dahin auszulegen [ist], dass er einer nationalen Regelung entgegensteht, die den Schutz und die Sicherheit der Verkehrs- und Standortdaten, insbesondere den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten zum Gegenstand hat, ohne im Rahmen der Bekämpfung von Straftaten diesen Zugang ausschließlich auf die Zwecke einer Bekämpfung schwerer Straftaten zu beschränken, ohne den Zugang einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde zu unterwerfen und ohne vorzusehen, dass die betreffenden Daten im Gebiet der Union auf Vorrat zu speichern sind“;

AJ. in der Erwägung, dass die Rechtsprechung des EGMR deutlich macht, dass jede Überwachung im Einklang mit dem Gesetz erfolgen, einem legitimen Zweck dienen sowie erforderlich und verhältnismäßig sein muss; in der Erwägung, dass der Rechtsrahmen darüber hinaus präzise, wirksame und umfassende Garantien für die Anordnung, die Durchführung und mögliche Rechtsmittel gegen Überwachungsmaßnahmen bieten muss, die einer angemessenen gerichtlichen Überprüfung und einer wirksamen Aufsicht unterliegen müssen[22];

AK. in der Erwägung, dass das Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen 108), das kürzlich als Übereinkommen 108+ modernisiert wurde, für die Verarbeitung personenbezogener Daten zu Zwecken der staatlichen (nationalen) Sicherheit, einschließlich der Verteidigung, gilt; in der Erwägung, dass alle Mitgliedstaaten Vertragsparteien dieses Übereinkommens sind;

AL. in der Erwägung, dass wesentliche Aspekte des Einsatzes von Überwachungs- und Spähsoftware zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten und der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, in den Anwendungsbereich des EU-Rechts fallen;

AM. in der Erwägung, dass die Charta die Bedingungen für jede Einschränkung der Ausübung der Grundrechte festlegt, nämlich dass die Einschränkung gesetzlich vorgesehen sein muss, den Wesensgehalt der betreffenden Rechte und Freiheiten achten

[22] https://www.echr.coe.int/documents/fs_mass_surveillance_eng.pdf

muss, dem Grundsatz der Verhältnismäßigkeit unterliegen muss und nur vorgenommen werden darf, wenn sie erforderlich ist und tatsächlich den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer entspricht; in der Erwägung, dass bei der Verwendung von Spähsoftware der Eingriff in das Recht auf Privatsphäre so schwerwiegend ist, dass der Einzelne faktisch seines Rechts beraubt wird und die Verwendung nicht immer als verhältnismäßig angesehen werden kann, unabhängig davon, ob die Maßnahme als notwendig erachtet werden kann, um die legitimen Ziele eines demokratischen Staates zu erreichen;

AN. in der Erwägung, dass die Datenschutzrichtlinie für elektronische Kommunikation vorsieht, dass die Mitgliedstaaten die Vertraulichkeit der Kommunikation sicherstellen; in der Erwägung, dass der Einsatz von Überwachungsinstrumenten eine Einschränkung des durch die Datenschutzrichtlinie für elektronische Kommunikation gewährten Rechts auf Schutz von Endgeräten darstellt; in der Erwägung, dass durch solche Einschränkungen die nationalen Gesetze über Spähsoftware in den Anwendungsbereich der Datenschutzrichtlinie für elektronische Kommunikation fallen würden, ähnlich wie die nationalen Gesetze zur Vorratsdatenspeicherung; in der Erwägung, dass ein regelmäßiger Einsatz intrusiver Spähsoftware-Technologie nicht mit der Rechtsordnung der Union vereinbar wäre;

AO. in der Erwägung, dass ein Staat nach internationalem Recht nur das Recht hat, potenzielle Straftaten innerhalb seines Hoheitsgebiets zu untersuchen, und dass er auf die Unterstützung anderer Staaten zurückgreifen muss, wenn die Ermittlungen in anderen Staaten stattfinden müssen, es sei denn, es gibt eine Grundlage für die Durchführung von Ermittlungen in dem anderen Hoheitsgebiet aufgrund eines internationalen Abkommens oder – im Falle der Mitgliedstaaten – aufgrund des Unionsrechts;

AP. in der Erwägung, dass die Infektion eines Geräts mit Spähsoftware und die anschließende Erhebung von Daten über die Server von Mobilfunkdiensteanbietern erfolgen; in der Erwägung, dass das kostenlose Roaming innerhalb der Union dazu geführt hat, dass Personen manchmal Mobilfunkverträge in anderen Mitgliedstaaten als ihrem Wohnsitzmitgliedstaat abschließen, und dass es im Unionsrecht derzeit keine Rechtsgrundlage für die Erhebung von Daten in dem anderen Mitgliedstaat mittels Spähsoftware gibt;

AQ. in der Erwägung, dass der frühere Sonderberichterstatter der Vereinten Nationen zur Förderung und zum Schutz des Rechts auf Freiheit der Meinung und des Ausdrucks, David Kaye[23], und die derzeitige Sonderberichterstatterin der Vereinten Nationen zur Förderung und zum Schutz des Rechts auf Freiheit der Meinung und des Ausdrucks, Irene Khan[24], ein sofortiges Moratorium für den Einsatz, die Weitergabe und den Verkauf von Überwachungsinstrumenten fordern, bis strenge Menschenrechtsgarantien eingeführt werden, um die Praktiken zu regulieren und sicherzustellen, dass

[23] „Surveillance and human rights“, Bericht des Sonderberichterstatters zur Förderung und zum Schutz des Rechts auf Freiheit der Meinung und des Ausdrucks, A/HRC/41/35, 2019.
[24] Amt des Hohen Kommissars der Vereinten Nationen für Menschenrechte, „Spyware scandal: UN experts call for moratorium on sale of ‚life threatening‘ surveillance tech“.

Regierungen und nichtstaatliche Akteure die Instrumente auf legitime Weise einsetzen;

AR. in der Erwägung, dass es Fälle gibt, in denen Spähsoftwareunternehmen, insbesondere Intellexa, nicht nur die Abhör- und Extraktionstechnologie selbst, sondern auch den gesamten Dienst, auch als „Hacking als Dienst“ oder „aktive Cyberintelligenz“ bezeichnet, verkauft haben, wobei sie ein Paket von Überwachungs- und Abhörtechniken sowie Schulungen für Personal und technische, operative und methodische Unterstützung anbieten; in der Erwägung, dass dieser Dienst es dem Unternehmen ermöglichen könnte, Kontrolle über die gesamte Überwachungstätigkeit auszuüben und die Überwachungsdaten zu aggregieren. in der Erwägung, dass es für die zuständigen Behörden nahezu unmöglich ist, diese Praxis zu überwachen und zu kontrollieren; in der Erwägung, dass dies die Einhaltung der Grundsätze der Verhältnismäßigkeit, der Notwendigkeit, der Legitimität, der Rechtmäßigkeit und der Angemessenheit erschwert; in der Erwägung, dass dieser Dienst von der israelischen Verteidigungsagentur (DECA) nicht zugelassen ist; in der Erwägung, dass Zypern genutzt wurde, um bestehende Beschränkungen nach israelischem Recht zu umgehen, um Hacking als Dienst zu erbringen;

AS. in der Erwägung, dass die Mitgliedstaaten die Richtlinie 2014/24/EU bzw. die Richtlinie 2009/81/EG über die Vergabe öffentlicher Aufträge und die Beschaffung von Verteidigungsgütern einhalten müssen; in der Erwägung, dass sie Ausnahmen gemäß Artikel 346 Absatz 1 Buchstabe b AEUV angemessen rechtfertigen müssen, da die sensiblen Merkmale der Beschaffung im Bereich Verteidigung in der Richtlinie 2009/81/EG ausdrücklich berücksichtigt werden, und das WHO-Übereinkommen über das öffentliche Beschaffungswesen in der am 30. März 2012 geänderten Fassung[25] beachten müssen, wenn sie Partei dieses Übereinkommens sind;

AT. in der Erwägung, dass der EDSB betont hat, dass die Mitgliedstaaten die Europäische Menschenrechtskonvention und die Rechtsprechung des EGMR achten müssen, durch die die Überwachungstätigkeiten zu Zwecken der nationalen Sicherheit eingeschränkt werden; in der Erwägung, dass die Überwachung darüber hinaus, wenn sie zu Strafverfolgungszwecken eingesetzt wird, mit dem Unionsrecht und insbesondere mit der Charta sowie mit EU-Richtlinien wie der Datenschutzrichtlinie für elektronische Kommunikation und der Richtlinie zum Datenschutz bei der Strafverfolgung im Einklang stehen muss;

AU. in der Erwägung, dass Berichten zufolge große Finanzinstitute versucht haben, die Hersteller von Spähsoftware dazu zu bewegen, von der Anwendung angemessener Menschenrechtsstandards und Sorgfaltspflichten abzusehen und weiterhin Spähsoftware an repressive Regime zu verkaufen;

AV. in der Erwägung, dass Israel im Rahmen des Programms Horizont 2020 bei der Gesamtbeteiligung an dem Programm unter den assoziierten Ländern an dritter Stelle steht; in der Erwägung, dass das Horizont-Europa-Abkommen mit Israel für den Zeitraum 2021-2027 mit einem Gesamtbudget von 95,5 Mrd. EUR ausgestattet ist[26]; in der Erwägung, dass israelischen Militär- und Sicherheitsunternehmen im Rahmen dieser

[25] https://www.wto.org/english/tratop_e/gproc_e/gpa_1994_e.htm.
[26] https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/israel-joins-horizon-europe-research-and-innovation-programme-2021-12-06_de

europäischen Programme[27] Mittel zur Verfügung gestellt wurden;

AW. in der Erwägung, dass das wichtigste Rechtsinstrument für die Entwicklungspolitik der Union die Verordnung (EU) 2021/947[28] (Verordnung über das Instrument „NDICI/Europa in der Welt“) ist und dass Unionsmittel über die in der Haushaltsordnung vorgesehenen Finanzierungsarten bereitgestellt werden können; in der Erwägung, dass die Unterstützung im Falle einer Verschlechterung der Demokratie, der Menschenrechte oder der Rechtsstaatlichkeit in Drittländern ausgesetzt werden kann;

1. betont die unbestreitbare Bedeutung des Schutzes der Privatsphäre, des Rechts auf Menschenwürde und Privatsphäre, des Rechts auf Familienleben, der Meinungs- und Informationsfreiheit, der Versammlungs- und Vereinigungsfreiheit und des Rechts auf ein faires Verfahren in einer zunehmend digitalen Welt, in der immer mehr unserer Aktivitäten online stattfinden;

2. ist der festen Überzeugung, dass Verstöße gegen diese Grundrechte und Grundfreiheiten von entscheidender Bedeutung für die Achtung der in den Verträgen und in anderen Quellen festgelegten gemeinsamen Rechtsgrundsätze sind, und stellt fest, dass die Demokratie selbst auf dem Spiel steht, da der Einsatz von Spähsoftware gegen Politiker, die Zivilgesellschaft und Journalisten eine abschreckende Wirkung hat und das Recht auf friedliche Versammlung, freie Meinungsäußerung und öffentliche Beteiligung stark beeinträchtigt;

3. verurteilt aufs Schärfste den Einsatz von Spähsoftware durch Regierungen oder Mitglieder von Regierungsbehörden oder staatlichen Einrichtungen der Mitgliedstaaten zum Zwecke der Überwachung, Erpressung, Einschüchterung, Manipulation und Diskreditierung von Oppositionsmitglieder, Kritikern und der Zivilgesellschaft, der Ausschaltung der demokratischen Kontrolle und der Pressefreiheit, der Manipulation von Wahlen sowie der Untergrabung der Rechtsstaatlichkeit durch die gezielte Ausspähung von Richtern, Staatsanwälten und Rechtsanwälten zu politischen Zwecken;

4. weist darauf hin, dass durch diesen unrechtmäßigen Einsatz von Spähsoftware durch nationale Regierungen und Regierungen von Drittländern die Organe der Union und der Entscheidungsprozess direkt und indirekt beeinträchtigt werden und damit die Integrität der Demokratie in der Europäischen Union untergraben wird;

5. stellt mit großer Besorgnis fest, dass die derzeitige Governance-Struktur der Union grundsätzlich ungeeignet ist, auf Angriffe auf die Demokratie, die Grundrechte und die Rechtsstaatlichkeit aus dem Inneren der Union zu reagieren, und dass viele Mitgliedstaaten untätig bleiben; stellt fest, dass durch solche Bedrohungen in einem Mitgliedstaat die gesamte Union gefährdet wird;

---

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

28 Verordnung (EU) 2021/947 des Europäischen Parlaments und des Rates vom 9. Juni 2021 zur Schaffung des Instruments für Nachbarschaft, Entwicklungszusammenarbeit und internationale Zusammenarbeit – Europa in der Welt, zur Änderung und Aufhebung des Beschlusses Nr. 466/2014/EU des Europäischen Parlaments und des Rates und zur Aufhebung der Verordnung (EU) 2017/1601 des Europäischen Parlaments und des Rates und der Verordnung (EG, Euratom) Nr. 480/2009 des Rates (ABl. L 209 vom 14.6.2021, S. 1).

