Europees Parlement
2019-2024

Zittingsdocument

B9-0260/2023

22.5.2023

ONTWERPAANBEVELING VAN HET EUROPEES PARLEMENT AAN DE RAAD EN DE COMMISSIE

ingediend overeenkomstig artikel 208, lid 12, van het Reglement

naar aanleiding het onderzoek naar vermeende inbreuken op en gevallen van wanbeheer bij het toepassen van het Unierecht met betrekking tot het gebruik van Pegasus en soortgelijke spyware voor surveillance
(2023/2500(RSP))

Sophie in ’t Veld
namens de Enquêtecommissie om het gebruik van Pegasus en soortgelijke spyware voor surveillance te onderzoeken

B9-0260/2023

Aanbeveling van het Europees Parlement aan de Raad en de Commissie naar aanleiding van het onderzoek naar vermeende inbreuken op en gevallen van wanbeheer bij het toepassen van het Unierecht met betrekking tot het gebruik van Pegasus en soortgelijke spyware voor surveillance (2023/2500(RSP))

Het Europees Parlement,

– gezien het Verdrag betreffende de Europese Unie (VEU), en met name de artikelen 2, 4, 6, en 21,

– gezien de artikelen 16, 223, 225 en 226 van het Verdrag betreffende de werking van de Europese Unie (VWEU),

– gezien het Handvest van de grondrechten van de Europese Unie (het Handvest), en met name de artikelen 7, 8, 11, 17, 21, 41, 42 en 47,

– gezien Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (de "richtlijn betreffende privacy en elektronische communicatie")[1] ("e-privacyrichtlijn"),

– gezien Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)[2],

– gezien Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad[3],

– gezien Richtlijn 2013/40/EU van het Europees Parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ[4] van de Raad ("richtlijn cybercriminaliteit"),

– gezien Verordening (EU) 2021/821 van het Europees Parlement en de Raad van 20 mei 2021 tot instelling van een Unieregeling voor controle op de uitvoer, de tussenhandel, de technische bijstand, de doorvoer en de overbrenging van producten voor tweeërlei gebruik[5] (de "verordening inzake producten voor tweeërlei gebruik"),

– gezien Besluit (GBVB) 2019/797 van de Raad van 17 mei 2019 betreffende beperkende

[1] PB L 201 van 31.7.2002, blz. 37.
[2] PB L 119 van 4.5.2016, blz. 1.
[3] PB L 119 van 4.5.2016, blz. 89.
[4] PB L 218 van 14.8.2013, blz. 8.
[5] PB L 206 van 11.6.2021, blz. 1.

maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen[6], zoals gewijzigd bij Besluit (GBVB) 2021/796 van de Raad van 17 mei 2021[7],

– gezien de Akte betreffende de verkiezing van de leden van het Europees Parlement door middel van rechtstreekse algemene verkiezingen[8],

– gezien Besluit 95/167/EG, Euratom, EGKS van het Europees Parlement, de Raad en de Commissie van 6 maart 1995 tot vaststelling van de wijze van uitoefening van het enquêterecht van het Europees Parlement[9],

– gezien Besluit (EU) 2022/480 van het Europees Parlement van 10 maart 2022 over de instelling van een enquêtecommissie om het gebruik van de Pegasus en soortgelijke spyware voor surveillance te onderzoeken, en houdende de vaststelling van het onderwerp van de enquête, alsook van de bevoegdheden, het aantal leden en de duur van het mandaat van de commissie[10],

– gezien Richtlijn (EU) 2018/843 van het Europees Parlement en de Raad van 30 mei 2018 tot wijziging van Richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van de Richtlijnen 2009/139/EG en 2013/36/EU[11] (“antiwitwasrichtlijn”),

– gezien het voorstel van 16 september 2022 voor een verordening van het Europees Parlement en de Raad tot vaststelling van een gemeenschappelijk kader voor mediadiensten op de interne markt (“verordening mediavrijheid”) en tot wijziging van Richtlijn 2010/13/EU (COM(2022)0457),

– gezien artikel 12 van de Universele Verklaring inzake de rechten van de mens,

– gezien het arrest van het Hof van Justitie van de Europese Unie (HvJ-EU) in zaak C-37/20[12] over de antiwitwasrichtlijn, waarin het Hof stelt dat de bepaling dat de lidstaten ervoor moeten zorgen dat informatie over de uiteindelijk begunstigden van binnen hun grondgebied opgerichte vennootschappen en andere juridische entiteiten in alle gevallen voor elk lid van de bevolking toegankelijk moet zijn, ongeldig is,

