Europäisches Parlament
2019–2024

Untersuchungsausschuss zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware

B9-0000/2023

4.1.2023

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

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

B9-0000/2023

Entwurf einer Empfehlung des Europäischen Parlaments an den Rat und die Kommission nach der Prüfung von behaupteten Verstößen gegen das Unionsrecht und Missständen bei dessen Anwendung im Zusammenhang mit dem Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware[1] (2023/2500(RSP))

Das Europäische Parlament,

– unter Hinweis 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 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 (Datenschutzrichtlinie für elektronische Kommunikation)[2],

– 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, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)[3],

– 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[4],

– 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],

– 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

[1] Der Entwurf des Berichts beruht auf dem Dokument, in dem die Berichterstatterin ihre Erkenntnisse darlegt. Jede Person, die im Verlauf der Untersuchung namentlich genannt wird und der dies zum Nachteil gereichen könnte, hat das Recht, vom Ausschuss gehört zu werden. Das Sekretariat ist zu erreichen unter pega-secretariat@europarl.europa.eu.
[2] ABl. L 201 vom 31.7.2002, S. 37.
[3] ABl. L 119 vom 4.5.2016, S. 1.
[4] ABl. L 119 vom 4.5.2016, S. 89.
[5] ABl. L 206 vom 11.6.2021, S. 1.

bedrohen[6], in der durch den Beschluss (GASP) 2021/796 des Rates vom 17. Mai 2021[7] geänderten Fassung,

– 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 19. April 1995 über Einzelheiten der Ausübung des Untersuchungsrechts des Europäischen Parlaments[9],

– unter Hinweis auf die Charta der Vereinten Nationen und die Leitprinzipien der Vereinten Nationen für Wirtschaft und Menschenrechte[10],

– unter Hinweis auf die Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten, insbesondere ihre Artikel 8, 9, 13 und 17, und die Protokolle zu dieser Konvention,

– 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[11] sowie auf seine Empfehlungen im Hinblick auf die Stärkung der IT-Sicherheit in den Organen, Einrichtungen und sonstigen Stellen der Union,

– unter Hinweis auf den Bericht der Venedig-Kommission betreffend die demokratische Aufsicht der Sicherheitsdienste[12] und das Gutachten über das Gesetz vom 15. Januar 2016 zur Änderung des Polizeigesetzes und bestimmter anderer Gesetze[13],

– gestützt auf Artikel 208 seiner Geschäftsordnung,

A. in der Erwägung, dass sich herausgestellt hat, dass staatliche Stellen in mehreren Ländern, sowohl in den Mitgliedstaaten als auch in Drittländern, Pegasus und andere Marken von 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 Menschenrechten und Demokratie deutlich wird;

---

[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] https://www.auswaertiges-amt.de/blob/266624/b51c16faf1b3424d7efa060e8aaa8130/un-leitprinzipien-de-data.pdf.
[11] ABl. C 378 vom 9.11.2017, S. 104.
[12] https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)010-e
[13] https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)012-e

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

C. in der Erwägung, dass verschlüsselte mobile Kommunikationsanwendungen zum Aufkommen der Spähsoftware-Branche geführt haben, mit der bestehende Schwachstellen in den Betriebssystemen von Smartphones ausgenutzt werden, um Software zu installieren, mit der Spähsoftware in das Telefon importiert werden kann, auch durch „Zero-Click“, was die Extraktion von Daten vor der Verschlüsselung ermöglicht;

D. in der Erwägung, dass der Einsatz von Überwachungs- und Spähsoftware die Ausnahme bleiben sollte und immer einer wirksamen und sinnvollen 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, den Terrorismus und schwere Straftaten betreffen;

E. in der Erwägung, dass jede Überwachung durch Überwachungs- und Spähsoftware nachträglich von einer unabhängigen Aufsichtsbehörde überprüft werden muss, die sicherstellen muss, dass jede genehmigte Überwachung im Einklang mit den Grundrechten und den vom Gerichtshof der Europäischen Union (EuGH), dem Europäischen Gerichtshof für Menschenrechte (EGMR) und der Venedig-Kommission festgelegten Bedingungen durchgeführt wird, und die in der Lage sein muss, die Überwachung zu beenden, wenn dies nicht der Fall ist;

F. in der Erwägung, dass eine Überwachung durch Überwachungs- und 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, insbesondere der Artikel 7, 8, 11, 17, 21 und 47 der Charta, in denen die in der Charta verankerten spezifischen 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;

G. in der Erwägung, dass die Rechte der Zielpersonen in der Charta der Grundrechte 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;

H. in der Erwägung, dass aus den Aussagen der Opfer hervorgeht, dass Rechtsbehelfe und Bürgerrechte zwar auf dem Papier bestehen mögen, aber angesichts der Behinderung durch staatliche Stellen, der fehlenden Umsetzung des Rechts auf Information der Opfer und des Verwaltungsaufwands für den Nachweis des Opferstatus zumeist leerlaufen;

I. in der Erwägung, dass die polnische Regierung die institutionellen und rechtlichen Schutzmechanismen, einschließlich angemessener Aufsichts- und Kontrollverfahren, geschwächt und abgeschafft hat, sodass den Opfern keine wirksamen Rechtsmittel zur Verfügung stehen; in der Erwägung, dass die Überwachungs- und Spähsoftware

Pegasus illegal eingesetzt wurde, um Journalisten, Politiker, Staatsanwälte und Akteure der Zivilgesellschaft zu politischen Zwecken auszuspähen;

J. in der Erwägung, dass die ungarische Regierung die institutionellen und rechtlichen Schutzmechanismen, einschließlich angemessener Aufsichts- und Kontrollverfahren, geschwächt und abgeschafft hat, sodass den Opfern keine wirksamen Rechtsmittel zur Verfügung stehen; in der Erwägung, dass die Überwachungs- und Spähsoftware Pegasus illegal eingesetzt wurde, um Journalisten, Politiker, Staatsanwälte und Akteure der Zivilgesellschaft zu politischen Zwecken auszuspähen;