6. betont, dass die digitalen Standards für technologische Entwicklungen in der Union die Grundrechte wahren müssen;

7. vertritt den festen Standpunkt, dass die Ausfuhr von Spähsoftware aus der Union in Diktaturen und repressive Regime mit einer schlechten Menschenrechtsbilanz, in denen solche Instrumente gegen Menschenrechtsaktivisten, Journalisten und Regierungskritiker eingesetzt werden, einen schweren Verstoß gegen die in der Charta verankerten Grundrechte und eine eklatante Verletzung der Ausfuhrbestimmungen der Union darstellt;

8. äußert darüber hinaus seine Besorgnis über die unrechtmäßige Verwendung von und den unrechtmäßigen Handel mit Spähsoftware durch Mitgliedstaaten, die zusammen die Union zu einem Zielort für die Spähsoftware-Branche machen;

9. ist besorgt über die Angriffe mit Spähsoftware von Nicht-EU-Ländern auf prominente Persönlichkeiten, Menschenrechtsverteidiger und Journalisten in der Union;

10. ist ebenso besorgt über die offensichtliche Zurückhaltung bei der Untersuchung von Fällen von Spähsoftware-Missbrauch, sowohl dann, wenn es sich bei dem Verdächtigen um eine Regierungsstelle der Union handelt, als auch, wenn es sich um eine Regierungsstelle eines Drittlandes handelt; stellt fest, dass die gerichtlichen Untersuchungen von Spähsoftware-Missbrauch gegenüber Regierungschefs und Ministern der EU-Mitgliedstaaten und der Kommission sowie Mitgliedern der Zivilgesellschaft, Journalisten oder politischen Gegnern nur sehr langsam vorankommen und es ihnen an Transparenz mangelt;

11. stellt fest, dass der Rechtsrahmen einiger Mitgliedstaaten keine präzisen, wirksamen und umfassenden Garantien für die Anordnung und Durchführung von und mögliche Rechtsmittel gegen Überwachungsmaßnahmen bietet; stellt fest, dass solche Maßnahmen einem legitimen Ziel dienen sowie erforderlich und verhältnismäßig sein müssen;

12. bedauert, dass die Regierungen der Mitgliedstaaten, der Rat und die Kommission nicht uneingeschränkt an der Untersuchung mitarbeiten und nicht alle relevanten und aussagekräftigen Informationen weitergeben, um den Untersuchungsausschuss bei der Erfüllung seiner im Mandat festgelegten Aufgaben zu unterstützen; erkennt an, dass einige dieser Informationen möglicherweise strengen rechtlichen Anforderungen in Bezug auf Geheimhaltung und Vertraulichkeit unterliegen; ist der Auffassung, dass die kollektive Antwort des Rates völlig unzureichend ist und dem in Artikel 4 Absatz 3 EUV verankerten Grundsatz der loyalen Zusammenarbeit widerspricht;

13. kommt zu dem Schluss, dass offenbar weder die Mitgliedstaaten noch der Rat oder die Kommission daran interessiert sind, sich mit ganzer Kraft dafür einzusetzen, den Missbrauch von Spähsoftware umfassend zu untersuchen, und dass sie somit wissentlich die Regierungen der Union schützen, die die Menschenrechte innerhalb und außerhalb der Union verletzen;

14. kommt zu dem Schluss, dass es in Polen zu erheblichen Verstößen und Missständen bei der Umsetzung des Unionsrechts gekommen ist;

15. fordert Polen auf:

(a) die Generalstaatsanwaltschaft aufzufordern, Ermittlungen über den Missbrauch von Spähsoftware einzuleiten;

(b) dringend ausreichende institutionelle und rechtliche Garantien wiederherzustellen, einschließlich wirksamer Ex-ante- und Ex-post-Kontrollen sowie unabhängiger Aufsichtsmechanismen, einschließlich einer gerichtlichen Überprüfung der Überwachungstätigkeiten; betont, dass im Rahmen einer wirksamen Ex-ante-Kontrolle das Ersuchen an das Gericht um operative Überwachung sowie die gerichtliche Anordnung für eine solche Überwachung eine klare Begründung und Angabe der technischen Mittel für die Überwachung enthalten sollten und dass im Rahmen einer wirksamen Ex-post-Kontrolle eine Verpflichtung eingeführt werden sollte, die der Überwachung unterliegende Person über diese Tatsache, die Dauer, den Umfang und die Art und Weise der Verarbeitung der im Rahmen der operativen Überwachung erlangten Daten zu informieren;

(c) eine einheitliche Gesetzgebung zum Schutz der Bürgerinnen und Bürger einzuführen, unabhängig davon, ob die operative Überwachung von der Staatsanwaltschaft, den Geheimdiensten oder einer anderen staatlichen Einrichtung durchgeführt wird;

(d) dem Urteil des Verfassungsgerichtshofs zum Polizeigesetz von 1990 nachzukommen;

(e) dem Gutachten der Venedig-Kommission zum Polizeigesetz von 2016 nachzukommen;

(f) den verschiedenen Urteilen des EGMR zu entsprechen, wie dem Urteil in der Rechtssache *Roman Zakharov*/*Russland* aus dem Jahr 2015, in dem hervorgehoben wird, dass strenge Überwachungskriterien, eine ordnungsgemäße richterliche Genehmigung und Aufsicht, die sofortige Vernichtung irrelevanter Daten, die richterliche Kontrolle von Dringlichkeitsverfahren und die Verpflichtung zur Benachrichtigung der von Überwachungs- und Spähmaßnahmen betroffenen Personen wichtig sind, sowie dem Urteil in der Rechtssache *Klass u. a.*/*Deutschland* aus dem Jahr 1978, in dem dargelegt wird, dass die Überwachung von ausreichender Bedeutung sein muss, um einen solchen Eingriff in die Privatsphäre zu rechtfertigen;

(g) allen Urteilen des EuGH und des EGMR in Bezug auf die Unabhängigkeit der Justiz und den Vorrang des Unionsrechts zu entsprechen;

(h) den Artikel 168a des neu gefassten Gesetzes zur Änderung der Strafprozessordnung von 2016 zurückzunehmen;

(i) die volle Unabhängigkeit der Justiz wiederherzustellen und die gesetzlichen Befugnisse aller einschlägigen Aufsichtsorgane zu achten, wie des Bürgerbeauftragten, des Präsidenten des Amts für den Schutz personenbezogener Daten und des Obersten Rechnungshofes, um sicherzustellen, dass alle Aufsichtsorgane uneingeschränkte Kooperation und Zugang zu Informationen erhalten und alle Personen, die ins Visier genommen wurden, umfassend informiert werden;

(j) dringend die zufällige Zuteilung von Fällen an die Richter der Gerichte für jeden Antrag, der eingereicht wird, auch am Wochenende und außerhalb der normalen

Geschäftszeiten einzurichten, um die Auswahl „freundlicher Richter“ durch die Geheimdienste zu vermeiden, und die Transparenz eines solchen Systems sicherzustellen, indem unter anderem der Algorithmus, auf dessen Grundlage ein Richter nach dem Zufallsprinzip einem Fall zugeteilt wird, öffentlich zugänglich gemacht wird;

(k) das traditionelle System der parlamentarischen Kontrolle, bei dem die Oppositionspartei den Vorsitz des parlamentarischen Kontrollausschusses für die Sonderdienste übernimmt, wiedereinzuführen;

(l) die Situation rund um den Missbrauch von Spähsoftware in Polen dringend zu klären, um sicherzustellen, dass die Integrität der bevorstehenden Wahlen nicht infrage gestellt wird;

(m) die Richtlinie (EU) 2016/680 (Richtlinie zum Datenschutz bei der Strafverfolgung) ordnungsgemäß um- und durchsetzen und sicherstellen, dass die Datenschutzbehörde befugt ist, die Verarbeitung personenbezogener Daten unter anderem durch Behörden wie das Zentrale Amt für Korruptionsbekämpfung und die Agentur für innere Sicherheit zu überwachen;

(n) die Hinweisgeber-Richtlinie umzusetzen;

(o) von der Verabschiedung von neuen Bestimmungen über die elektronische Kommunikation, die gegen die Europäische Menschenrechtskonvention (EMRK) verstoßen, abzusehen;

(p) die Verfügbarkeit wirksamer Rechtsbehelfe für die Bürgerinnen und Bürger Polens sicherzustellen, die von der Umsetzung von Gesetzen betroffen sind, die gegen die polnische Verfassung und die EMRK verstoßen;

(q) Europol aufzufordern, alle Fälle von mutmaßlichem Missbrauch von Spähsoftware zu untersuchen;

(r) eine unabhängige verfassungsrechtliche Überprüfung der Gesetze in Polen sicherzustellen;

(s) die Unabhängigkeit der Rolle des Generalstaatsanwalts vom Justizminister wiederherzustellen, um sicherzustellen, dass die Ermittlungen bei mutmaßlichen Grundrechtsverletzungen frei von politischen Erwägungen sind;

16. fordert die Kommission dringend auf, die Vereinbarkeit des polnischen Gesetzes von 2018 über den Schutz personenbezogener Daten, die im Zusammenhang mit der Verhütung und Bekämpfung von Verbrechen verarbeitet werden, mit der EU-Richtlinie zum Datenschutz bei der Strafverfolgung zu prüfen und gegebenenfalls ein Vertragsverletzungsverfahren einzuleiten;

17. kommt zu dem Schluss, dass es in Ungarn zu erheblichen Verstößen und Missständen bei der Umsetzung des Unionsrechts gekommen ist;

18. fordert Ungarn auf:

(a) dringend ausreichende institutionelle und rechtliche Garantien wiederherzustellen, einschließlich wirksamer, verbindlicher Ex-ante- und Ex-post-Kontrollen sowie unabhängiger Aufsichtsmechanismen, einschließlich der gerichtlichen Überprüfung von Überwachungstätigkeiten; betont, dass im Rahmen einer wirksamen Ex-ante-Kontrolle das Ersuchen an das Gericht um operative Überwachung sowie die gerichtliche Anordnung für eine solche Überwachung eine klare Begründung und Angabe der technischen Mittel für die Überwachung enthalten sollten und dass im Rahmen einer wirksamen Ex-post-Kontrolle eine Verpflichtung eingeführt werden sollte, die der Überwachung unterliegende Person über diese Tatsache, die Dauer, den Umfang und die Art und Weise der Verarbeitung der im Rahmen der operativen Überwachung erlangten Daten zu informieren;

(b) den verschiedenen Urteilen des EGMR zu entsprechen, wie dem Urteil in der Rechtssache *Roman Zakharov*/*Russland* aus dem Jahr 2015, in dem hervorgehoben wird, dass strenge Überwachungskriterien, eine ordnungsgemäße richterliche Genehmigung und Aufsicht, die sofortige Vernichtung irrelevanter Daten, die richterliche Kontrolle von Dringlichkeitsverfahren und die Verpflichtung zur Benachrichtigung der von Überwachungs- und Spähmaßnahmen betroffenen Personen wichtig sind, sowie dem Urteil in der Rechtssache *Klass u. a.*/*Deutschland* aus dem Jahr 1978, in dem dargelegt wird, dass die Überwachung von ausreichender Bedeutung sein muss, um einen solchen Eingriff in die Privatsphäre zu rechtfertigen, und dass die überwachten Personen darüber unterrichtet werden müssen;

(c) allen Urteilen des EuGH und des EGMR in Bezug auf die Unabhängigkeit der Justiz und den Vorrang des Unionsrechts zu entsprechen;

(d) unabhängige Aufsichtsgremien im Einklang mit dem Urteil des EGMR in der Rechtssache *Hüttl*/*Ungarn* wiedereinzusetzen, in dem das Gericht feststellt, dass die Nationale Behörde für Datenschutz und Informationsfreiheit (NAIH) nicht in der Lage ist, eine unabhängige Aufsicht über die Verwendung von Spähsoftware durchzuführen, da die Geheimdienste berechtigt sind, den Zugang zu bestimmten Dokumenten unter Berufung auf die Geheimhaltung zu verweigern;

(e) die vollständige Unabhängigkeit der Justiz und aller einschlägigen Aufsichtsorgane wiederherzustellen, wie des Bürgerbeauftragten und der Datenschutzbehörden, um sicherzustellen, dass alle Aufsichtsorgane uneingeschränkte Kooperation und Zugang zu Informationen erhalten und alle Personen, die ins Visier genommen wurden, umfassend informiert werden;

(f) wieder unabhängige Mitarbeiter in Führungspositionen in Aufsichtsgremien einzusetzen, wie dem Verfassungsgericht, dem Obersten Gerichtshof, dem Rechnungshof, der Staatsanwaltschaft, der Ungarischen Nationalbank und dem Nationalen Wahlausschuss;

(g) die Hinweisgeber-Richtlinie umzusetzen;

(h) Europol aufzufordern, alle Fälle von mutmaßlichem Missbrauch von Spähsoftware zu untersuchen;

(i) von der Verabschiedung von neuen Bestimmungen über die elektronische

Kommunikation, die gegen die EMRK verstoßen, abzusehen;

(j) die Verfügbarkeit wirksamer Rechtsbehelfe für die Bürgerinnen und Bürger Ungarns sicherzustellen, die von der Umsetzung von Gesetzen betroffen sind, die gegen die ungarische Verfassung und die EMRK verstoßen;

19. kommt zu dem Schluss, dass es in Griechenland zu Verstößen und Missständen bei der Umsetzung des Unionsrechts gekommen ist;

20. fordert Griechenland auf:

(a) dringend institutionelle und rechtliche Garantien wiederherzustellen und zu stärken, einschließlich wirksamer Ex-ante- und Ex-post-Kontrollen sowie unabhängiger Aufsichtsmechanismen;