– gezien artikel 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten,

– gezien het handvest van de Verenigde Naties en de leidende beginselen van de Verenigde Naties inzake bedrijfsleven en mensenrechten[13],

– gezien de verklaring van Michelle Bachelet, Hoge Commissaris van de Verenigde

---

[6] PB L 129 I van 17.5.2019, blz. 13.
[7] PB L 174 I van 18.5.2021, blz. 1.
[8] PB L 278 van 8.10.1976, blz. 5.
[9] PB L 113 van 19.5.1995, blz. 1.
[10] PB L 98 van 25.3.2022, blz. 72.
[11] PB L 156 van 19.6.2018, blz. 43-74.
[12] Arrest van het Hof (Grote kamer) van 22 november 2022, C-37/20, *WM* en *Sovim SA* tegen *Luxembourg Business Registers*, EU:C:2022:912.
[13] https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

Naties voor de mensenrechten, van 19 juli 2022, getiteld “Use of spyware to surveil journalists and human rights defenders”,

– gezien de opmerking van Dunja Mijatovic, commissaris voor de Mensenrechten van de Raad van Europa, van 27 januari 2023, getiteld “Highly intrusive spyware threatens the essence of human rights”[14],

– gezien het document “Preliminary Remarks on Modern Spyware” van de Europese Toezichthouder voor gegevensbescherming (EDPS) van 15 februari 2022[15],

– gezien het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, en met name de artikelen 8, 10, 13, 14 en 17, alsook de protocollen daarbij,

– gezien de dreigingsevaluatie voor zware en georganiseerde criminaliteit (Socta) van Europol van 2021, getiteld “A Corrupting Influence: the Infiltration and Undermining of Europe’s Economy and Society by Organised Crime”,

– gezien het verslag 2017 van het Bureau van de Europese Unie voor de grondrechten (FRA) getiteld “Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU”, en de updates die op 28 februari 2023 zijn voorgelegd aan de Enquêtecommissie om het gebruik van Pegasus en soortgelijke spyware voor surveillance te onderzoeken (PEGA),

– gezien zijn resolutie van 12 maart 2014 over het surveillanceprogramma van de NSA in de VS, toezichthoudende instanties in verschillende lidstaten en gevolgen voor de grondrechten van EU-burgers en voor de trans-Atlantische samenwerking op het gebied van justitie en binnenlandse zaken[16], en met name de aanbevelingen daarin betreffende de versterking van de IT-beveiliging in de instellingen, organen en instanties van de EU,

– gezien advies 24/2022 van de EDPS van 11 november 2022 inzake de EU-verordening mediavrijheid,

– gezien het glossarium betreffende malware en spyware opgesteld door het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa),

– gezien het besluit van de Europese Ombudsman over de wijze waarop de Europese Commissie de gevolgen voor de mensenrechten heeft beoordeeld alvorens Afrikaanse landen steun te verlenen voor de ontwikkeling van bewakingscapaciteiten (zaak 1904/2021/MHZ),

– gezien de verklaring van mevrouw Irene Kahn, speciale rapporteur van de VN voor de bevordering en bescherming van het recht op vrijheid van mening en meningsuiting, en de heer Fernand de Varennes, speciale rapporteur van de VN voor minderhedenkwesties, d.d. 2 februari 2023, waarin zij aandringen op een onderzoek naar het spionageprogramma in het kader waarvan Catalaanse leiders zouden zijn

[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] PB C 378 van 9.11.2017, blz. 104.

bespioneerd[17],

– gezien het verslag van de Europese Commissie voor democratie middels het recht (Commissie van Venetië) over het democratisch toezicht op de veiligheidsdiensten[18] en haar advies getiteld “Poland – Opinion on the Act of 15 January 2016 amending the Police Act and Certain Other Acts”[19],

– gezien het verslag van de Enquêtecommissie om het gebruik van Pegasus en soortgelijke spyware voor surveillance te onderzoeken (A9-0189/2023),