K. in der Erwägung, dass griechische Parlamentsabgeordnete, Abgeordnete der Opposition und der Nea Demokratia (ND), Parteifreunde der ND und Journalisten mit der nach griechischem Recht illegalen Spähsoftware Predator ausspioniert wurden; in der Erwägung, dass viele der Zielpersonen auch vom griechischen Geheimdienst EYP offiziell überwacht 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 erteilt hat; in der Erwägung, dass die Regierung auf den Skandal mit Gesetzesänderungen reagiert hat, die das Recht der Zielperson, nach einer Überwachung informiert zu werden, weiter einschränken;

L. in der Erwägung, dass Enthüllungen zwei Kategorien von Spähzielen in Spanien ergeben haben; in der Erwägung, dass die erste Kategorie den Premierminister und den Verteidigungsminister umfasst, von denen angenommen wird, dass sie von Marokko ausspioniert werden; in der Erwägung, dass der zweite Fall etwa 65 Opfer betrifft, die als „CatalanGate“ bezeichnet werden, darunter katalanische Parlamentarier, Abgeordnete, Rechtsanwälte und Akteure der Zivilgesellschaft; in der Erwägung, dass die spanischen Behörden im Mai 2020 zugegeben haben, 18 dieser 65 Opfer mit gerichtlicher Genehmigung ins Visier genommen zu haben, dass sie jedoch unter Berufung auf die nationale Sicherheit keine weiteren Angaben gemacht haben;

M. in der Erwägung, dass es Behauptungen gibt, die zypriotische Regierungspartei spähe Kritiker aus, dass aber bisher keine Infektionen von Überwachungs- und Spähsoftware festgestellt worden sind; in der Erwägung, dass Zypern ein wichtiges europäisches Exportzentrum für die Überwachungsindustrie und ein attraktiver Standort für Unternehmen ist, die Überwachungstechnologien verkaufen;

N. in der Erwägung, dass es deutliche Hinweise darauf gibt, dass unter anderem die Regierungen von Marokko und Ruanda Unionsbürger mit Spähsoftware ausspioniert haben, darunter den französischen Staatspräsidenten, den spanischen Premierminister und Verteidigungsminister, den damaligen belgischen Premierminister, den ehemaligen Kommissionspräsidenten und ehemaligen italienischen Premierminister sowie die Tochter von Paul Rusesabagina;

O. 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 von der unrechtmäßigen Verwendung von

Spähsoftware absehen werden, dass aber in Ermangelung eines soliden Rechtsrahmens mit Schutzmaßnahmen und Überwachung die Gefahr des Missbrauchs sehr hoch ist;

P. in der Erwägung, dass die Regierungen und Parlamente der Mitgliedstaaten dem Parlament keine aussagekräftigen Informationen über die rechtlichen Rahmenbedingungen für die Verwendung von Spähsoftware in ihren Mitgliedstaaten 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;

Q. in der Erwägung, dass mehrere wichtige Personen aus der Spähsoftware-Branche eine maltesische Staatsangehörigkeit erlangt haben, um frei innerhalb der Union und aus der Union heraus agieren zu können.

R. in der Erwägung, dass verschiedene Anbieter von Spähsoftware in einem oder mehreren Mitgliedstaaten gemeldet 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;

S. in der Erwägung, dass alle Mitgliedstaaten außer Zypern am Wassenaar-Arrangement über Ausfuhrkontrollen für konventionelle Waffen sowie Güter und Technologien mit doppeltem Verwendungszweck teilnehmen;

T. in der Erwägung, dass die israelische Ausfuhrregelung[14] grundsätzlich für alle israelischen Staatsbürger gilt, auch wenn sie von der EU aus operieren; in der Erwägung, dass Israel kein Teilnehmerland des Wassenaar-Arrangements ist, aber behauptet, dessen Standards dennoch anzuwenden;

U. 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 einen ersten Durchführungsbericht herausgegeben hat[15];

V. in der Erwägung, dass sich Hersteller von Spähsoftware, die in Drittländer exportieren, in der Union niederlassen, um Ansehen zu gewinnen, während sie mit Spähsoftware für totalitäre Regime handeln; in der Erwägung, dass Ausfuhren aus der Union an totalitäre Regime oder nichtstaatliche Akteure stattfinden, was einen Verstoß gegen die EU-Ausfuhrbestimmungen für Überwachungstechnologien darstellt;

W. in der Erwägung, dass Amesys und Nexa Technologies derzeit in Frankreich wegen der

[14] Verteidigungsausfuhrkontrollgesetz 5766-2007, israelisches Verteidigungsministerium.
[15] https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1662029750223&uri=COM%3A2022%3A434%3AFIN

Ausfuhr von Überwachungstechnologie nach Libyen, Ägypten und Saudi-Arabien strafrechtlich verfolgt werden; in der Erwägung, dass die in Griechenland ansässigen Intellexa-Unternehmen ihre Produkte nach Bangladesch, Sudan, Madagaskar und in mindestens ein arabisches Land exportiert haben sollen, 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 und die Türkei, und dass Marokkos Geheimdienste von Amnesty und Forbidden Stories beschuldigt werden, die Spähsoftware Pegasus gegen Journalisten und Politiker einzusetzen; in der Erwägung, dass nicht bekannt ist, ob Ausfuhrgenehmigungen für die Ausfuhr von Spähsoftware in alle diese Länder erteilt wurden;

X. 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 der örtlichen Polizeibehörden, besucht wird;

Y. in der Erwägung, dass die Mitgliedstaaten behaupten, dass Angelegenheiten, die die nationale Sicherheit betreffen, nicht unter die Verträge fallen, da Artikel 4 Absatz 2 EUV vorsieht, dass die nationale Sicherheit in der alleinigen Zuständigkeit der Mitgliedstaaten verbleibt;

Z. in der Erwägung, dass der Gerichtshof entschieden hat (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“.

AA. in der Erwägung, dass der Gerichtshof entschieden hat (C-203/15), dass „Art. 15 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“;

AB. in der Erwägung, dass der Gerichtshof entschieden hat (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“;

AC. 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 und dass alle Mitgliedstaaten diesem Übereinkommen beigetreten sind;