(b) alle Ausfuhrgenehmigungen, die nicht in vollem Umfang mit der Verordnung über Güter mit doppeltem Verwendungszweck in Einklang stehen, dringend aufzuheben und den Vorwürfen illegaler Ausfuhren, u. a. in den Sudan, nachzugehen;

(c) sicherzustellen, dass die Behörden frei und ungehindert allen Behauptungen über den Einsatz von Spähsoftware nachgehen können;

(d) die Abänderung 826/145 des Gesetzes 2472/1997, mit der die Möglichkeit der Hellenischen Behörde für Kommunikationssicherheit und Datenschutz (ADAE), die Bürgerinnen und Bürger über die Aufhebung der Vertraulichkeit von Mitteilungen zu informieren, abgeschafft wurde, dringend zurückzuziehen; das Gesetz Nr. 5002/2022 zu ändern, um das Recht der betroffenen Personen, auf Antrag sofortige Information zu erhalten, sobald die Überwachung abgeschlossen ist, wiederherzustellen und andere Bestimmungen zu berichtigen, die die Garantien, die Kontrolle und die Rechenschaftspflicht schwächen;

(e) die vollständige Unabhängigkeit der Justiz und aller einschlägigen Aufsichtsorgane wiederherzustellen, wie des Bürgerbeauftragten und der Datenschutzbehörden, und die Unabhängigkeit der ADAE vollständig zu achten, um sicherzustellen, dass alle Aufsichts- und Überwachungsorgane uneingeschränkt Kooperation und Zugang zu Informationen erhalten und alle Personen, die ins Visier genommen wurden, umfassend informiert werden;

(f) dafür zu sorgen, dass die ADAE ein elektronisches Archiv einrichten kann, um ihre Aufgabe erfüllen zu können;

(g) die Situation rund um den Missbrauch von Spähsoftware in Griechenland dringend zu klären, um sicherzustellen, dass die Integrität der bevorstehenden Wahlen nicht infrage gestellt wird;

(h) die Gesetzesänderung von 2019 rückgängig zu machen, mit der der nationale Nachrichtendienst (EYP) der direkten Kontrolle des Premierministers unterstellt wurde; verfassungsrechtliche Garantien sicherzustellen und eine parlamentarische Kontrolle der Arbeit des Nachrichtendienstes zu ermöglichen, ohne dass der Vorwand der Vertraulichkeit von Informationen vorgeschoben werden kann;

(i) die Unabhängigkeit der Führung der nationalen Transparenzbehörde (EAD) sicherzustellen;

(j) sicherzustellen, dass die Justiz über alle notwendigen Mittel und Unterstützung verfügt, um den mutmaßlichen Spähsoftware-Missbrauch zu untersuchen und physische Beweise von Proxys, Maklerfirmen und Spähsoftware-Anbietern zu beschlagnahmen, die mit den Infektionen durch Spähsoftware in Verbindung stehen;

(k) Europol aufzufordern, sich unverzüglich an den Ermittlungen zu beteiligen;

(l) eine politische Einmischung in die Arbeit des Generalstaatsanwalts zu unterlassen;

21. kommt zu dem Schluss, dass der Rechtsrahmen in Spanien insgesamt mit den Anforderungen der Verträge im Einklang steht; weist jedoch darauf hin, dass einige Reformen erforderlich sind und dass die Umsetzung in der Praxis voll und ganz im Einklang mit den Grundrechten stehen und den Schutz der Öffentlichkeitsbeteiligung gewährleisten muss;

22. fordert Spanien daher auf:

(a) eine umfassende, faire und wirksame Untersuchung durchzuführen, in der alle mutmaßlichen Fälle des Einsatzes von Spähsoftware, einschließlich der 47 Fälle, in denen noch unklar ist, ob die betroffenen Personen vom spanischen nationalen Nachrichtendienst (CNI) mit einer gerichtlichen Anordnung ins Visier genommen wurden oder ob eine andere Behörde gerichtliche Anordnungen erhalten hat, um sie rechtmäßig ins Visier zu nehmen, sowie die Verwendung von Spähsoftware gegen den Premierminister und Mitglieder der Regierung vollständig geklärt sind, und die Ergebnisse im Einklang mit den geltenden Gesetzen so weit wie möglich vorzulegen;

(b) den betroffenen Personen angemessenen Zugang zu der vom Obersten Gerichtshof erteilten richterlichen Genehmigung an das CNI, um 18 Personen ins Visier zu nehmen, zu gewähren;

(c) mit den Gerichten zusammenzuarbeiten, um sicherzustellen, dass Personen, die mit Spähsoftware ins Visier genommen werden, Zugang zu echten und sinnvollen Rechtsbehelfen haben und dass gerichtliche Ermittlungen unverzüglich unparteiisch und gründlich abgeschlossen werden, wofür ausreichende Ressourcen bereitgestellt werden sollten;

(d) die Reform des Rechtsrahmens des CNI einzuleiten, wie im Mai 2022 angekündigt;

(e) Europol, das mit technischem Fachwissen einen Beitrag leisten könnte, aufzufordern, sich an den Ermittlungen zu beteiligen;

23. kommt zu dem Schluss, dass es Beweise für Missstände bei der Umsetzung der EU-Verordnung über Güter mit doppeltem Verwendungszweck in Zypern gibt, die eine genaue Überprüfung erfordern;

24. fordert Zypern auf:

(a) alle für Spähsoftware erteilten Ausfuhrgenehmigungen gründlich zu prüfen und gegebenenfalls aufzuheben;

(b) die Verbringung von Spähsoftware-Material zwischen Mitgliedstaaten innerhalb des EU-Binnenmarkts eingehend zu prüfen und die unterschiedlichen israelischen Unternehmen bzw. Unternehmen im Besitz und unter der Leitung israelischer Bürgerinnen und Bürger, die in Zypern registriert und an derartigen Tätigkeiten beteiligt sind, zu erfassen;

(c) den Bericht des Sonderbeauftragten zum Fall „Spyware Van“ freizugeben, wie vom Ausschuss während seiner offiziellen Reise nach Zypern gefordert;

(d) mit Unterstützung von Europol alle Behauptungen über den unrechtmäßigen Einsatz und die Ausfuhr von Spähsoftware, insbesondere gegen Journalisten, Rechtsanwälte, Akteure der Zivilgesellschaft und zyprische Bürgerinnen und Bürger, umfassend zu untersuchen;

25. ist der Ansicht, dass die Lage in einigen anderen Mitgliedstaaten ebenfalls Anlass zur Sorge gibt, insbesondere angesichts der Existenz einer lukrativen und expandierenden Spähsoftware-Branche, die vom guten Ruf, dem Binnenmarkt und der Freizügigkeit der Union profitiert und einige Mitgliedstaaten wie Zypern und Bulgarien in die Lage versetzt, zu einer Drehscheibe für die Ausfuhr von Spähsoftware an repressive Regime in aller Welt zu werden

26. ist der Auffassung, dass das Versagen oder die Weigerung einiger nationaler Behörden, einen angemessenen Schutz für die Bürgerinnen und Bürger der Union sicherzustellen, wozu auch Regelungslücken und das Fehlen geeigneter Rechtsinstrumente zählen, mit aller gebotenen Deutlichkeit aufzeigen, dass Maßnahmen auf Unionsebene unerlässlich sind, um dafür zu sorgen, dass der Wortlaut der Verträge eingehalten wird und die Rechtsvorschriften der Union beachtet werden, damit das Recht der Bürger, in einem sicheren Umfeld zu leben, in dem Menschenwürde, Privatleben, personenbezogene Daten und Eigentum im Sinne der Richtlinie 2012/29/EU, gemäß der jedes Opfer einer Straftat ein Recht auf Unterstützung und Schutz entsprechend seinen individuellen Bedürfnissen hat, geachtet wird;

27. kommt zu dem Schluss, dass bei der Umsetzung des Unionsrechts schwerwiegende Mängel unterlaufen sind, als die Kommission und der Europäische Auswärtige Dienst (EAD) Drittländern, darunter auch zehn Ländern in der Sahelzone, Unterstützung für den Aufbau von Überwachungskapazitäten gewährt haben[29];

28. vertritt den Standpunkt, dass der Handel mit und die Verwendung von Spähsoftware streng geregelt werden muss; ist sich jedoch darüber im Klaren, dass der Gesetzgebungsprozess längere Zeit benötigen könnte, während dem Missbrauch umgehend ein Ende gesetzt werden muss; fordert die Annahme von Bedingungen für die rechtmäßige Nutzung, den Verkauf, den Erwerb und die Weitergabe von Spähsoftware; besteht darauf, dass die Mitgliedstaaten für einen fortgesetzten Einsatz von Spähsoftware bis zum 31. Dezember 2023 alle folgenden Bedingungen erfüllen

[29] Entscheidung in der Rechtssache 1904/2021/MHZ, abrufbar unter https://www.ombudsman.europa.eu/de/decision/de/163491.

müssen:

(a) Alle Fälle von mutmaßlichem Missbrauch von Spähsoftware werden von den zuständigen Strafverfolgungs-, Staatsanwaltschafts- und Justizbehörden umfassend untersucht und unverzüglich aufgeklärt;

(b) sie weisen nach, dass der Rahmen für den Einsatz von Spähsoftware mit den von der Venedig-Kommission festgelegten Standards und der einschlägigen Rechtsprechung des EuGH und des EGMR im Einklang steht;

(c) sie geben die ausdrückliche Zusage, Europol gemäß Artikel 4, 5 und 6 der Europol-Verordnung bei Ermittlungen wegen des Verdachts der unrechtmäßigen Verwendung von Spähsoftware einzubeziehen und

(d) dass alle Ausfuhrgenehmigungen, die nicht vollständig mit der Verordnung über Güter mit doppeltem Verwendungszweck im Einklang stehen, aufgehoben werden;

29. ist der Auffassung, dass die Erfüllung dieser Bedingungen von der Kommission bis zum 30. November 2023 bewertet werden muss; ist ferner der Ansicht, dass die Ergebnisse der Bewertung in einem öffentlichen Bericht offengelegt werden müssen;

30. betont, dass die Bekämpfung von Schwerkriminalität und Terrorismus sowie die Fähigkeit, dies zu tun, für die Mitgliedstaaten zwar von entscheidender Bedeutung sind, der Schutz der Grundrechte und der Demokratie jedoch unerlässlich ist. betont ferner, dass der Einsatz von Spähsoftware durch die Mitgliedstaaten verhältnismäßig sein muss und nicht willkürlich erfolgen darf und dass die Überwachung nur unter eng begrenzten, vorher festgelegten Umständen genehmigt werden darf; ist der Auffassung, dass wirksame Ex-ante-Mechanismen zur Sicherstellung der gerichtlichen Kontrolle für den Schutz der individuellen Freiheiten von entscheidender Bedeutung sind; bekräftigt, dass die Rechte des Einzelnen nicht gefährdet werden dürfen, indem ein uneingeschränkter Zugang zur Überwachung ermöglicht wird; unterstreicht, dass es ebenfalls wichtig ist, dass die Justiz in der Lage ist, eine substanzielle und wirksame Ex-post-Kontrolle im Bereich der Überwachungsanträge für Zwecke der nationalen Sicherheit durchzuführen, um sicherzustellen, dass ein unverhältnismäßiger Einsatz von Spähsoftware durch Regierungen angefochten werden kann;

31. betont, dass der Einsatz von Spähsoftware für die Strafverfolgung direkt durch Maßnahmen auf der Grundlage von Titel 5 Kapitel 4 AEUV über die justizielle Zusammenarbeit in Strafsachen geregelt werden sollte; betont, dass die Konfiguration von Spähsoftware, die in die EU eingeführt und anderweitig in Verkehr gebracht wird, durch eine Maßnahme auf der Grundlage von Artikel 114 AEUV geregelt werden sollte; stellt fest, dass der Einsatz von Spähsoftware für Zwecke der nationalen Sicherheit nur indirekt geregelt werden kann, z. B. durch Grundrechte und Datenschutzvorschriften;

32. ist der Auffassung, dass aufgrund der transnationalen Dimension und der EU-Dimension des Einsatzes von Spähsoftware eine koordinierte und transparente Kontrolle auf EU-Ebene erforderlich ist, um nicht nur den Schutz der EU-Bürgerinnen und -Bürger, sondern auch die Gültigkeit von Beweismitteln, die durch Spähsoftware in grenzüberschreitenden Fällen gesammelt wurden, sicherzustellen, und dass auf der

Grundlage von Titel 5 Kapitel 4 AEUV ein eindeutiger Bedarf an gemeinsamen EU-Normen besteht, die den Einsatz von Spähsoftware durch Stellen der Mitgliedstaaten regeln und sich auf die vom EuGH, vom EGMR, von der Venedig-Kommission und der Agentur für Grundrechte[30] festgelegten Standards stützen; ist der Ansicht, dass solche EU-Normen zumindest die folgenden Elemente berücksichtigen sollten:

(a) Der geplante Einsatz von Spähsoftware sollte nur in besonderen Ausnahmefällen zum Schutz der nationalen Sicherheit genehmigt werden und einer wirksamen, verbindlichen und aussagekräftigen richterlichen Vorabgenehmigung durch eine unparteiische und unabhängige Justizbehörde oder ein sonstiges unabhängiges demokratisches Aufsichtsgremium unterliegen, die bzw. das Zugang zu allen einschlägigen Informationen hat, aus denen sich die Notwendigkeit und Verhältnismäßigkeit der geplanten Maßnahme ergibt;