– gezien artikel 208, lid 12, van zijn Reglement,

A. overwegende dat, dankzij de inspanningen van CitizenLab en Amnesty Tech en talrijke onderzoeksjournalisten, is gebleken dat overheidsinstanties in verschillende landen, zowel lidstaten als niet-EU-landen, Pegasus en soortgelijke spyware voor surveillance hebben gebruikt tegen journalisten, politici, rechtshandhavingsfunctionarissen, diplomaten, advocaten, zakenlieden, actoren uit het maatschappelijk middenveld en andere actoren, voor politieke en zelfs criminele doeleinden; overwegende dat dergelijke praktijken uiterst alarmerend zijn en het risico aantonen van misbruik van surveillancetechnologieën met als doel de fundamentele mensenrechten, de democratie en verkiezingsprocessen te ondermijnen;

B. overwegende dat wanneer in het verslag de term “spyware” wordt gebruikt, daarmee “Pegasus en soortgelijke spyware voor surveillance” wordt bedoeld, zoals gedefinieerd in het besluit van het Parlement tot instelling van de commissie PEGA;

C. overwegende dat is vastgesteld dat overheidsactoren zich schuldig hebben gemaakt aan misleiding en dit met opzet hebben gedaan, in die zin dat zij gebruik hebben gemaakt van spyware die eruit ziet als een gewoon programma of bestand of als gewone inhoud (“Trojaans paard”), bijvoorbeeld nepberichten van overheidsinstanties; overwegende dat het ook is voorgekomen dat overheidsinstanties gebruikmaakten van telefoonexploitanten om schadelijke inhoud door te geven aan apparaten van personen; overwegende dat spyware kan worden ingezet door gebruik te maken van “zero-day”-beveiligingslekken zonder dat er sprake is van interactie van het doelwit met besmette inhoud, dat alle sporen van de aanwezigheid van de spyware na uitschakeling ervan gewist kunnen worden, en dat de koppeling tussen de operators op afstand en de server onzichtbaar kan worden;

D. overwegende dat het afluisteren van telefoongesprekken in de begindagen van mobiele communicatie plaatsvond door middel van het onderscheppen van oproepen en later van tekstberichten in de vorm van platte tekst;

E. overwegende dat de opkomst van versleutelde mobiele communicatietoepassingen heeft geleid tot de opkomst van de spyware-industrie, waarbij de bestaande kwetsbaarheden in besturingssystemen van smartphones worden gebruikt om software te installeren 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

spyware in de telefoon importeert, onder meer door middel van klikvrije infecties zonder medeweten van of enige actie door de gebruiker, waardoor gegevens kunnen worden geëxtraheerd voordat ze worden versleuteld; overwegende dat het vanwege het ontwerp van dergelijke “zero-click”-spyware uiterst moeilijk is om daadwerkelijk en doeltreffend toezicht te houden op het gebruik ervan;

F. overwegende dat kennis over kwetsbaarheden in softwaresystemen rechtstreeks tussen partijen of via makelaars wordt verhandeld; overwegende dat niet-overheidsactoren en criminele organisaties zich bezighouden met deze handel;

G. overwegende dat de handel in en het verzamelen van “zero-day”-kwetsbaarheden de integriteit en veiligheid van de communicatie en de cyberveiligheid van EU-burgers fundamenteel ondermijnen;

H. overwegende dat spyware de uitzondering moet blijven en altijd een doeltreffende, bindende en zinvolle voorafgaande rechterlijke toestemming van een onpartijdige en onafhankelijke rechterlijke instantie vergt, die ervoor moet zorgen dat de maatregel noodzakelijk en evenredig is en strikt beperkt blijft tot gevallen die verband houden met de nationale veiligheid, of waarbij terrorisme en zware criminaliteit betrokken zijn; overwegende dat surveillancetechnieken gemakkelijk kunnen worden misbruikt in omgevingen waar geen doeltreffende controlemechanismen zijn;

I. overwegende dat elke surveillanceactiviteit door middel van spyware achteraf moet worden getoetst door een onafhankelijke toezichthoudende autoriteit, die ervoor moet zorgen dat elke toegestane surveillanceactiviteit wordt uitgevoerd met inachtneming van de grondrechten en in overeenstemming met de voorwaarden die zijn vastgesteld door het HvJ-EU, het Europees Hof voor de Rechten van de Mens (EHRM) en de Commissie van Venetië; overwegende dat deze toezichthoudende autoriteit die achteraf toetst, onmiddellijk de beëindiging van de surveillance dient te gelasten wanneer wordt vastgesteld dat deze onverenigbaar is met bovengenoemde rechten en voorwaarden;