AD. in der Erwägung, dass der Einsatz 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 fällt;

AE. in der Erwägung, dass in der Charta die Bedingungen für die Einschränkung der Ausübung der Grundrechte festlegt sind: Die Einschränkung muss gesetzlich vorgesehen sein, den Wesensgehalt der betreffenden Rechte und Freiheiten achten, dem Grundsatz der Verhältnismäßigkeit unterliegen und darf nur auferlegt werden, wenn sie notwendig ist und tatsächlich den von der Union anerkannten Zielen des Allgemeininteresses oder der Notwendigkeit, die Rechte und Freiheiten anderer zu schützen, entspricht; in der Erwägung, dass im Falle 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 als verhältnismäßig angesehen werden kann, unabhängig davon, ob die Maßnahme als notwendig erachtet werden kann, um die legitimen Ziele eines demokratischen Staates zu erreichen;

AF. 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 dadurch 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;

AG. 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;

AH. in der Erwägung, dass die Infektion eines Geräts mit Spähsoftware und die anschließende Sammlung von Daten über die Server des Mobilfunkanbieters erfolgt und dass das freie Roaming innerhalb der Union dazu geführt hat, dass Personen immer häufiger Mobilfunkverträge aus anderen Mitgliedstaaten als dem haben, in dem sie leben, gibt es im Unionsrecht derzeit keine Rechtsgrundlage für die Sammlung von Daten in dem anderen Mitgliedstaat durch den Einsatz von Spähsoftware;

AI. in der Erwägung, dass die Mitgliedstaaten die Richtlinie 2014/24/EU und die Richtlinie 2009/81/EG über die öffentliche Auftragsvergabe und die Auftragsvergabe im Bereich Verteidigung beachten müssen, eine Ausnahme gemäß Artikel 346 Absatz 1 Buchstabe b AEUV angemessen rechtfertigen müssen, da die sensiblen Merkmale der Beschaffung im Bereich Verteidigung in der Richtlinie von 2009 ausdrücklich berücksichtigt werden, und das WHO-Übereinkommen über das öffentliche Beschaffungswesen in der am 30. März 2012 geänderten Fassung[16] beachten müssen, wenn sie Partei dieses Übereinkommens sind;

AJ. 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 totalitäre Regime zu verkaufen;

AK. in der Erwägung, dass Israel seit 2000 an den Forschungsprogrammen der Union teilnimmt; in der Erwägung, dass israelischen Militär- und Sicherheitsunternehmen im Rahmen dieser europäischen Programme Mittel zur Verfügung gestellt wurden;

AL. in der Erwägung, dass das wichtigste Rechtsinstrument im Rahmen der Entwicklungspolitik der Union die Verordnung (EU) 2021/947 – die Verordnung über das NDICI – Europa in der Welt[17] – ist und dass die Finanzierung durch die Union über die in der Haushaltsordnung vorgesehenen Finanzierungsarten erfolgen kann, auch wenn die Hilfe im Fall einer Verschlechterung der Demokratie, der Menschenrechte oder der Rechtsstaatlichkeit in Drittländern ausgesetzt werden könnte;

1. hebt die unbestreitbare Bedeutung des Schutzes der Privatsphäre und des Rechts auf Menschenwürde und Privatsphäre in einer zunehmend digitalen Welt hervor, in der immer mehr unserer Aktivitäten online stattfinden;

2. ist der festen Überzeugung, dass die Verletzung des Rechts auf Würde, Privatsphäre und Privatleben nicht nur eine Frage der Achtung der in den Verträgen und in anderen Quellen festgelegten gemeinsamen Rechtsgrundsätze ist, sondern eine grundlegende

[16] https://www.wto.org/english/tratop_e/gproc_e/gpa_1994_e.htm.
[17] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32021R0947&qid=1673533558345&from=EN

Frage, ob das künftige menschliche Leben frei und demokratisch oder durch digitale Prozesse kontrolliert sein wird;

3. verurteilt aufs Schärfste den Einsatz von Spähsoftware durch Regierungen oder Regierungsmitglieder der Mitgliedstaaten zum Zwecke der Überwachung, Erpressung, Einschüchterung, Manipulation und Diskreditierung von Opposition und Kritikern, der Ausschaltung der demokratischen Kontrolle und der Pressefreiheit sowie der Manipulation von Wahlen;

4. weist darauf hin, dass durch diesen unrechtmäßigen Einsatz von Spähsoftware durch nationale Regierungen direkt und indirekt die Organe der Union und der Entscheidungsprozess 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 aus dem Inneren der Union zu reagieren;

6. 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 grobe Verletzung der Ausfuhrbestimmungen der Union darstellt;

7. ist der Ansicht, dass es in Polen, Ungarn, Griechenland, Spanien und Zypern zu Verstößen oder Missständen bei der Umsetzung des Unionsrechts in Bezug auf die Verwendung von und den Handel mit Spähsoftware gekommen ist;

8. äußert darüber hinaus seine Besorgnis über die Verwendung von und den Handel mit Spähsoftware durch andere Mitgliedstaaten, die gemeinsam die Union als sicheren Hafen für die Spähsoftware-Branche pflegen und dabei häufig gegen die Gesetze und Normen der Union verstoßen;

9. ist ferner der Ansicht, dass Regierungsstellen von Drittländern hochrangige Persönlichkeiten in der Union mit Spähsoftware ins Visier genommen haben;

10. ist ebenso besorgt über die offensichtliche Zurückhaltung bei der Untersuchung von Spähangriffen, 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 Spähangriffen auf Regierungschefs und Minister der EU-Mitgliedstaaten nur sehr langsam vorankommen und es ihnen an Transparenz mangelt;

11. verurteilt die Weigerung der Regierungen der Mitgliedstaaten, des Rates und der Kommission, uneingeschränkt an der Untersuchung mitzuarbeiten und alle relevanten und aussagekräftigen Informationen weiterzugeben; ist der Auffassung, dass die kollektive Antwort des Rates völlig unzureichend ist und dem Grundsatz der loyalen Zusammenarbeit widerspricht;