(b) die gezielte Überwachung mit Spähsoftware sollte nur so lange dauern wie unbedingt erforderlich, die richterliche Vorabgenehmigung sollte den genauen Umfang und die Dauer für jedes Gerät, auf das zugegriffen wird, festlegen, und das Hacking darf nur verlängert werden, wenn eine weitere richterliche Genehmigung für eine andere festgelegte Dauer erteilt wird, da es sich um Spähsoftware handelt und die Möglichkeit einer rückwirkenden Überwachung besteht. Die Behörden der Mitgliedstaaten sollten außerdem nur einzelne Endgeräte oder Konten von Betroffenen ins Visier nehmen und davon absehen, Anbieter von Internet- und Technologiediensten zu hacken, um zu vermeiden, dass nicht betroffene Nutzer in Mitleidenschaft gezogen werden;

(c) die Genehmigung für den Einsatz von Spähsoftware darf nur in Ausnahmefällen für Ermittlungen in einer eingeschränkten und abschließenden Aufzählung von eindeutig und präzise definierten schweren Straftaten erteilt werden, die eine tatsächliche Bedrohung für die nationale Sicherheit darstellen, und Spähsoftware darf nur gegen Personen eingesetzt werden, bei denen hinreichende Anhaltspunkte dafür vorliegen, dass sie solche schweren Straftaten begangen haben oder planen;

(d) Daten, die durch Vorrechte oder Immunitäten in Bezug auf bestimmte Personengruppen (z. B. Politiker, Ärzte usw.) oder besonders geschützte Beziehungen (z. B. das Anwaltsgeheimnis) oder durch Vorschriften über die Feststellung und Beschränkung der strafrechtlichen Verantwortlichkeit im Zusammenhang mit der Pressefreiheit und der Freiheit der Meinungsäußerung in anderen Medien geschützt sind, dürfen nicht mithilfe von Spähsoftware abgefragt werden, es sei denn, es liegen unter richterlicher Aufsicht hinreichende Gründe vor, die die Beteiligung an kriminellen Machenschaften oder Angelegenheiten der nationalen Sicherheit bestätigen, für die ein gemeinsamer Rahmen gelten sollte;

(e) für die Überwachung mit der Spähsoftware-Technologie müssen besondere Regeln aufgestellt werden, da sie einen unbegrenzten rückwirkenden Zugriff auf Nachrichten, Dateien und Metadaten ermöglicht;

(f) die Mitgliedstaaten sollten zumindest die Zahl der genehmigten und abgelehnten

[30] Agentur für Grundrechte, *Überwachung durch Nachrichtendienste: Grundrechtsschutz und Rechtsbehelfe in der Europäischen Union – Teil II - Zusammenfassung*, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2-summary_de.pdf

Anträge auf Überwachung sowie die Art und den Zweck der Untersuchung veröffentlichen und jede Untersuchung anonym in einem nationalen Register mit einer eindeutigen Kennung registrieren, damit sie im Falle eines Missbrauchsverdachts untersucht werden kann;

(g) die nationalen Kontrollstellen sollten den Mitgliedstaaten Bericht erstatten, und die Mitgliedstaaten sollten der Kommission diese Informationen anschließend regelmäßig mitteilen. Die Kommission sollte diese Informationen in ihrem jährlichen Bericht über die Rechtsstaatlichkeit einfließen lassen, damit die Verwendung von Spähsoftware in den Mitgliedstaaten vergleichbar ist;

(h) das Recht auf Benachrichtigung der betroffenen Person: Nach Beendigung der Überwachung sollten die Behörden die Personen darüber informieren, dass sie von den Behörden mit Spähsoftware überwacht wurden, darunter Informationen über das Datum und die Dauer der Überwachung, die für die Überwachung ausgestellte Anordnung, die erhaltenen Daten, Informationen darüber, wie und von welchen Akteuren diese Daten verwendet wurden, das Datum der Löschung der Daten sowie das Recht und die praktischen Modalitäten, bei den zuständigen Behörden administrative und gerichtliche Rechtsmittel einzulegen; stellt fest, dass eine solche Benachrichtigung ohne ungebührliche Verzögerung übermittelt werden sollte, es sei denn, eine unabhängige Justizbehörde gewährt einen Aufschub der Benachrichtigung für den Fall, dass eine sofortige Benachrichtigung den Zweck der Überwachung ernsthaft gefährden würde;

(i) das Recht auf Benachrichtigung von Personen, auf deren Daten zugegriffen wurde, die nicht zu den Zielpersonen gehören: Nach Ablauf des Zeitraums, für den die Überwachung genehmigt wurde, sollten die Behörden die Personen benachrichtigen, deren Recht auf Privatsphäre durch den Einsatz von Spähsoftware stark beeinträchtigt wurde, die aber nicht Ziel der Operation waren. Die Behörden sollten diese Person benachrichtigen, dass deren Daten von den Behörden eingesehen wurden, und Informationen über das Datum und die Dauer der Überwachung, die für die Überwachung ausgestellte Anordnung, die erhaltenen Daten, darüber, wie und von welchen Akteuren diese Daten verwendet wurden, sowie das Datum der Löschung der Daten bereitstellen; stellt fest, dass eine solche Benachrichtigung ohne ungebührliche Verzögerung übermittelt werden sollte, es sei denn, eine unabhängige Justizbehörde gewährt einen Aufschub der Benachrichtigung für den Fall, dass eine sofortige Benachrichtigung den Zweck der Überwachung ernsthaft gefährden würde;

(j) eine wirksame, verbindliche und unabhängige Ex-post-Kontrolle über den Einsatz von Spähsoftware, wobei die dafür zuständigen Stellen über alle erforderlichen Mittel und Befugnisse verfügen müssen, um eine sinnvolle Kontrolle auszuüben, die mit einer parteiübergreifenden parlamentarischen Kontrolle mit entsprechender Freigabe und einem uneingeschränkten Zugang zu hinreichenden Informationen gekoppelt sein muss, um sich zu vergewissern, dass die Überwachung rechtmäßig und verhältnismäßig war; die parlamentarische Aufsicht über sensible vertrauliche Informationen sollte durch erforderliche Infrastrukturen, Verfahren und Sicherheitsüberprüfungen erleichtert werden. Unabhängig von der Definition oder Abgrenzung des Begriffs der nationalen Sicherheit müssen die nationalen Aufsichtsgremien für die gesamte Bandbreite der nationalen Sicherheit zuständig sein;

(k) die Grundprinzipien eines ordnungsgemäßen Verfahrens und der gerichtlichen Kontrolle müssen im Mittelpunkt der Regelung für Überwachungsspähsoftware stehen;

(l) einen sinnvollen Rechtsbehelf für direkte und indirekte Zielpersonen und die Tatsache, dass Personen, die nach ihren eigenen Angaben von der Überwachung beeinträchtigt werden, Zugang zu Rechtsmitteln durch eine unabhängige Stelle haben müssen; fordert daher die Einführung einer Meldepflicht für staatliche Behörden, einschließlich angemessener Fristen für die Meldung, wobei die Zustellung erfolgt, sobald die Sicherheitsbedrohung vorüber ist;

(m) Rechtsbehelfe müssen sowohl rechtlich als auch faktisch wirksam sowie bekannt und zugänglich sein; betont, dass für solche Rechtsbehelfe eine zügige, gründliche und unparteiische Untersuchung durch ein unabhängiges Aufsichtsgremium erforderlich ist und dass dieses Gremium über Zugang sowie Fachwissen und technische Fähigkeiten verfügen sollte, um alle relevanten Daten zu verarbeiten, damit es feststellen kann, ob die von den Behörden vorgenommene Sicherheitsbewertung einer Person zuverlässig und verhältnismäßig ist; in Fällen, in denen ein Missbrauch nachweislich festgestellt wurde, sollten – je nach den einschlägigen nationalen Rechtsvorschriften in den Mitgliedstaaten – angemessene Sanktionen, entweder strafrechtlicher oder verwaltungsrechtlicher Art, verhängt werden;

(n) die Verbesserung des kostenlosen Zugangs der betroffenen Personen zu technologischem Fachwissen in dieser Phase, da die bessere Verfügbarkeit und Erschwinglichkeit technologischer Verfahren, wie z. B. forensischer Analysen, es den betroffenen Personen ermöglichen würde, vor Gericht stichhaltigere Argumente vorzubringen, und die Vertretung der betroffenen Personen vor Gericht durch den Ausbau der technologischen Kapazitäten der Rechtsvertretungen und der Justiz stärken würde, damit die betroffenen Personen besser beraten werden, Verstöße zu erkennen und die Überwachung des Missbrauchs von Spähsoftware und die Rechenschaftspflicht darüber zu verbessern;

(o) die Stärkung der Verteidigungsrechte und des Rechtes auf ein faires Verfahren, indem sichergestellt wird, dass Personen, die einer Straftat beschuldigt werden, die Richtigkeit, Echtheit, Verlässlichkeit und sogar Rechtmäßigkeit der gegen sie verwendeten Beweise überprüfen können und dürfen, sodass daher jede pauschale Anwendung der nationalen Vorschriften über das Verteidigungsgeheimnis abgelehnt wird;

(p) während der Überwachung sollten die Behörden alle Daten löschen, die für die genehmigten Ermittlungen irrelevant sind, und nach Abschluss der Überwachung und der Ermittlungen, für die die Genehmigung erteilt wurde, sollten die Behörden die Daten sowie alle damit zusammenhängenden Dokumente, wie z. B. Notizen, die während dieses Zeitraums angefertigt wurden, löschen, und diese Löschung muss aufgezeichnet werden und nachprüfbar sein;

(q) einschlägige Informationen, die durch Spähsoftware erlangt werden, sollten nur für befugte Behörden und ausschließlich für den Zweck einer Operation zugänglich sein. Dieser Zugang sollte auf einen bestimmten, im Gerichtsverfahren festgelegten Zeitraum beschränkt sein;

(r) es müssen Mindeststandards für die Rechte des Einzelnen in Strafverfahren hinsichtlich

der Zulässigkeit von Beweisen festgelegt werden, die mithilfe von Spähsoftware gesammelt wurden. Die Möglichkeit falscher oder manipulierter Informationen, die durch den Einsatz von Spähsoftware erzeugt wurden (Impersonation), muss in das Strafprozessrecht aufgenommen werden;

(s) die Mitgliedstaaten müssen sich gegenseitig benachrichtigen, wenn Bürger oder Einwohner eines anderen Mitgliedstaats oder eine Mobilfunknummer eines Betreibers in einem anderen Mitgliedstaat überwacht werden;

(t) die Überwachungssoftware muss eine Markierung enthalten, damit die Aufsichtsorgane bei einem Missbrauchsverdacht den Verursacher eindeutig identifizieren können. Die obligatorische Signatur für jeden Einsatz von Spähsoftware sollte aus einer individuellen Kennzeichnung der handelnden Behörde, der Art der verwendeten Spähsoftware und einer anonymisierten Fallnummer bestehen;

33. fordert die Mitgliedstaaten auf, öffentliche Konsultationen mit den Betroffenen durchzuführen, die Transparenz des Gesetzgebungsverfahrens sicherzustellen und bei der Ausarbeitung neuer Rechtsvorschriften über die Verwendung und den Verkauf von Spähsoftware EU-Standards und -Schutzmaßnahmen zu berücksichtigen;

34. betont, dass nur Spähsoftware, die so konzipiert ist, dass durch sie die Funktionalität von Spähsoftware gemäß dem Rechtsrahmen nach Ziffer 29 ermöglicht und erleichtert wird, auf dem Binnenmarkt in Verkehr gebracht, entwickelt oder in der Union verwendet werden darf; bekräftigt, dass eine solche Verordnung über das Inverkehrbringen von Spähsoftware, die von sich aus auf Rechtsstaatlichkeit auf der Grundlage von Artikel 114 AEUV bedacht ist, den Bürgerinnen und Bürgern der Union ein hohes Schutzniveau bieten sollte; ist der Ansicht, dass es nicht zu rechtfertigen ist, dass die Verordnung über Güter mit doppeltem Verwendungszweck Bürgerinnen und Bürgern von Drittländern zwar seit 2021 Schutz vor der Ausfuhr von Spähsoftware aus der EU bietet, den EU-Bürgern und -Bürgerinnen jedoch kein gleichwertiger Schutz gewährt wird;

35. ist der Ansicht, dass nur Abhör- und Extraktionstechnologie von Unternehmen in der EU verkauft und von den Mitgliedstaaten erworben werden darf und nicht „Hacking als Dienstleistung“, was die Bereitstellung technischer, operativer und methodischer Unterstützung der Überwachungstechnologie einschließt und dem Anbieter den Zugang zu einer unverhältnismäßig großen Menge an Daten ermöglicht, der mit den Grundsätzen der Verhältnismäßigkeit, Notwendigkeit, Legitimität, Rechtmäßigkeit und Angemessenheit unvereinbar ist; fordert die Kommission auf, diesbezüglich einen Gesetzgebungsvorschlag vorzulegen;

36. betont, dass Spähsoftware nur für den Verkauf an und die Verwendung durch Behörden in Verkehr gebracht werden darf, die in einer abschließenden Aufzählung genannt werden und deren Auftrag die Untersuchung von Straftaten oder den Schutz der nationalen Sicherheit umfasst, wofür der Einsatz von Spähsoftware genehmigt werden kann; ist der Ansicht, dass Sicherheitsbehörden nur dann Spähsoftware einsetzen sollten, wenn alle Empfehlungen der Agentur für Grundrechte umgesetzt wurden[31];