J. overwegende dat spyware voor surveillance die niet voldoet aan de vereisten van het Unierecht en de jurisprudentie van het HvJ-EU en het EHRM, in strijd is met de waarden die zijn verankerd in artikel 2 VEU en de grondrechten van het Handvest, met name die van de artikelen 7, 8, 11, 17, 21 en 47, waarin specifieke rechten, vrijheden en beginselen worden erkend, zoals de eerbiediging van het privéleven en het familie- en gezinsleven, de bescherming van persoonsgegevens, de vrijheid van meningsuiting en van informatie, het recht op eigendom, het recht op non-discriminatie, alsook het recht op een doeltreffende voorziening in rechte, een onpartijdig gerecht en het vermoeden van onschuld;

K. overwegende dat de rechten van de betrokken personen zijn vastgelegd in het Handvest en in internationale verdragen, met name het recht op privacy en het recht op een onpartijdig gerecht, alsmede in de EU-voorschriften inzake de rechten van verdachten en beklaagden; overwegende dat deze rechten zijn bevestigd in de jurisprudentie van het HvJ-EU en het EHRM;

L. overwegende dat de gevolgen van gerichte surveillance voor vrouwen bijzonder ernstig kunnen zijn, aangezien de autoriteiten de toegenomen sociale controle waar vrouwen mee te maken hebben, kunnen gebruiken om via spyware verkregen privé- en intieme

gegevens in te zetten in het kader van lastercampagnes;

M. overwegende dat uit de getuigenissen van de personen die doelwit zijn, blijkt dat er op papier weliswaar rechtsmiddelen en burgerrechten bestaan, deze meestal van nul en generlei waarde zijn als gevolg van obstructie door overheidsinstanties, het ontbreken of niet eerbiedigen van het recht van personen die doelwit zijn om te worden geïnformeerd en de administratieve belemmering van personen die moeten bewijzen dat zij doelwit zijn geweest; overwegende dat het zelfs in systemen met snelle en open procedures vanwege het karakter van spyware zeer moeilijk is om het daderschap en de aard van en de mate waarin een persoon doelwit is geweest, aan te tonen;

N. overwegende dat rechtbanken geen forensisch bewijs van onafhankelijke deskundigen hebben aanvaard, maar alleen bewijs dat gebaseerd is op onderzoek van de autoriteiten, de veiligheid of de wetshandhaving die achter een aanval zouden zitten; overwegende dat doelwitten daardoor in een paradoxale situatie terechtkomen en niet kunnen aantonen dat zij het slachtoffer zijn van spyware;

O. overwegende dat de Poolse regering institutionele en juridische waarborgen, met inbegrip van adequate toezicht- en controleprocedures, heeft afgezwakt en afgeschaft, waardoor personen die het doelwit zijn geworden van spyware in feite niet meer beschikken over zinvolle rechtsmiddelen; overwegende dat Pegasus-surveillancespyware illegaal voor politieke doeleinden is ingezet om journalisten, politici van de oppositie, advocaten, openbaar aanklagers en actoren uit het maatschappelijk middenveld te bespioneren;

P. overwegende dat de Hongaarse regering institutionele en juridische waarborgen, met inbegrip van adequate toezicht- en controleprocedures, heeft afgezwakt en afgeschaft, waardoor personen die het doelwit zijn geworden van spyware in feite niet meer beschikken over zinvolle rechtsmiddelen; overwegende dat de Pegasus-surveillancespyware illegaal voor politieke doeleinden is ingezet om journalisten, politici van de oppositie, advocaten, openbaar aanklagers en actoren uit het maatschappelijk middenveld te bespioneren;