12. kommt zu dem Schluss, dass weder die Mitgliedstaaten noch der Rat, noch die Kommission den Wunsch haben, den Spionageskandal aufzuklären, und somit wissentlich die Regierungen der Union schützen, die die Menschenrechte innerhalb und außerhalb der Union verletzen;

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

14. fordert Polen auf:

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

b) dem Urteil des Verfassungsgerichtshofs zum Polizeigesetz von 1990 nachzukommen;

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

d) 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 Opfer 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;

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

f) die vollständige Unabhängigkeit der Justiz und aller einschlägigen Aufsichtsorgane wiederherzustellen, wie des Bürgerbeauftragten und der Datenschutzbehörden, um sicherzustellen, dass alle Aufsichtsorgane uneingeschränkt zusammenarbeiten und Zugang zu Informationen erhalten und alle Opfer umfassend informiert werden;

g) 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;

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

i) die polnische Staatsanwaltschaft aufzufordern, Ermittlungen über den

Missbrauch von Spähsoftware einzuleiten;

j) die Hinweisgeber-Richtlinie umzusetzen;

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

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

16. fordert Ungarn auf:

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

b) den verschiedenen Urteilen des EGMR zu entsprechen, wie dem Urteil in der Rechtssache Klass u. a./Deutschland aus dem Jahr 1978, in dem das Erfordernis der Benachrichtigung von Personen, die Ziel der Überwachung waren, dargelegt wird;

c) unabhängige Aufsichtsgremien im Einklang mit dem Urteil des EGMR in der Rechtssache Hüttl/Ungarn wiedereinzusetzen, in dem das Gericht feststellt, dass die NAIH (Nationale Behörde für Datenschutz und Informationsfreiheit) 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;

d) die vollständige Unabhängigkeit der Justiz und aller einschlägigen Aufsichtsorgane wiederherzustellen, wie des Bürgerbeauftragten und der Datenschutzbehörden, um sicherzustellen, dass alle Aufsichtsorgane uneingeschränkt zusammenarbeiten und Zugang zu Informationen erhalten und alle Opfer umfassend informiert werden;

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

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

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

18. 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 ADAE (Hellenische Behörde für Kommunikationssicherheit und Datenschutz), die Bürgerinnen und Bürger über die Aufhebung der Vertraulichkeit von Mitteilungen zu informieren, abgeschafft wurde, dringend zurückzuziehen;

e) die vollständige Unabhängigkeit der Justiz und aller einschlägigen Aufsichtsorgane wiederherzustellen, wie des Bürgerbeauftragten und der Datenschutzbehörden, um sicherzustellen, dass alle Aufsichtsorgane uneingeschränkt zusammenarbeiten und Zugang zu Informationen erhalten und alle Opfer umfassend informiert werden;

f) die Gesetzesänderung von 2019 rückgängig zu machen, mit der der EYP (Nationale Nachrichtendienst) der direkten Kontrolle des Premierministers unterstellt wurde;

g) dringend die Hinweisgeber-Richtlinie umzusetzen;

h) die Unabhängigkeit der EAD-Führung sicherzustellen;

i) dringend eine polizeiliche Untersuchung des mutmaßlichen Spähsoftware-Missbrauchs einzuleiten und physische Beweise von Proxys, Maklerfirmen und Spähsoftware-Anbietern zu beschlagnahmen, die mit den Infektionen durch Spähsoftware in Verbindung stehen;

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

19. kommt zu dem Schluss, dass der Rechtsrahmen in Spanien zwar mit den Anforderungen der Verträge und den Urteilen des EuGH und des EGMR im Einklang zu stehen scheint, die tatsächliche Umsetzung jedoch Fragen aufwirft, da Mitglieder des Parlaments sowie Anwälte, Politiker, Aktivisten und Journalisten ins Visier genommen wurden, ohne dass eine strafrechtliche Anklage oder eine offensichtliche unmittelbare Gefahr für die nationale Sicherheit vorlag;

20. fordert die Regierung Spaniens auf:

a) vollständige Klarheit über alle mutmaßlichen Fälle der Verwendung von Spähsoftware zu schaffen;

b) für einen echten und sinnvollen Rechtsschutz für alle Opfer und den unverzüglichen Abschluss der gerichtlichen Ermittlungen zu sorgen;

c) die anhaltende Krise im Justizwesen dringend zu lösen;

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

22. fordert die Regierung Zyperns auf:

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

b) den Bericht des Sonderermittlers im Fall des „Spyware Van“ (Spähsoftware-Wagen) zu veröffentlichen;

c) mit Unterstützung von Europol alle Behauptungen über den unrechtmäßigen Einsatz von Spähsoftware, insbesondere gegen Journalisten, Rechtsanwälte und Akteure der Zivilgesellschaft, umfassend zu untersuchen;

23. ist der Ansicht, dass die Lage in 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 Mitgliedstaaten wie Zypern und Bulgarien in die Lage versetzt, zu einer Drehscheibe für den Export von Spähsoftware an undemokratische Regime in aller Welt zu werden;

24. ist der Auffassung, dass das Versagen oder die Weigerung der nationalen Behörden, einen angemessenen Schutz der Unionsbürgerinnen und -bürger sicherzustellen, mit aller gebotenen Deutlichkeit zeigt, dass Maßnahmen auf Unionsebene unerlässlich sind, um dafür zu sorgen, dass der Wortlaut der Verträge eingehalten und die Rechtsvorschriften der Union beachtet werden, damit die Rechte der Bürgerinnen und Bürger auf Menschenwürde, Privatleben, personenbezogene Daten und Eigentum geachtet werden;

25. kommt zu dem Schluss, dass die Kommission und der Europäische Auswärtige Dienst (EAD) Verstöße und Missstände bei der Umsetzung des Unionsrechts begangen haben, als sie Drittländern, darunter auch zehn Ländern in der Sahelzone, Unterstützung beim Aufbau von Überwachungskapazitäten gewährten;