[31] https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2-

37. hebt die Verpflichtung hervor, eine Version von Spähsoftware zu verwenden, die so gestaltet ist, dass sie den Zugriff auf sämtliche auf einem Gerät gespeicherte Daten minimiert und dass der Zugriff auf Daten auf das für den Zweck der genehmigten Untersuchung unbedingt erforderliche Mindestmaß beschränkt ist;

38. kommt zu dem Schluss, dass es möglich sein muss, den Erwerb von Spähsoftware durch einen Mitgliedstaat von einer unabhängigen und unparteiischen Prüfstelle mit entsprechender Freigabe prüfen zu lassen;

39. betont, dass alle Unternehmen, die Spähsoftware auf dem Binnenmarkt in Verkehr bringen, strenge Sorgfaltspflichten einhalten sollten und dass Unternehmen, die sich bei einem öffentlichen Vergabeverfahren als Lieferanten bewerben, einem Überprüfungsverfahren unterzogen werden sollten, bei dem es auch um die Reaktion des Unternehmens auf Menschenrechtsverletzungen mit ihrer Software und um die Frage geht, ob sich die Technologie auf Daten stützt, die in undemokratischen und missbräuchlichen Überwachungspraktiken gesammelt wurden; betont, dass die zuständigen nationalen Aufsichtsbehörden der Kommission jährlich über die Einhaltung der Vorschriften Bericht erstatten sollten;

40. betont, dass Unternehmen, die Überwachungstechnologien oder -dienste für staatliche Akteure anbieten, den zuständigen nationalen Aufsichtsbehörden die Art der Ausfuhrgenehmigungen offenlegen sollten;

41. unterstreicht, dass die Mitgliedstaaten eine „Cooling-off"-Frist festlegen sollten, in der es ehemaligen Mitarbeitern von Regierungsstellen oder -behörden untersagt ist, für Spähsoftware-Firmen zu arbeiten;

Notwendigkeit, den Begriff der nationalen Sicherheit abzustecken

42. ist besorgt über Fälle, in denen man sich in ungerechtfertigter Weise auf die „nationale Sicherheit" berufen hat, um den Einsatz und die Verwendung von Spähsoftware, die Sicherstellung absoluter Geheimhaltung und die fehlende Rechenschaftspflicht zu begründen; begrüßt die im Einklang mit der Rechtsprechung des EuGH[32] stehende Erklärung der Kommission, dass ein bloßer Verweis auf die nationale Sicherheit nicht als unbegrenzte Ausnahme von der Anwendung des Unionsrechts ausgelegt werden kann und einer klaren Begründung bedarf, und fordert die Kommission auf, dieser Erklärung in Fällen, in denen Anzeichen für einen Missbrauch vorliegen, Folge zu leisten; ist der Ansicht, dass in einer demokratischen transparenten Gesellschaft, die sich an die Rechtsstaatlichkeit hält, solche Einschränkungen im Namen der nationalen Sicherheit eher die Ausnahme als die Regel sein werden;

43. ist der Auffassung, dass der Begriff der nationalen Sicherheit dem engeren Anwendungsbereich des Begriffs der inneren Sicherheit gegenübergestellt werden

---

summary_de.pdf

Urteil vom 6. Oktober 2020, Rechtssache C-623/17, *Privacy International* gegen *Secretary of State for Foreign and Commonwealth Affairs u. a.*, EU:C:2020:790, Rn. 44, und Urteile vom 6. Oktober 2020, verbundene Rechtssachen C-511/18, C-512/18 und C-520/18, *La Quadrature du Net u. a.* gegen *Premier ministre u. a.*, EU:C:2020:791, Rn. 99: „[...] doch kann die bloße Tatsache, dass eine nationale Maßnahme zum Schutz der nationalen Sicherheit getroffen wurde, nicht dazu führen, dass das Unionsrecht unanwendbar ist und die Mitgliedstaaten von der erforderlichen Beachtung dieses Rechts entbunden werden."

muss, wobei letzterer einen breiteren Anwendungsbereich hat, der auch die Verhütung von Gefahren für die Bürgerinnen und Bürger sowie insbesondere die Durchsetzung des Strafrechts umfasst;

44. bedauert, dass sich Schwierigkeiten daraus ergeben, dass eine gemeinsame rechtliche Definition des Begriffs „nationale Sicherheit“ fehlt, in deren Rahmen Kriterien für die Bestimmung der rechtlichen Regelung in Fragen der nationalen Sicherheit festgelegt werden, und dass es an einer klaren Abgrenzung des Bereichs mangelt, in dem eine solche Sonderregelung gelten kann;

45. ist der Auffassung, dass der Einsatz von Spähsoftware eine Einschränkung der Grundrechte darstellt; ist ferner der Auffassung, dass in Fällen, in denen ein Begriff in einem rechtlichen Kontext verwendet wird, der die Übertragung von Rechten und die Auferlegung von Verpflichtungen (und insbesondere Einschränkungen der Grundrechte des Einzelnen) mit sich bringt, dieser Begriff klar und für alle von ihm betroffenen Personen vorhersehbar sein muss; weist erneut darauf hin, dass in der Charta der Grundrechte vorgesehen ist, dass jede Einschränkung der Grundrechte gemäß Artikel 52 Absatz 1 gesetzlich angeordnet werden muss; ist daher der Ansicht, dass der Begriff „nationale Sicherheit“ klar definiert werden muss; betont, dass der Bereich der nationalen Sicherheit unabhängig von der genauen Abgrenzung in seiner Gesamtheit einer unabhängigen, verbindlichen und wirksamen Aufsicht unterliegen muss;

46. betont, dass die Behörden, wenn sie sich zur Rechtfertigung des Einsatzes von Spähsoftware auf Gründe der nationalen Sicherheit berufen, zusätzlich zu dem in Absatz 29 festgelegten Rahmen die Einhaltung des Unionsrechts nachweisen sollten, einschließlich der Einhaltung der Grundsätze der Verhältnismäßigkeit, der Notwendigkeit, der Legitimität, der Rechtmäßigkeit und der Angemessenheit; hebt hervor, dass die Begründung leicht zugänglich sein und einer nationalen Kontrollinstanz zwecks Bewertung zur Verfügung gestellt werden sollte;

47. weist in diesem Zusammenhang erneut darauf hin, dass alle Mitgliedstaaten das Übereinkommen Nr. 108+ unterzeichnet haben, in dem Normen und Verpflichtungen zum Schutz von Personen bei der Verarbeitung personenbezogener Daten, auch für Zwecke der nationalen Sicherheit, festgelegt sind; weist darauf hin, dass das Übereinkommen Nr. 108+ einen verbindlichen europäischen Rahmen für die Verarbeitung von Daten durch Nachrichten- und Sicherheitsdienste darstellt; fordert alle Mitgliedstaaten nachdrücklich auf, dieses Übereinkommen unverzüglich zu ratifizieren, seine Normen bereits in nationales Recht umzusetzen und im Bereich der nationalen Sicherheit entsprechend zu handeln;

48. betont, dass Ausnahmen und Beschränkungen bei einer begrenzten Anzahl von Bestimmungen des Übereinkommens nur dann zulässig sind, wenn sie mit den in Artikel 11 des Übereinkommens genannten Anforderungen im Einklang stehen, was bedeutet, dass bei der Umsetzung des Übereinkommens 108+ jede spezifische Ausnahme und Beschränkung gesetzlich vorgesehen sein muss, den Kern der Grundrechte und -freiheiten respektieren muss und rechtfertigen muss, dass sie „in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme“ aus einem der in Artikel 11 aufgeführten legitimen Gründe darstellt[33], und dass solche

[33] Diese Beurteilung ist in der Rechtsprechung des EGMR vorgesehen, die dem Staat/Gesetzgeber die Beweislast

Ausnahmen und Beschränkungen die „unabhängige und wirksame Überprüfung und Aufsicht nach dem innerstaatlichen Recht der jeweiligen Vertragspartei“ nicht beeinträchtigen dürfen;

49. stellt ferner fest, dass im Übereinkommen Nr. 108+ hervorgehoben wird, dass die Aufsicht „Untersuchungs- und Eingriffsbefugnisse“ haben muss; ist der Ansicht, dass eine wirksame Überprüfung und Aufsicht verbindliche Befugnisse in Bereichen voraussetzt, in denen die Auswirkungen auf die Grundrechte am stärksten sind, insbesondere in den Phasen des Zugriffs auf personenbezogene Daten, ihrer Analyse und Speicherung;

50. ist der Auffassung, dass das Fehlen verbindlicher Befugnisse der Aufsichtsgremien im Bereich der nationalen Sicherheit nicht mit dem im Übereinkommen Nr. 108+ festgelegten Kriterium vereinbar ist, dass dies „in einer demokratischen Gesellschaft eine notwendige [und verhältnismäßige] Maßnahme ist“;

51. weist darauf hin, dass das Übereinkommen Nr. 108+ eine sehr begrenzte Anzahl von Ausnahmen in Bezug auf Artikel 15 des Übereinkommens zulässt, jedoch keine derartigen Ausnahmen, insbesondere im Zusammenhang mit Absatz 2 [Sensibilisierungspflichten], Absatz 3 [Konsultation zu legislativen und administrativen Maßnahmen], Absatz 4 [Anträge und Beschwerden von Einzelpersonen], Absatz 5 [Unabhängigkeit und Unparteilichkeit], Absatz 6 [notwendige Ressourcen für die wirksame Erfüllung der Aufgaben], Absatz 7 [regelmäßige Berichterstattung], Absatz 8 [Vertraulichkeit], Absatz 9 [Möglichkeit der Einlegung von Rechtsmitteln] und Absatz 10 [keine Befugnis in Bezug auf Gremien, die im Rahmen ihrer justiziellen Tätigkeit handeln];

Bessere Umsetzung und Durchsetzung geltender Rechtsvorschriften

52. hebt die Unzulänglichkeiten des nationalen Rechtsrahmens und die Notwendigkeit einer besseren Durchsetzung der geltenden Rechtsvorschriften der Union hervor, um diesen Mängeln entgegenzuwirken; stellt fest, dass die folgenden Rechtsvorschriften der Union zwar relevant sind, aber zu häufig nicht ordnungsgemäß umgesetzt und/oder durchgesetzt werden: die Geldwäscherichtlinie, die Richtlinie zum Datenschutz bei der Strafverfolgung, die Vorschriften für das öffentliche Beschaffungswesen, die Verordnung über Güter mit doppeltem Verwendungszweck, die Rechtsprechung (Urteile zur Überwachung und zur nationalen Sicherheit) sowie die Richtlinie über den Schutz von Hinweisgebern; fordert die Kommission auf, die Mängel bei der Umsetzung und Durchsetzung zu untersuchen und darüber Bericht zu erstatten sowie einen Fahrplan zur Behebung dieser Mängel bis spätestens zum 1. August 2023 vorzulegen;

53. hält die ordnungsgemäße Umsetzung und strikte Durchsetzung des Rechtsrahmens der Union zum Datenschutz, insbesondere der Richtlinie zum Datenschutz bei der Strafverfolgung, der Datenschutz-Grundverordnung und der Datenschutzrichtlinie für elektronische Kommunikation, für ausschlaggebend; hält es für ebenso wichtig, dass die

---

auferlegt. Die einschlägige Rechtsprechung des EGMR umfasst: *Roman Zakharov* gegen *Russland* (Antrag Nr. 47143/06), 4. Dezember 2015; *Szabó und Vissy* gegen *Ungarn* (Antrag Nr. 37138/14), 12. Januar 2016; *Big Brother Watch u. a.* gegen *das Vereinigte Königreich* (Anträge Nr. 58170/13, Nr. 62322/14 und Nr. 24969/15), 25. Mai 2021 und *Centrum För Rättvisa* gegen *Schweden* (Antrag Nr. 35252/08), 25. Mai 2021.

einschlägigen Urteile des EuGH vollständig umgesetzt werden, was in mehreren Mitgliedstaaten noch immer nicht der Fall ist; weist darauf hin, dass der Kommission eine zentrale Rolle bei der Durchsetzung des Unionsrechts und der Sicherstellung seiner einheitlichen Anwendung in der gesamten Union zukommt und dass sie alle verfügbaren Instrumente, einschließlich Vertragsverletzungsverfahren in Fällen anhaltender Nichteinhaltung, nutzen sollte;

54. fordert, dass das Wassenaar-Arrangement zu einer für alle Teilnehmer verbindlichen Vereinbarung mit dem Ziel wird, es zu einem internationalen Vertrag werden zu lassen;

55. fordert Zypern und Israel auf, zu Teilnehmerstaaten des Wassenaar-Arrangements zu werden; erinnert die Mitgliedstaaten daran, dass sämtliche Anstrengungen unternommen werden müssen, damit Zypern und Israel dem Wassenaar-Arrangement beitreten können;

56. betont, dass das Wassenaar-Arrangement einen Menschenrechtsrahmen enthalten sollte, in dem die Lizenzierung von Spähsoftware-Technologien eingeschlossen ist und mit dem die Einhaltung der Vorschriften durch Unternehmen, die Spähsoftware-Technologien herstellen, bewertet und überprüft wird, und dass die Teilnehmer den Erwerb von Überwachungstechnologien von Staaten, die dem Arrangement nicht angehören, verbieten sollten;