26. fordert die Kommission und den EAD auf:

a) unverzüglich jegliche Unterstützung für Drittländer einzustellen, mit der darauf abgezielt wird, ihnen die Entwicklung von Überwachungskapazitäten zu ermöglichen oder eine solche Entwicklung anderweitig zu erleichtern;

b) ein geeignetes Verfahren zur Bewertung der Auswirkungen auf die Menschen- und Grundrechte zu entwickeln, mit dem Artikel 51 der Charta der Grundrechte in vollem Umfang Rechnung getragen wird;

c) dem Parlament und dem Rat das Verfahren der Folgenabschätzung für Menschen- und Grundrechte vorzulegen;

d) die Folgenabschätzung für Menschen- und Grundrechte durchzuführen;

e) jegliche Unterstützung für Drittländer einzustellen, mit der darauf abgezielt wird, ihnen die Entwicklung von Überwachungskapazitäten zu ermöglichen oder eine solche Entwicklung anderweitig zu erleichtern, wenn die Achtung der Menschen- und Grundrechte, einschließlich der Rechtsstaatlichkeit, des Schutzes der demokratischen Grundsätze, der Politiker, der Menschenrechtsverteidiger und der Journalisten nicht sichergestellt werden kann;

27. 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 viel Zeit in Anspruch nehmen wird, und fordert die sofortige Verabschiedung eines bedingten Moratoriums für den Verkauf, den Erwerb, die Weitergabe und die Verwendung von Spähsoftware, das von Land zu Land aufgehoben werden muss, wenn die folgenden Bedingungen erfüllt sind:

a) Alle Fälle von mutmaßlichem Missbrauch von Spähsoftware von den zuständigen Strafverfolgungs-, Staatsanwaltschafts- und Justizbehörden wurden umfassend untersucht und unverzüglich geklärt und

b) es wurde nachgewiesen, dass der Rahmen für die Verwendung von Spähsoftware mit den von der Venedig-Kommission festgelegten Standards und der einschlägigen Rechtsprechung des EuGH und des EGMR übereinstimmt, und

c) es wurde die ausdrückliche Zusage gegeben, jedem Ersuchen von Europol gemäß Artikel 6 Absatz 1 a Europol-Verordnung in Bezug auf Ermittlungen wegen des Verdachts der unrechtmäßigen Verwendung von Spähsoftware nachzukommen, und

d) es wurden alle Ausfuhrgenehmigungen, die nicht vollständig mit dem Buchstaben und dem Geist der Verordnung über Güter mit doppeltem Verwendungszweck übereinstimmen, aufgehoben;

28. ist der Auffassung, dass die Erfüllung der Bedingungen von der Kommission bewertet werden muss;

29. vertritt die Auffassung, dass es einen eindeutigen Bedarf an gemeinsamen EU-Standards zur Regelung der Verwendung von Spähsoftware durch die Einrichtungen der Mitgliedstaaten gibt, die sich auf die vom EuGH, dem EGMR und der Venedig-Kommission festgelegten Standards stützen; ist der Ansicht, dass solche EU-Normen zumindest die folgenden Elemente umfassen sollten:

a) Der geplante Einsatz von Spähsoftware muss einer wirksamen und aussagekräftigen richterlichen Vorabgenehmigung durch eine unparteiische und unabhängige Justizbehörde unterliegen, die 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 festlegen, und das Hacken 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;

c) die Genehmigung für den Einsatz von Spähsoftware darf nur für Ermittlungen in einer eingeschränkten und abschließenden Aufzählung von Straftaten erteilt werden, und Spähsoftware darf nur gegen Personen eingesetzt werden, bei denen hinreichende Anhaltspunkte dafür vorliegen, dass sie solche Straftaten begangen haben oder planen;

d) es sollte eine nicht abschließende, aber verbindliche Aufzählung von privilegierten und sensiblen Berufen wie Anwälten, Journalisten, Politikern und Ärzten geben, die nicht Ziel von Spähsoftware sein dürfen;

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 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) das Recht auf Benachrichtigung der betroffenen Bürgerinnen und Bürger: Nach Beendigung der Überwachung sollten die Behörden die Bürgerinnen und Bürger darüber informieren, dass sie von den Behörden mit Spähsoftware überwacht wurden, einschließlich Informationen über das Datum und die Dauer der Überwachung, die für die Überwachung ausgestellte Anordnung, die erhaltenen Daten, Informationen darüber, wie diese Daten verwendet wurden und von welchen Akteuren, sowie das Datum der Löschung der Daten; stellt fest, dass eine solche Benachrichtigung unverzüglich erfolgen sollte, es sei denn, eine unabhängige Justizbehörde gewährt einen Aufschub der Benachrichtigung; in diesem Fall würde eine sofortige Benachrichtigung den Zweck der Überwachung ernsthaft gefährden;

h) eine wirksame und unabhängige Ex-post-Kontrolle über den Einsatz von Spähsoftware, bei der alle erforderlichen Mittel und Befugnisse gegeben sein müssen, um eine sinnvolle Kontrolle auszuüben, und die mit einer parteiübergreifenden parlamentarischen Kontrolle und einem uneingeschränkten Zugang zu Informationen gekoppelt sein muss;

i) einen sinnvollen Rechtsbehelf für direkte und indirekte Zielpersonen und dass Personen, die behaupten, von der Überwachung beeinträchtigt zu sein, Zugang zu Rechtsmitteln durch eine unabhängige Stelle haben sollten; fordert daher die Einführung einer Meldepflicht für staatliche Behörden, einschließlich angemessener Fristen für die Meldung, wobei die Zustellung erfolgt, sobald

die Sicherheitsbedrohung vorüber ist;

j) 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, 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;

k) es ist wichtig, dass der kostenlose Zugang der Opfer zu technischem Fachwissen in dieser Phase verbessert wird, da eine bessere Verfügbarkeit und Erschwinglichkeit technischer Verfahren, wie z. B. der forensischen Analyse, es den Opfern ermöglichen würde, vor Gericht bessere Argumente vorzubringen;

l) während der Überwachung sollten die Behörden alle irrelevanten Daten löschen, 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;

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

30. betont, dass nur Spähsoftware, die so konfiguriert ist, dass durch sie die Funktionalität von Spähsoftware gemäß dem Rechtsrahmen nach Artikel 82 AEUV ermöglicht und erleichtert wird und insbesondere die verschiedenen Rollen der beteiligten Behörden unterstützt werden, auf dem Binnenmarkt in Verkehr gebracht, entwickelt oder in der Union verwendet werden darf;

31. betont, dass Spähsoftware nur für den Verkauf an und die Verwendung durch eine abschließende Aufzählung von Behörden in Verkehr gebracht werden darf, deren Auftrag die Untersuchung von Straftaten umfasst, für die der Einsatz von Spähsoftware genehmigt werden kann;

32. hebt die Verpflichtung hervor, eine Version von Spähsoftware zu verwenden, die so programmiert ist, dass sie den Zugriff auf Daten minimiert, d. h. die Spähsoftware sollte nicht auf alle auf einem Gerät gespeicherten Daten zugreifen können, sondern so programmiert sein, dass der Zugriff auf Daten auf das unbedingt erforderliche Maß beschränkt ist;

33. kommt zu dem Schluss, dass der Erwerb von Spähsoftware durch einen Mitgliedstaat von einer unabhängigen, unparteiischen Prüfstelle geprüft werden muss;

34. betont, dass alle Einrichtungen, die Spähsoftware auf dem Binnenmarkt in Verkehr

bringen, strenge Sorgfaltspflichten erfüllen sollten, einschließlich der Überprüfung potenzieller Kunden, und der Kommission jährlich über die Einhaltung dieser Pflichten Bericht erstatten sollten;

Eine Definition der „nationalen Sicherheit“ ist wichtig

35. verurteilt die Berufung auf die „nationale Sicherheit“ als Vorwand für den Missbrauch von Spähsoftware und für absolute Geheimhaltung und fehlende Rechenschaftspflicht; begrüßt die Erklärung der Kommission, dass ein bloßer Verweis auf die nationale Sicherheit nicht als unbegrenzte Ausnahme von den normalen Vorschriften ausgelegt werden kann, und fordert die Kommission auf, dieser Erklärung in den Fällen, in denen ein offensichtlicher Missbrauch vorliegt, Folge zu leisten;

36. fordert eine gemeinsame rechtliche Definition des Begriffs „nationale Sicherheit“ und die Festlegung von Kriterien für die Bestimmung der rechtlichen Regelung in Fragen der nationalen Sicherheit sowie eine klare Abgrenzung des Bereichs, in dem eine solche Sonderregelung gelten kann;

37. ist der Auffassung, dass der Einsatz von Spähsoftware eine Einschränkung der Grundrechte darstellt; weist erneut darauf hin, dass in der Charta der Grundrechte vorgesehen ist, dass jede Einschränkung der Grundrechte gemäß Artikel 52 Absatz 1 gesetzlich vorgesehen sein muss; ist daher der Ansicht, dass es wichtig ist, den Begriff „nationale Sicherheit“ zu definieren;

Bessere Durchsetzung der geltenden Rechtsvorschriften

38. unterstreicht die Unzulänglichkeiten des nationalen Rechtsrahmens und dass eine bessere Durchsetzung des bestehenden Unionsrechts wichtig ist, um diesen Mängeln entgegenzuwirken; stellt fest, dass die folgenden Unionsvorschriften zwar relevant sind, aber nicht ordnungsgemäß durchgesetzt werden: die Geldwäscherichtlinie, die Vorschriften für das öffentliche Beschaffungswesen, die Verordnung über Güter mit doppeltem Verwendungszweck, die Rechtsprechung (Urteile zur Überwachung und zur nationalen Sicherheit) und die Hinweisgeber-Richtlinie; 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 Sommer 2023 vorzulegen;

39. hält die strikte Umsetzung und Durchsetzung des Rechtsrahmens der Union zum Datenschutz, insbesondere der Strafverfolgungsrichtlinie, der allgemeinen Datenschutzverordnung und der Datenschutzrichtlinie für elektronische Kommunikation, für eine entscheidende Voraussetzung; hält es für ebenso wichtig, dass die einschlägigen Urteile des EuGH vollständig umgesetzt werden, was in mehreren Mitgliedstaaten noch nicht der Fall ist, wobei der Kommission eine zentrale Rolle bei der Durchsetzung des EU-Rechts und der Sicherstellung seiner einheitlichen Anwendung in der gesamten Union zukommt;

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

41. fordert, dass Zypern ein Teilnehmerstaat des Wassenaar-Arrangements wird, und weist

den Rat, die Mitgliedstaaten und die Kommission erneut darauf hin, dass alle Anstrengungen unternommen werden müssen, um Zypern den Beitritt zum Wassenaar-Arrangement zu ermöglichen;

42. 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 Kauf von Überwachungstechnologien von Staaten, die dem Arrangement nicht angehören, verbieten sollten;

43. betont, dass die Kommission angesichts der Enthüllungen über Spähsoftware eine eingehende Untersuchung der Ausfuhrgenehmigungen durchführen sollte, die für die Verwendung von Spähsoftware im Rahmen der Verordnung über Güter mit doppeltem Verwendungszweck erteilt wurden;

44. 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;

45. 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 zur internen Repression und/oder zur Begehung schwerer Verstöße gegen die Menschenrechte und das humanitäre Völkerrecht bestimmt sind oder bestimmt sein könnten;

46. 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;

47. betont, dass die benannten nationalen Behörden, die für die Genehmigung und 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 das betreffende Gut mit doppeltem Verwendungszweck enthalten: die Anzahl der beantragten Genehmigungen, den Namen des Ausfuhrlandes, die Beschreibung des Ausfuhrunternehmens und die Angabe, ob es sich bei diesem Unternehmen um eine Tochtergesellschaft handelt, eine Beschreibung des Endnutzers und des Bestimmungsortes, den Wert der Ausfuhrgenehmigung, die Gründe für die Genehmigung oder Verweigerung der Ausfuhrgenehmigung; hebt hervor, dass diese Berichte vierteljährlich veröffentlicht werden sollten; fordert die Einrichtung eines ständigen parlamentarischen Ausschusses mit Zugang zu Verschlusssachen durch die Kommission, um die parlamentarische Kontrolle sicherzustellen;