57. betont, dass die Kommission und die Mitgliedstaaten angesichts der Enthüllungen über Spähsoftware eine eingehende Untersuchung der Ausfuhrgenehmigungen durchführen sollten, die für die Verwendung von Spähsoftware im Rahmen der Verordnung über Güter mit doppeltem Verwendungszweck erteilt wurden, und dass die Kommission die Ergebnisse dieser Bewertung an das Parlament weitergeben sollte;

58. unterstreicht die Notwendigkeit der Rückverfolgbarkeit und Rechenschaftspflicht bei der Ausfuhr von Spähsoftware und erinnert daran, dass EU-Unternehmen nur dann Spähsoftware exportieren können sollten, wenn sie nachweisen, dass die Rückverfolgbarkeit gegeben ist, um sicherzustellen, dass die Verantwortung stets zugewiesen werden kann;

59. betont, dass die Kommission die Neufassung der Verordnung über Güter mit doppeltem Verwendungszweck regelmäßig überprüfen und ordnungsgemäß durchsetzen muss, um ein „Ausfuhrregelungs-Shopping“ in der gesamten Union zu vermeiden, wie es derzeit in Bulgarien und Zypern der Fall ist, und dass die Kommission über angemessene Ressourcen für diese Aufgabe verfügen sollte;

60. fordert die Kommission auf, für ausreichende Personalkapazitäten für die Referate zu sorgen, die für die Überwachung und Durchsetzung der Verordnung über Güter mit doppeltem Verwendungszweck zuständig sind;

61. fordert eine Änderung der Verordnung über Güter mit doppeltem Verwendungszweck, um in Artikel 15 klarzustellen, dass Ausfuhrgenehmigungen für Güter mit doppeltem Verwendungszweck nicht erteilt werden dürfen, wenn die Güter dazu bestimmt sind oder bestimmt sein können, bei interner Repression und/oder der Begehung schwerer Verstöße gegen die Menschenrechte und das humanitäre Völkerrecht verwendet zu werden; fordert, dass Sorgfaltsprüfungen in Bezug auf die Menschenrechte im Rahmen

des Genehmigungsverfahrens sowie weitere Verbesserungen wie die Bereitstellung von Rechtsmitteln für Opfer von Menschenrechtsverletzungen und eine transparente Berichterstattung über die durchgeführte Sorgfaltsprüfung vollständig umgesetzt werden;

62. fordert Änderungen der Verordnung über Güter mit doppeltem Verwendungszweck, um sicherzustellen, dass die Durchfuhr in Fällen verboten ist, in denen Güter zur internen Repression und/oder zur Begehung schwerer Verstöße gegen die Menschenrechte und das humanitäre Völkerrecht bestimmt sind oder bestimmt sein könnten;

63. betont, dass die benannten nationalen Behörden, die für die Genehmigung oder Verweigerung von Ausfuhrgenehmigungen für Güter mit doppeltem Verwendungszweck zuständig sind, im Rahmen einer künftigen Änderung der Verordnung über Güter mit doppeltem Verwendungszweck ausführliche Berichte vorlegen sollten, die auch Informationen über Folgendes enthalten: über das betreffende Gut mit doppeltem Verwendungszweck, die Anzahl der beantragten Lizenzen, den Namen des Ausfuhrlandes, eine Beschreibung des Ausfuhrunternehmens und eine Angabe, ob es sich bei diesem Unternehmen um eine Tochtergesellschaft handelt, eine Beschreibung des Endnutzers und des Bestimmungsortes, den Wert der Ausfuhrgenehmigung und die Gründe für die Genehmigung oder Verweigerung der Ausfuhrgenehmigung; hebt hervor, dass diese Berichte vierteljährlich veröffentlicht werden sollten; fordert, dass eigens dafür ein ständiger parlamentarischer Ausschusses mit Zugang zu Verschlusssachen der Kommission eingerichtet wird, um die parlamentarische Kontrolle sicherzustellen;

64. betont, dass bei einer künftigen Änderung der Verordnung über Güter mit doppeltem Verwendungszweck die Ausnahme von der Verpflichtung zur Übermittlung von Informationen an die Kommission aus Gründen sensibler Geschäftsinformationen, der Verteidigungs- und Außenpolitik oder der nationalen Sicherheit abgeschafft werden muss; ist stattdessen der Auffassung, dass die Kommission beschließen kann, bestimmte Informationen in ihrem Jahresbericht als vertraulich einzustufen, damit sensible Informationen für Nicht-EU-Staaten nicht zugänglich sind;

65. betont, dass die Definition von Gütern für digitale Überwachung in der Neufassung der Verordnung über Güter mit doppeltem Verwendungszweck nicht einschränkend ausgelegt werden darf, sondern alle Technologien in diesem Bereich einschließen sollte, wie z. B. Geräte zum Abhören oder Stören der mobilen Telekommunikation, Intrusion-Software, Systeme oder Ausrüstung zur Überwachung der Kommunikation in IP-Netzen, Software, die speziell dafür konzipiert oder geändert wurde, damit sie durch die Strafverfolgung überwacht oder analysiert werden kann, Laser-akustische Detektionsausrüstung, forensische Werkzeuge, mit denen Rohdaten aus einem Rechen- oder Kommunikationsgerät extrahiert und die Kontrollen der „Authentisierung“ oder Autorisierung des Geräts umgangen werden können, elektronische Systeme oder Ausrüstung, die entweder für die Überwachung und Beobachtung des elektromagnetischen Spektrums für das militärische Nachrichtenwesen oder zu Sicherheitszwecken konzipiert wurden bzw. wurde, und unbemannte Luftfahrzeuge, mit denen eine Überwachung durchgeführt werden kann;

66. fordert weitere europäische Rechtsvorschriften, mit denen von Unternehmen, die

Überwachungstechnologien herstellen und/oder ausführen, verlangt wird, dass sie im Einklang mit den Leitprinzipien der Vereinten Nationen für Wirtschaft und Menschenrechte Rahmen für Menschenrechte und Sorgfaltspflicht einrichten;

Internationale Zusammenarbeit zum Schutz der Bürgerinnen und Bürger

67. fordert eine gemeinsame Spähsoftware-Strategie der EU und der USA, die eine gemeinsame weiße und/oder schwarze Liste von Spähsoftware-Anbietern umfasst, deren Werkzeuge von ausländischen Regierungen mit schlechter Menschenrechtsbilanz missbraucht wurden oder missbraucht zu werden drohen, um Regierungsbeamte, Journalisten und die Zivilgesellschaft böswillig ins Visier zu nehmen, die gegen die Sicherheits- und Außenpolitik der Union agieren und die (nicht) an Behörden verkaufen dürfen, sowie gemeinsame Kriterien für die Aufnahme von Anbietern in eine der beiden Listen, Regelungen für eine gemeinsame Berichterstattung der EU und der USA über die Branche, gemeinsame Kontrollen, gemeinsame Sorgfaltspflichten für Anbieter und die Kriminalisierung des Verkaufs von Spähsoftware an nichtstaatliche Akteure;

68. fordert den EU-US-Handels- und Technologierat auf, umfassende und offene Konsultationen mit der Zivilgesellschaft für die Entwicklung der gemeinsamen Strategie und der Standards der EU und der USA durchzuführen, zu denen auch die gemeinsame weiße und/oder schwarze Liste gehört bzw. gehören;

69. fordert die Aufnahme von Gesprächen mit anderen Ländern, insbesondere mit Israel, um einen Rahmen für die Vermarktung von Spähsoftware und Ausfuhrgenehmigungen zu schaffen, in dem Regeln für die Transparenz, eine Liste der in Bezug auf die Menschenrechtsstandards infrage kommenden Länder und Regelungen für die Sorgfaltspflicht enthalten sind;

70. stellt fest, dass im Vergleich zu den USA, wo die NSO-Group rasch in die schwarze Liste aufgenommen wurde und der US-Präsident eine Executive Order unterzeichnete, in der es heißt, dass keine kommerzielle Spähsoftware eingesetzt werden darf, die für die Regierung der Vereinigten Staaten erhebliche Risiken im Bereich der Spionageabwehr oder Sicherheit oder erhebliche Risiken einer missbräuchlichen Nutzung durch eine ausländische Regierung oder eine ausländische Person birgt, auf EU-Ebene keine ausreichenden Maßnahmen in Bezug auf die Einfuhr von Spähsoftware und die Durchsetzung der Ausfuhrbestimmungen ergriffen wurden;

71. kommt zu dem Schluss, dass die Ausfuhrbestimmungen der Union und ihre Durchsetzung zum Schutz der Menschenrechte in Nicht-EU-Staaten gestärkt und mit den erforderlichen Werkzeugen zur wirksamen Umsetzung ihrer Bestimmungen versehen werden müssen; weist darauf hin, dass die EU versuchen sollte, sich mit den USA und anderen Verbündeten zusammenzutun, um den Handel mit Spähsoftware zu regulieren und ihre gemeinsame Marktmacht zu nutzen, um Veränderungen zu erzwingen, und solide Standards für Transparenz, Rückverfolgbarkeit und Rechenschaftspflicht mit Blick auf den Einsatz von Überwachungstechnologien festzulegen, was in einer Initiative auf Ebene der Vereinten Nationen gipfeln sollte;

Zero-Day-Sicherheitslücken

72. fordert eine Regelung für die Aufdeckung, Weitergabe, Behebung und Ausnutzung von

Sicherheitslücken sowie Offenlegungsverfahren, damit die Grundlage der Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie)[34] und der Vorschlag für ein Cyberresilienzgesetz[35] ergänzt werden;

73. ist der Ansicht, dass Wissenschaftler in der Lage sein müssen, Schwachstellen zu erforschen und ihre Ergebnisse weiterzugeben, ohne zivil- und strafrechtlich haftbar gemacht zu werden, was unter anderem im Einklang mit der Richtlinie zur Bekämpfung der Cyberkriminalität und der Urheberrechtsrichtlinie steht;

74. fordert die Hauptakteure der Branche auf, Anreize für Wissenschaftler zu schaffen, sich an der Schwachstellenforschung zu beteiligen, indem sie in Pläne zur Behandlung von Schwachstellen und in die Offenlegungspraxis innerhalb der Branche und mit der Zivilgesellschaft investieren und Bug-Bounty-Programme durchführen;

75. fordert die Kommission auf, ihre Unterstützung und Finanzierung für Bug-Bounty-Projekte und andere Projekte, die darauf abzielen, nach Sicherheitslücken zu suchen und diese zu beheben, zu verstärken und einen koordinierten Ansatz für die obligatorische Offenlegung von Sicherheitslücken unter den Mitgliedstaaten festzulegen;

76. fordert ein Verbot des Verkaufs von Schwachstellen in einem System zu anderen Zwecken als der Stärkung der Sicherheit dieses Systems und eine Verpflichtung, die Ergebnisse aller Schwachstellenforschung in koordinierter und verantwortungsvoller Weise offenzulegen, sodass die öffentliche Sicherheit gefördert und das Risiko einer Ausnutzung der Schwachstelle auf ein Mindestmaß beschränkt wird;

77. fordert öffentliche und private Einrichtungen auf, eine öffentlich zugängliche Kontaktstelle einzurichten, bei der Schwachstellen auf koordinierte und verantwortungsvolle Weise gemeldet werden können, und fordert von den Organisationen, die Informationen über Schwachstellen in ihrem System erhalten, unverzüglich für Abhilfe zu sorgen; ist der Auffassung, dass Organisationen – wenn Patches verfügbar sind – verpflichtet werden sollten, geeignete Maßnahmen zu ergreifen, um eine rasche und garantierte Bereitstellung sicherzustellen, was Teil eines koordinierten und verantwortungsvollen Offenlegungsprozesses wäre;

78. ist der Ansicht, dass die Mitgliedstaaten ausreichende finanzielle, technische und personelle Ressourcen für die Sicherheitsforschung und die Behebung von Schwachstellen bereitstellen sollten;

79. fordert die Mitgliedstaaten auf, gesetzlich vorgeschriebene Verfahren für die Gleichbehandlung von Schwachstellen auszuarbeiten, in denen festgelegt wird, dass Schwachstellen standardmäßig offengelegt werden müssen und nicht ausgebeutet werden dürfen und dass jede Entscheidung, davon abzuweichen, eine Ausnahme sein und anhand der Erfordernisse der Notwendigkeit und der Verhältnismäßigkeit bewertet

[34] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (ABl. L 333 vom 27.12.2022, S. 80).