48. 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 des geschäftlich sensiblen Charakters, der Verteidigungs- und Außenpolitik oder der nationalen Sicherheit abgeschafft werden muss; ist stattdessen der Auffassung, dass die Kommission, um zu verhindern, dass sensible Informationen Drittländern zugänglich gemacht werden, beschließen kann, bestimmte Informationen in ihrem Jahresbericht als vertraulich einzustufen;

49. 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, besonders entwickelt oder geändert für die Überwachung oder Analyse zur Verhütung oder Verfolgung von Straftaten oder zum Strafvollzug, 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, konstruiert entweder für die Überwachung oder Beobachtung des elektromagnetischen Spektrums für militärisch-nachrichtendienstliche oder sicherheitsmäßige Zwecke, und unbemannte Luftfahrzeuge, mit denen eine Überwachung durchgeführt werden kann;

50. 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 einen Rahmen für Menschenrechte und Sorgfaltspflicht einrichten;

Internationale Zusammenarbeit zum Schutz der Bürgerinnen und Bürger

51. fordert eine gemeinsame Spähsoftware-Strategie der EU und der USA, einschließlich einer gemeinsamen weißen und/oder schwarzen Liste von Spähsoftware-Anbietern, die (nicht) an Behörden verkaufen dürfen, gemeinsamer Kriterien für die Aufnahme von Anbietern in eine der beiden Listen, einer gemeinsamen Berichterstattung der EU und der USA über die Branche, gemeinsamer Kontrollen, gemeinsamer Sorgfaltspflichten für Anbieter und der Kriminalisierung des Verkaufs von Spähsoftware an nichtstaatliche Akteure;

52. fordert den EU-US-Handels- und Technologierat auf, umfassende und offene Konsultationen mit der Zivilgesellschaft für die Entwicklung der gemeinsamen Strategie und der Standards EU-USA durchzuführen;

53. 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 infrage kommenden Länder und Regelungen für die Sorgfaltspflicht enthalten sind;

54. betont, dass im Vergleich zu den USA, wo die NSO schnell auf die schwarze Liste gesetzt wurde und es parteiübergreifende Initiativen für Rechtsvorschriften über kommerzielle Spähsoftware gibt, in der Union keine Maßnahmen in Bezug auf die Einfuhr von Spähsoftware getroffen wurden und die Durchsetzung der Ausfuhrbestimmungen völlig unzureichend ist;

55. kommt zu dem Schluss, dass die Ausfuhrbestimmungen der Union und ihre Durchsetzung zum Schutz der Menschenrechte in Drittländern mit mehr Nachdruck betrieben werden müssen und 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;

Zero-Day-Schwachstellen

56. fordert unbeschadet der NIS2-Richtlinie und des Cyberresilienzgesetzes eine Regelung für die Aufdeckung, Weitergabe, Behebung und Ausnutzung von Sicherheitslücken;

57. 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, u. a. gemäß den Rechtsvorschriften zur Cyberkriminalität und der Urheberrechtsrichtlinie;

58. 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;

59. fordert ein Verbot des gewerbsmäßigen Handels mit Sicherheitslücken und eine Verpflichtung zur Offenlegung der Ergebnisse der Schwachstellenforschung, damit sie behoben werden können;

60. fordert die Organisationen auf, eine öffentlich zugängliche Kontaktstelle einzurichten, bei der Schwachstellen auf standardisierte Weise offengelegt werden können, und die Organisationen, die Informationen über Schwachstellen in ihrem System erhalten, aufzufordern, unverzüglich für Abhilfe zu sorgen; fordert eine maximale Frist für die Behebung der gemeldeten Schwachstellen nach der Meldung;

61. fordert ein Verbot für Behörden, Schwachstellen zu erwerben, offenzuhalten oder auf Vorrat zu lagern, außer in begrenzten, genau festgelegten Fällen mit klaren, gesetzlich geregelten Verfahren für die Gleichbehandlung von Schwachstellen, mit einer Prüfung der Notwendigkeit/Verhältnismäßigkeit für die Entscheidung, eine Schwachstelle offenzulegen oder ausnahmsweise zurückzuhalten, und mit strengen Regeln für die Verzögerung der Meldung, die einer strengen Kontrolle durch eine unabhängige Aufsichtsbehörde unterliegen;

Telekommunikationsnetze

62. betont, dass die Lizenz des Hauptbetreibers, über den der staatliche Akteur Zugang hat, entzogen werden sollte, wenn ein staatlicher Akteur einen Zugangspunkt zum SS7-Netz hat;

63. betont, dass die derzeitige unbegrenzte Möglichkeit für Unbekannte, jede beliebige Nummer für jedes Land der Welt zu kaufen, besser reguliert werden sollte, um böswillige Aktivitäten zu erschweren;

64. fordert die Telekommunikationsanbieter auf, entschlossen und nachweislich gegen

Spoofing vorzugehen;

Schutz der Privatsphäre in der elektronischen Kommunikation

65. fordert die rasche Verabschiedung der Verordnung über Privatsphäre und elektronische Kommunikation in einer 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; weist darauf hin, dass der Anwendungsbereich der Überwachung nicht über die Datenschutzrichtlinie für elektronische Kommunikation hinausgehen sollte;

Die Rolle von Europol

66. erklärt sich bestürzt darüber, dass Europol sich weigert, ihre neu erworbenen Befugnisse gemäß der Verordnung (EU) 2022/991, mit der es ihr ermöglicht wird, den zuständigen Behörden der betroffenen Mitgliedstaaten die Einleitung, Durchführung oder Koordinierung strafrechtlicher Ermittlungen vorzuschlagen, in vollem Umfang zu nutzen, insbesondere wenn die nationalen Behörden nicht in der Lage oder nicht willens sind, Ermittlungen durchzuführen, und insbesondere, wenn die begründete Sorge besteht, dass Beweise vernichtet werden könnten;