[35] Vorschlag vom 15. September 2022 für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen an Produkte mit digitalen Bestandteilen und zur Änderung der Richtlinie (EU) 2019/1020 (COM(2022) 0454).

werden muss, wobei auch zu berücksichtigen ist, ob die von der Schwachstelle betroffene Infrastruktur von einem großen Teil der Bevölkerung genutzt wird und einer strengen Aufsicht durch ein unabhängiges Kontrollgremium sowie transparenten Verfahren und Entscheidungen unterliegt;

Telekommunikationsnetze

80. betont, dass jedem Diensteanbieter die Lizenz entzogen werden sollte, bei dem festgestellt wurde, dass er den unbefugten Zugang zur nationalen und/oder internationalen Mobilfunksignalisierungsinfrastruktur aller Generationen (derzeit 2G bis 5G) erleichtert;

81. betont, dass die Verfahren, mit denen neue Telefonnummern aus der ganzen Welt von böswilligen Akteuren erstellt werden können, besser reguliert werden sollten, um illegale Tätigkeiten zu erschweren;

82. betont, dass Telekommunikationsanbieter sicherstellen müssen, dass sie in der Lage sind, einen potenziellen Missbrauch des Zugangs, der Kontrolle oder der wirksamen Endnutzung der Signalisierungsinfrastruktur zu erkennen, den Dritte durch kommerzielle oder sonstige Vereinbarungen in dem Mitgliedstaat, in dem sie tätig sind, erzielen;

83. fordert die Mitgliedstaaten auf, dafür zu sorgen, dass die zuständigen nationalen Behörden im Einklang mit den Bestimmungen der NIS-2-Richtlinie das Ausmaß der Resilienz der Telekommunikationsanbieter gegenüber unbefugten Eingriffen bewerten;

84. fordert die Telekommunikationsanbieter auf, entschlossen und nachweislich gegen die verschiedenen Formen der unbefugten Nachahmung des von einem Netzelement ausgehenden Telekommunikationsverkehrs vorzugehen, die darauf abzielt, auf die für rechtmäßige Nutzer bestimmten Daten oder Dienste zuzugreifen, sowie andere Aktivitäten zu unterbinden, die die Manipulation des normalen Betriebs von Mobilfunknetzelementen und -infrastrukturen zu Überwachungszwecken durch böswillige Akteure, einschließlich staatlicher Akteure und krimineller Gruppen, umfassen;

85. fordert die Mitgliedstaaten auf, Maßnahmen zu ergreifen, um sicherzustellen, dass staatliche Akteure außerhalb der EU, die die Grundrechte nicht achten, keine Kontrolle oder wirksame Endnutzung über die strategische Infrastruktur oder Einfluss auf Entscheidungen im Zusammenhang mit der strategischen Infrastruktur innerhalb der Union, einschließlich der Telekommunikationsinfrastruktur, haben;

86. fordert alle Mitgliedstaaten auf, vorrangig mehr in den Schutz kritischer Infrastrukturen, wie z. B. nationaler Telekommunikationssysteme, zu investieren und Lücken beim Schutz vor Verletzungen der Privatsphäre, Datenlecks und unbefugtem Eindringen zu schließen, damit die Grundrechte der Bürgerinnen und Bürger geschützt werden;

87. fordert die zuständigen nationalen Behörden auf, die Stärkung der Kapazitäten der Anbieter sowie die Reaktionsfähigkeiten aktiv zu fördern, um die Identifizierung von Personen, die illegal ins Visier genommen wurden, sowie die Benachrichtigung und die Meldung von Vorfällen besser zu unterstützen, damit eine kontinuierliche und messbare

Zuverlässigkeit gewährleistet und die Ausnutzung von Sicherheitslücken durch böswillige Akteure außerhalb und innerhalb der EU eingedämmt wird;

Digitaler Datenschutz

88. fordert die rasche Verabschiedung der Verordnung über Privatsphäre und elektronische Kommunikation, und zwar in einer Art und Weise, bei der die Rechtsprechung zu den Einschränkungen für die nationale Sicherheit und der Notwendigkeit, den Missbrauch von Überwachungstechnologien zu verhindern, in vollem Umfang berücksichtigt und das Grundrecht auf Privatsphäre gestärkt wird und solide Garantien und eine wirksame Durchsetzung vorgesehen sind; weist darauf hin, dass der Anwendungsbereich für rechtmäßige Abhörmaßnahmen nicht über die Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) hinausgehen sollte;

89 fordert den Schutz der gesamten elektronischen Kommunikation, ihrer Inhalte und Metadaten vor dem Missbrauch persönlicher Daten und privater Kommunikation durch private Unternehmen und staatliche Stellen; weist darauf hin, dass Instrumente der digitalen Sicherheit durch Technik wie die Ende-zu-Ende-Verschlüsselung nicht geschwächt werden sollten;

90. fordert die Kommission auf, die Umsetzung der Datenschutzrichtlinie für elektronische Kommunikation durch die Mitgliedstaaten in der gesamten EU zu bewerten und bei Verstößen Vertragsverletzungsverfahren einzuleiten;

Die Rolle von Europol

91. nimmt zur Kenntnis, dass der PEGA-Ausschuss durch ein Schreiben von Europol an den Vorsitzenden dieses Ausschusses vom April 2023 darüber unterrichtet wird, dass Europol mit Griechenland, Ungarn, Bulgarien, Spanien und Polen Kontakt aufgenommen hat, um festzustellen, ob strafrechtliche Ermittlungen oder andere Untersuchungen nach den geltenden Bestimmungen des nationalen Rechts laufen oder geplant sind, die von Europol unterstützt werden könnten; betont, dass das Anbieten von Unterstützung an die Mitgliedstaaten nicht die Einleitung, Durchführung oder Koordinierung einer strafrechtlichen Ermittlung im Sinne von Artikel 6 darstellt;

92. fordert Europol auf, ihre neu erworbenen Befugnisse gemäß Artikel 6 Absatz 1a der Verordnung (EU) 2022/991, mit der es ihr ermöglicht wird, den zuständigen Behörden der betroffenen Mitgliedstaaten gegebenenfalls die Einleitung, Durchführung oder Koordinierung von Ermittlungen vorzuschlagen, in vollem Umfang zu nutzen; weist darauf hin, dass es gemäß Artikel 6 Sache der Mitgliedstaaten ist, einen solchen Vorschlag abzulehnen;

93. fordert alle Mitgliedstaaten auf, sich gegenüber dem Europäischen Parlament und dem Rat zu verpflichten, Europol in die Ermittlungen über einen mutmaßlich unrechtmäßigen Einsatz von Spähsoftware auf nationaler Ebene einzubeziehen, insbesondere wenn ein Vorschlag im Sinne von Artikel 6 Absatz 1a der Verordnung (EU) 2022/991 vorgelegt wurde;

94. fordert die Mitgliedstaaten auf, innerhalb von Europol ein Register der nationalen Strafverfolgungsmaßnahmen zu erstellen, bei denen Spähsoftware eingesetzt wird,

wobei jede Maßnahme mit einem Code gekennzeichnet werden sollte, und die Verwendung von Spähsoftware durch Regierungen in den jährlichen Bericht von Europol zur Bewertung der Bedrohungslage im Bereich der organisierten Kriminalität im Internet aufzunehmen;

95. ist der Ansicht, dass Überlegungen über die Rolle von Europol angestellt werden müssen, wenn die nationalen Behörden die Ermittlungen nicht durchführen können oder diese ablehnen und eindeutige Bedrohungen für die Interessen und die Sicherheit der EU bestehen;

Entwicklungspolitik der EU

96. fordert die Kommission und den EAD auf, strengere Kontrollmechanismen einzuführen, um sicherzustellen, dass mit der Entwicklungshilfe der EU, einschließlich der Spende von Überwachungstechnologie und der Schulung für den Einsatz von Spähsoftware, keine Instrumente oder Tätigkeiten finanziert oder unterstützt werden, die gegen die Grundsätze der Demokratie, der guten Regierungsführung, der Rechtsstaatlichkeit und der Achtung der Menschenrechte verstoßen oder eine Gefahr für die internationale Sicherheit oder die grundlegende Sicherheit der EU und ihrer Mitgliedstaaten darstellen könnten; stellt fest, dass die von der Kommission vorgenommenen Bewertungen der Einhaltung des Unionsrechts, insbesondere der Haushaltsordnung, spezifische Kontrollkriterien und Durchsetzungsmechanismen enthalten sollten, um solche Missbräuche zu verhindern, einschließlich der möglichen vorübergehenden Aussetzung bestimmter Projekte, wenn ein Verstoß gegen diese Grundsätze festgestellt wird;

97. fordert die Kommission und den EAD auf, innerhalb eines Jahres [nach Veröffentlichung der PEGA-Empfehlungen] in jede Bewertung der Auswirkungen auf die Menschen- und Grundrechte einen Kontrollmechanismus in Bezug auf den potenziellen Missbrauch einer Observierung einzufügen, mit dem Artikel 51 der Charta der Grundrechte in vollem Umfang Rechnung getragen wird; betont, dass dieses Verfahren dem Parlament und dem Rat vorgelegt werden muss und dass diese Folgenabschätzung durchgeführt werden muss, bevor Drittstaaten unterstützt werden;

98. fordert den EAD auf, den missbräuchlichen Einsatz von Spähsoftware gegen Menschenrechtsverteidiger im EU-Jahresbericht über Menschenrechte und Demokratie zu erfassen;

Finanzordnung der EU

99. betont, dass die Achtung der Menschenrechte durch die Finanzbranche verbessert werden muss; betont, dass die 10+-Empfehlungen im Rahmen der Leitprinzipien der Vereinten Nationen für Wirtschaft und Menschenrechte in das Unionsrecht umgesetzt werden müssen und dass die Sorgfaltspflichtrichtlinie uneingeschränkt für die Finanzbranche gelten sollte, um die Achtung der Demokratie, der Menschenrechte und der Rechtsstaatlichkeit in der Finanzbranche sicherzustellen;

100. ist besorgt über die Auswirkungen der Entscheidung des EuGH auf die Richtlinie (EU) 2018/843 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der

Geldwäsche oder der Terrorismusfinanzierung[36], wonach die Informationen über das wirtschaftliche Eigentum von juristischen und natürlichen Personen, die in einem nationalen und öffentlich zugänglichen Register für wirtschaftliches Eigentum (UBO) eingetragen sind, für ungültig erklärt wurden[37]; betont, dass die künftige Richtlinie unter Berücksichtigung der Entscheidung des EuGH einen größtmöglichen Zugang der Öffentlichkeit ermöglichen sollte, sodass es schwieriger wird, den Kauf oder Verkauf von Spähsoftware durch Stellvertreter und Maklerfirmen zu verbergen;

Folgemaßnahmen nach Entschließungen des Parlaments

101. fordert die nachdrückliche Weiterverfolgung seiner Entschließung vom 12. März 2014 zu dem Überwachungsprogramm der Nationalen Sicherheitsagentur der Vereinigten Staaten, den Überwachungsbehörden in mehreren Mitgliedstaaten und den entsprechenden Auswirkungen auf die Grundrechte der der EU-Bürger und zu der transatlantischen Zusammenarbeit im Bereich Justiz und Inneres; betont, dass die darin enthaltenen Empfehlungen dringend umgesetzt werden müssen;

102. betont, dass trotz der Tatsache, dass die Aufsicht über die Tätigkeiten der Nachrichtendienste sowohl auf demokratischer Legitimität (starker Rechtsrahmen, Vorabgenehmigung und nachträgliche Überprüfung) als auch auf angemessenen technischen Fähigkeiten und Fachkenntnissen beruhen sollte, es der Mehrheit der derzeitigen Aufsichtsgremien in der EU und den USA dramatisch an beidem mangelt, insbesondere an den technischen Fähigkeiten;

103. fordert wie im Falle von Echelon alle nationalen Parlamente, die dies noch nicht getan haben, auf, eine effektive Aufsicht über die Nachrichtendienstaktivitäten durch Parlamentarier oder Sachverständigengremien mit Untersuchungsvollmachten einzurichten; ruft die nationalen Parlamente auf, sicherzustellen, dass diese Aufsichtsausschüsse/-gremien über ausreichende Ressourcen, technische Kenntnisse und Rechtsmittel, einschließlich des Rechts, Besichtigungen vor Ort durchzuführen, für eine effektive Kontrolle der Nachrichtendienste verfügen;

104. fordert die Bildung einer hochrangigen Gruppe, die in transparenter Weise und in Zusammenarbeit mit den Parlamenten Empfehlungen und weitere Schritte für eine stärkere demokratische Aufsicht, einschließlich der parlamentarischen Aufsicht, über die Nachrichtendienste auf EU-Ebene und eine stärkere Zusammenarbeit in der EU im Bereich der Aufsicht, insbesondere hinsichtlich der grenzüberschreitenden Dimension, vorschlagen soll;

105. Diese hochrangige Gruppe sollte:

(a) europäische Mindestnormen oder Leitlinien zur (vorab und nachträglich durchgeführten) Kontrolle der Nachrichtendienste auf der Grundlage bestehender bewährter Methoden und Empfehlungen internationaler Gremien, wie den VN und dem Europarat, definieren, einschließlich des Problems, dass Aufsichtsgremien nicht als dritte Partei im Sinne der „Drittparteiregel“ oder des Grundsatzes der „Kontrolle durch

[36] Urteil vom 22. November 2022, verbundene Rechtssachen C-37/20 und C-601/20, EU:C:2022:912
[37] EuGH Pressemitteilung Nr. 188/22, Urteil des Gerichtshofs in den verbundenen Rechtssachen C-37/20 und C-601/20.

den Urheber“ gelten, sowie zur Aufsicht und Rechenschaftspflicht ausländischer Nachrichtendienste;

(b) Kriterien für mehr Transparenz auf der Grundlage des allgemeinen Grundsatzes des Zugangs zu Informationen und der sogenannten „Tshwane-Prinzipien“ erarbeiten[38];

106. beabsichtigt, eine Konferenz mit nationalen – parlamentarischen und unabhängigen – Aufsichtsgremien zu organisieren;

107. fordert die Mitgliedstaaten auf, auf bewährte Methoden zurückzugreifen, um den Zugang ihrer Aufsichtsgremien zu Informationen bezüglich Nachrichtendienstaktivitäten, einschließlich Verschlusssachen und Informationen von anderen Diensten, zu verbessern und für die Befugnis zu Besichtigungen vor Ort, umfassende Befragungsbefugnisse, angemessene Ressourcen und technische Kenntnisse, völlige Unabhängigkeit von den jeweiligen Regierungen sowie eine Meldepflicht gegenüber den jeweiligen Parlamenten zu sorgen;

108. fordert die Mitgliedstaaten auf, die Zusammenarbeit der Aufsichtsgremien untereinander auszubauen;

109. fordert die Kommission auf, einen Vorschlag für ein Verfahren der Sicherheitsüberprüfung der EU für alle Amtsträger der EU vorzulegen, da das aktuelle System, das auf der vom Mitgliedstaat der Staatsangehörigkeit durchgeführten Sicherheitsüberprüfung beruht, unterschiedliche Anforderungen und Verfahrensdauern innerhalb nationaler Systeme ermöglicht und somit zu einer unterschiedlichen Behandlung von Parlamentsmitgliedern und ihren Mitarbeitern je nach Staatsangehörigkeit führt;

110. erinnert an die Bestimmungen der Interinstitutionellen Vereinbarung zwischen dem Parlament und dem Rat über die Übermittlung an und die Bearbeitung durch das Europäische Parlament von im Besitz des Rates befindlichen Verschlusssachen in Bezug auf Angelegenheiten, die nicht unter die Gemeinsame Außen- und Sicherheitspolitik fallen, welche zur Verbesserung der Aufsicht auf EU-Ebene verwendet werden sollten;

EU-Forschungsprogramme

111. fordert die Einführung strengerer und wirksamerer Kontrollmechanismen, um sicherzustellen, dass die Forschungsmittel der EU keine Instrumente, einschließlich Spähsoftware und Überwachungsinstrumente, finanzieren oder unterstützen, die gegen die Werte der EU verstoßen; stellt fest, dass die Bewertung der Einhaltung des Unionsrechts spezifische Kontrollkriterien enthalten sollte, um solche Missbräuche zu verhindern; fordert die Streichung von Forschungsmitteln der EU für Einrichtungen, die direkt oder indirekt an der Erleichterung von Menschenrechtsverletzungen durch Überwachungsinstrumente beteiligt sind oder waren;

112. betont, dass EU-Forschungsgelder, wie z. B. die „Horizont Europa“-Abkommen mit Drittländern, nicht dazu verwendet werden dürfen, zur Entwicklung von Spähsoftware

[38] Die weltweiten Prinzipien zur nationalen Sicherheit und dem Recht auf Informationen, Juni 2013.

und vergleichbaren Technologien beizutragen;

EU-Technologielabor

113. fordert die Kommission auf, unverzüglich ein unabhängig geführtes europäisches interdisziplinäres Forschungsinstitut zu gründen, das sich auf Forschung und Entwicklung an der Schnittstelle von Informations- und Kommunikationstechnologie, Grundrechten und Sicherheit konzentriert; betont, dass dieses Institut als unabhängige Struktur mit Experten, Akademikern und Vertretern der Zivilgesellschaft zusammenarbeiten und für die Teilnahme von Experten und Institutionen der Mitgliedstaaten offen sein sollte;

114. betont, dass dieses Institut zu einer besseren Sensibilisierung, Zuordnung und Verantwortlichkeit in und außerhalb von Europa beitragen sowie die europäische Talentschmiede erweitern und unser Verständnis dafür verbessern würde, wie Spähsoftware-Anbieter ihre Dienste entwickeln, pflegen, verkaufen und an Dritte liefern.

115. ist der Ansicht, dass das Institut beauftragt werden sollte, die unrechtmäßige Nutzung von Software für Zwecke der illegalen Überwachung aufzudecken und offenzulegen, zugängliche und kostenlose rechtliche und technische Unterstützung bereitzustellen, einschließlich der Überprüfung von Smartphones der Personen, die den Verdacht haben, dass sie Gegenstand von Spähsoftware sind, sowie die zum Aufspüren von Spähsoftware erforderlichen Instrumente zur Verfügung zu stellen, forensische analytische Untersuchungen für gerichtliche Ermittlungen durchzuführen und regelmäßig über den Einsatz und Missbrauch von Spähsoftware in der EU unter Berücksichtigung technologischer Aktualisierungen Bericht zu erstatten; ist der Ansicht, dass dieser Bericht jährlich vorgelegt und der Kommission, dem Parlament und dem Rat übermittelt werden sollte;

116. empfiehlt, dass die Kommission das ein EU-Technologielabor in enger Zusammenarbeit mit dem IT-Notfallteam für die Organe, Einrichtungen und sonstigen Stellen der EU (CERT EU) und der ENISA einrichtet und bei der Einrichtung dieses Labors einschlägige Experten konsultiert, um von bewährten Verfahren der Wissenschaft zu lernen;

117. betont, dass es wichtig ist, eine angemessene Finanzierung des EU-Technologielabors sicherzustellen;

118. empfiehlt, dass die Kommission ein Zertifizierungssystem für die Analyse und Authentifizierung von forensischem Material vorschlägt;

119. fordert die Kommission auf, die weltweiten Kapazitäten der Zivilgesellschaft zu unterstützen, um die Widerstandsfähigkeit gegenüber Spähsoftware-Angriffen und die Bereitstellung von Unterstützung und Dienstleistungen für die Bürger zu stärken;

Rechtsstaatlichkeit

120. betont, dass die Auswirkungen der unrechtmäßigen Verwendung von Spähsoftware in den Mitgliedstaaten viel ausgeprägter sind, in denen die Behörden, die normalerweise

mit den Untersuchungen, der Wiedergutmachung für die Betroffenen und der Gewährleistung der Rechenschaftspflicht betraut sind, vom Staat vereinnahmt werden, und dass man sich auf die nationalen Behörden nicht verlassen kann, wenn eine Krise der Rechtsstaatlichkeit besteht und die Unabhängigkeit der Justiz gefährdet ist;

121. fordert die Kommission daher auf, für eine wirksame Umsetzung ihres Instrumentariums zur Förderung der Rechtsstaatlichkeit zu sorgen, insbesondere durch:

(a) die Einführung einer umfassenderen Überwachung der Rechtsstaatlichkeit, einschließlich länderspezifischer Empfehlungen in Bezug auf den unrechtmäßigen Einsatz von Spähsoftware im jährlichen Bericht der Kommission über die Rechtsstaatlichkeit, die Bewertung der Reaktionsfähigkeit staatlicher Institutionen bei der Bereitstellung von Rechtsbehelfen für die Betroffenen, die Ausweitung des Geltungsbereichs ihres Jahresberichts über die Rechtsstaatlichkeit und die Einbeziehung aller Herausforderungen für die Demokratie, die Rechtsstaatlichkeit und die Grundrechte gemäß Artikel 2 EUV, wie vom Parlament wiederholt gefordert;

(b) die proaktive Einführung und Bündelung von Vertragsverletzungsverfahren gegen Mitgliedstaaten wegen rechtsstaatlicher Defizite, wie z. B. der Gefährdung der Unabhängigkeit der Justiz und der wirksamen Arbeitsweise von Polizei und Staatsanwaltschaft im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen;

EU-Fonds für Rechtsstreitigkeiten

122. fordert die unverzügliche Einrichtung eines EU-Fonds für Rechtsstreitigkeiten, um die tatsächlichen Prozesskosten zu decken und es den von Spähsoftware Betroffenen zu ermöglichen, gemäß der vom Parlament 2017 angenommenen vorbereitenden Maßnahme zur Einrichtung eines „finanziellen Beistandsfonds der EU für Prozessfälle im Zusammenhang mit Verletzungen der Demokratie, der Rechtsstaatlichkeit und der Grundrechte“ eine angemessene Entschädigung, einschließlich Schadensersatz für den illegalen Einsatz von Spähsoftware gegen sie, zu erhalten;

EU-Institutionen

123. äußert seine Besorgnis über die bisherige Untätigkeit der Kommission und fordert sie nachdrücklich auf, alle ihre Befugnisse als Hüterin der Verträge voll auszuschöpfen und eine umfassende und eingehende Untersuchung des Missbrauchs von und des Handels mit Spähsoftware in der EU durchzuführen;

124. fordert die Kommission nachdrücklich auf, eine umfassende Untersuchung aller Behauptungen und Verdachtsmomente in Bezug auf den Einsatz von Spähsoftware gegen ihre Beamten durchzuführen und dem Parlament sowie gegebenenfalls den zuständigen Strafverfolgungsbehörden Bericht zu erstatten;

125. fordert die Kommission auf, eine spezielle Arbeitsgruppe unter Einbeziehung der nationalen Wahlkommissionen für den Schutz der Europawahlen 2024 in der gesamten EU einzurichten; weist darauf hin, dass nicht nur ausländische, sondern auch interne Einmischung eine Bedrohung für die europäischen Wahlprozesse darstellt; betont, dass im Falle des Missbrauchs von Instrumenten zur totalen Überwachung wie Pegasus die

Wahlen beeinträchtigt werden können;

126. stellt fest, dass der Untersuchungsausschuss zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware (PEGA-Ausschuss) eine kollektive Antwort des Rates auf die Anfragen des Europäischen Parlaments an alle einzelnen Mitgliedstaaten erst am Vorabend der Veröffentlichung des Berichtsentwurfs, also etwa vier Monate nach den Schreiben des Parlaments, erhalten hat; erklärt sich bestürzt über die Untätigkeit des Europäischen Rates und des Ministerrates und fordert angesichts des Ausmaßes der Bedrohung der Demokratie in Europa einen eigenen Gipfel des Europäischen Rates;

127. fordert den Rat der Europäischen Union auf, die Entwicklungen im Zusammenhang mit dem Einsatz von Spähsoftware und deren Auswirkungen auf die in Artikel 2 EUV verankerten Werte bei den gemäß Artikel 7 Absatz 1 EUV organisierten Anhörungen zu erörtern;

128. vertritt den Standpunkt, dass das Parlament über umfassende Untersuchungsbefugnisse verfügen sollte, einschließlich eines besseren Zugangs zu als Verschlusssache eingestuften und nicht als Verschlusssache eingestuften Informationen sowie der Befugnis, Zeugen vorzuladen, Zeugen förmlich aufzufordern, unter Eid auszusagen, und die angeforderten Informationen innerhalb bestimmter Fristen bereitzustellen; verweist erneut auf den Standpunkt des Parlaments in seine Vorschlag vom 23. Mai 2012 für eine Verordnung des Europäischen Parlaments über Einzelheiten der Ausübung des Untersuchungsrechts des Europäischen Parlaments und zur Aufhebung des Beschlusses 95/167/EG, EURATOM, EGKS des Europäischen Parlaments, des Rates und der Kommission[39], fordert den Rat auf, unverzüglich auf diesen Vorschlag für eine Verordnung hin tätig zu werden, damit dem Europäischen Parlament ein angemessenes Untersuchungsrecht eingeräumt wird;

129. nimmt die Bemühungen des Parlaments zur Erkennung von Infektionen mit Spähsoftware zur Kenntnis; ist jedoch der Ansicht, dass der Schutz der Mitarbeiter im Hinblick auf die Vorrechte und die Immunität der ausgespähten Personen gestärkt werden sollte; weist darauf hin, dass jeder Angriff auf die politischen Rechte der Mitglieder ein Angriff auf die Unabhängigkeit und Souveränität des Organs sowie ein Angriff auf die Rechte der Wähler ist;

130. fordert das Präsidium des Parlaments auf, ein Protokoll für Fälle anzunehmen, in denen Mitglieder oder Mitarbeiter des Parlaments direkt oder indirekt Ziel von Spähsoftware geworden sind, und betont, dass alle Fälle vom Parlament den zuständigen Strafverfolgungsbehörden gemeldet werden müssen; betont, dass das Parlament in solchen Fällen rechtliche und technische Unterstützung leisten sollte;

131. beschließt, die Initiative zu ergreifen, um eine interinstitutionelle Konferenz einzuberufen, in der das Parlament, der Rat und die Kommission Reformen des Regierens anstreben müssen, mit denen die institutionellen Fähigkeit der EU gestärkt werden, angemessen auf Angriffe von innen auf Demokratie und Rechtsstaatlichkeit zu reagieren und sicherzustellen, dass die EU über wirksame supranationale Methoden zur Durchsetzung der Verträge und des abgeleiteten Rechts im Fall der Nichteinhaltung

[39] ABl. C 264 E vom 13.9.2013, S. 41.

durch die Mitgliedstaaten verfügt;

132. fordert die Annahme des Vorschlags der Kommission für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Maßnahmen für ein hohes gemeinsames Niveau der Cybersicherheit in den Organen, Einrichtungen, Ämtern und Agenturen der Union (COM(2022/0122) und deren anschließenden raschen Umsetzung und strikten Durchsetzung, um das Risiko einer Infektion von Geräten und Systemen, die von Bediensteten und Politikern der EU-Organe und -Einrichtungen genutzt werden, mit Spähsoftware zu verringern;

133. fordert die EU auf, dem Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten beizutreten;

134. fordert den Europäischen Bürgerbeauftragten auf, innerhalb des Europäischen Netzes der Bürgerbeauftragten Diskussionen über die Auswirkungen des Missbrauchs der allgegenwärtigen Überwachung auf demokratische Prozesse und Bürgerrechte zu initiieren; fordert das Netz auf, Empfehlungen für wirksame und sinnvolle Rechtsbehelfe in der gesamten EU zu erarbeiten;

Legislative Maßnahmen

135. fordert die Kommission auf, auf der Grundlage dieser Empfehlung rasch Legislativvorschläge vorzulegen;

°

° °

136. beauftragt seine Präsidentin, diese Entschließung den Mitgliedstaaten, dem Rat, der Kommission und Europol zu übermitteln.