67. fordert alle Mitgliedstaaten auf, sich zu verpflichten, den Vorschlägen von Europol im Rahmen des oben genannten Artikels zuzustimmen;

68. fordert Europol auf, ein Register der Strafverfolgungsmaßnahmen zu erstellen, bei denen Spähsoftware innerhalb von Europol 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;

69. fordert die Überarbeitung der Europol-Verordnung, damit Europol in Ausnahmefällen auch ohne Zustimmung der Mitgliedstaaten strafrechtliche Ermittlungen einleiten kann, wenn die nationalen Behörden versagen oder sich weigern zu ermitteln und eindeutige Bedrohungen für die Interessen und die Sicherheit der EU vorliegen;

Entwicklungshilfe der EU

70. fordert die Kommission auf, strengere Kontrollmechanismen einzuführen, um sicherzustellen, dass mit der Entwicklungshilfe der Union keine Instrumente finanziert oder unterstützt werden, die gegen die Grundsätze der Demokratie, der guten Regierungsführung, der Rechtsstaatlichkeit und der Achtung der Menschenrechte verstoßen 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;

Die Finanzordnung der Union

71. 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;

Weiterverfolgung der Entschließungen des Parlaments

72. 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-Bürgerinnen und -Bürger und zu der transatlantischen Zusammenarbeit im Bereich Justiz und Inneres; betont, dass die folgenden Empfehlungen dringend umgesetzt werden müssen;

73. betont, dass trotz der Tatsache, dass die Aufsicht über die Tätigkeiten der Nachrichtendienste sowohl auf demokratischer Legitimität (starker Rechtsrahmen, Vorabgenehmigung und Ex-post-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;

74. 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;

75. 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;

76. Diese hochrangige Gruppe sollte:

a) europäische Mindestnormen oder Leitlinien zur (Ex-ante- und Ex-post)-Aufsicht 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 den Urheber“ gelten, sowie zur Aufsicht und Rechenschaftspflicht ausländischer Nachrichtendienste;

b) die Dauer und die Reichweite jeder angeordneten Überwachung strikt begrenzen, sofern deren Fortsetzung nicht ordnungsgemäß durch die Genehmigungs-/Aufsichtsbehörde begründet wird; erneut darauf hinweisen,

dass die Dauer jeder angeordneten Überwachung verhältnismäßig und auf ihren Zweck begrenzt sein sollte;

c) Kriterien für mehr Transparenz auf der Grundlage des allgemeinen Grundsatzes des Zugangs zu Informationen und der sogenannten „Tshwane-Prinzipien“[18] erarbeiten;

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

78. 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;

79. fordert die Mitgliedstaaten auf, die Zusammenarbeit der Aufsichtsgremien untereinander auszubauen, insbesondere innerhalb des European Network of National Intelligence Reviewers (ENNIR — europäisches Expertennetz zur Kontrolle der Nachrichtendienste);

80. fordert die Kommission auf, einen Vorschlag für ein Verfahren der Sicherheitsüberprüfung der Union für alle Amtsträger der Union 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;

81. weist erneut hin auf 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;

Wissenschaftsprogramme der Union

82. fordert die Einführung strengerer Kontrollmechanismen, um sicherzustellen, dass die Forschungsmittel der Union keine Instrumente 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;

Ein Technologielabor der Union

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

83. fordert die Kommission auf, unverzüglich ein unabhängiges europäisches interdisziplinäres Institut zu gründen, das sich auf Forschung und Entwicklung an der Schnittstelle von Informations- und Kommunikationstechnologie, Grundrechten und Sicherheit konzentriert und auch die Aufgabe hat, die unrechtmäßige Verwendung von Software für illegale Überwachungszwecke aufzudecken und zu entlarven;

Rechtsstaatlichkeit

84. betont, dass die Auswirkungen der unrechtmäßigen Verwendung von Spähsoftware in den Mitgliedstaaten viel ausgeprägter sind, in denen die Behörden, die normalerweise mit der Untersuchung und der Wiedergutmachung für die Opfer betraut sind, vom Staat vereinnahmt werden, und dass man sich auf die nationalen Behörden nicht verlassen kann, wenn es eine Krise der Rechtsstaatlichkeit gibt;

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

    a) die Einführung einer umfassenderen Überwachung der Rechtsstaatlichkeit, einschließlich der Bewertung der Reaktionsfähigkeit staatlicher Institutionen bei der Bereitstellung von Rechtsmitteln für Opfer von Spähsoftware, insbesondere für Journalisten, und 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 Verfolgung 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, und

    c) die Ausweitung der Bewertung der Kommission für die Zwecke der Haushaltskonditionalitätsregelung zur Förderung der Rechtsstaatlichkeit, insbesondere durch die Untersuchung der Auswirkungen des Einsatzes von Spähsoftware auf die Rechenschaftspflicht bei öffentlichen Ausgaben;

Prozesskostenfonds der Union

86. fordert die unverzügliche Einrichtung eines Unionsfonds für Rechtsstreitigkeiten, um die tatsächlichen Prozesskosten zu decken und es den Opfern von Spähsoftware zu ermöglichen, im Einklang mit 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 zu erhalten;

Europäischer Rat, Rat der EU und Kommission

87. 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 Union durchzuführen;

88. 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;

89. 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 Europäischen 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;

90. vertritt den Standpunkt, dass das Parlament über umfassende Untersuchungsbefugnisse verfügen sollte, einschließlich der Befugnis, Zeugen vorzuladen, Zeugen förmlich aufzufordern, unter Eid auszusagen, und die angeforderten Informationen innerhalb bestimmter Fristen bereitzustellen;

91. beschließt, 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 den zuständigen Strafverfolgungsbehörden gemeldet werden müssen;

92. 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 Union gestärkt werden, angemessen auf Angriffe von innen auf Demokratie und Rechtsstaatlichkeit zu reagieren und sicherzustellen, dass die Union über wirksame supranationale Methoden zur Durchsetzung der Verträge und des abgeleiteten Rechts im Fall der Nichteinhaltung durch die Mitgliedstaaten verfügt;

Legislative Maßnahmen

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

°

° °

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