Q. overwegende dat officieel is bevestigd dat een lid van het Europees Parlement voor Griekenland en een Griekse journalist zijn afgeluisterd door de Griekse nationale inlichtingendienst (EYP) en dat zij het doelwit waren van Predator-spyware; overwegende dat een voormalige Amerikaans-Griekse werknemer bij Meta tegelijkertijd door het EYP werd afgeluisterd en het doelwit was van Predator-spyware, waarvan het gebruik volgens de Griekse wet illegaal is; overwegende dat volgens berichten in de media parlementsleden van oppositie- en regeringspartijen in Griekenland, partijactivisten en journalisten ook het doelwit zouden zijn geweest van Predator-spyware of conventionele afluisterapparatuur van het EYP of van beide; overwegende dat de Griekse regering ontkent dat zij Predator heeft gekocht of gebruikt, maar dat het zeer waarschijnlijk is dat Predator is ingezet door of namens personen die zeer dicht bij het kabinet van de premier staan; overwegende dat de Griekse regering heeft erkend dat zij aan Intellexa uitvoervergunningen heeft verleend voor de verkoop van de Predator-spyware aan repressieve regeringen, zoals Madagaskar en Sudan; overwegende dat de regering op het schandaal heeft gereageerd met wetswijzigingen die de rechten van doelwitten om te worden geïnformeerd nadat surveillance heeft

plaatsgevonden, nog verder inperken en die de werkzaamheden van onafhankelijke autoriteiten nog verder belemmeren;

R. overwegende dat aan de hand van onthullingen is vastgesteld dat spyware in Spanje tegen twee groepen doelwitten is ingezet; overwegende dat de eerste groep de premier en de minister van Defensie, de minister van Binnenlandse Zaken en andere hoge ambtenaren omvat; overwegende dat de tweede groep deel uitmaakt van wat door de organisatie CitizenLab ”CatalanGate“ wordt genoemd, en 65 doelwitten omvat, waaronder politieke figuren van de regionale regering van Catalonië, leden van de pro-Catalaanse onafhankelijkheidsbeweging, leden van het Europees Parlement, advocaten, academici en actoren uit het maatschappelijk middenveld; overwegende dat de Spaanse autoriteiten in mei 2022 toegaven 18 personen als doelwit te hebben genomen met toestemming van de rechter, hoewel zij tot dusverre de bevelschriften of andere informatie niet openbaar hebben gemaakt, waarbij zij zich op de nationale veiligheid beriepen om het gebruik van spyware voor surveillance in Spanje te rechtvaardigen; overwegende dat 47 andere personen ook doelwit zouden zijn geweest, maar geen andere informatie hebben ontvangen dan van CitizenLab;

S. overwegende dat er op Cyprus geen vermeende spyware-infecties zijn bevestigd; overwegende dat Cyprus een belangrijk Europees exportknooppunt is voor de surveillancesector en een aantrekkelijke locatie voor bedrijven die surveillancetechnologieën verkopen;

T. overwegende dat er sterke aanwijzingen zijn dat de regeringen van onder meer Marokko en Rwanda hooggeplaatste burgers van de Unie met spyware hebben bestookt, onder wie de president van Frankrijk, de premier, de minister van Defensie en de minister van Binnenlandse Zaken van Spanje, de voormalige premier van België, de voormalige voorzitter van de Commissie en de voormalige premier van Italië, en Carine Kanimba, de dochter van Paul Rusesabagina;

U. overwegende dat veilig kan worden aangenomen dat alle lidstaten een of meer spywaresystemen hebben gekocht of ingezet; overwegende dat de meeste regeringen in de Europese Unie zullen afzien van onrechtmatig gebruik van spyware, maar dat het risico op misbruik door het ontbreken van een solide rechtskader met waarborgen en toezicht en omdat het technisch ingewikkeld is om infecties op te sporen en de activiteiten van degenen die misbruik maken te volgen, zeer plausibel is;

V. overwegende dat de meeste regeringen en parlementen van de lidstaten het Europees Parlement geen betekenisvolle informatie hebben verstrekt over hun rechtskaders voor het gebruik van spyware die verder gaat dan wat reeds algemeen bekend was, ondanks een verplichting daartoe uit hoofde van artikel 3, lid 4, van het besluit van het Europees Parlement, de Raad en de Commissie van 6 maart 1995 tot vaststelling van de wijze van uitoefening van het enquêterecht van het Europees Parlement; overwegende dat het moeilijk is om de handhaving van de Uniewetgeving en de waarborgen, het toezicht en de rechtsmiddelen te beoordelen, hetgeen een adequate bescherming van de grondrechten van burgers in de weg staat;

W. overwegende dat in artikel 4, lid 3, VEU het volgende wordt bepaald: “krachtens het beginsel van loyale samenwerking respecteren de Unie en de lidstaten elkaar en steunen

zij elkaar bij de vervulling van de taken die uit de Verdragen voortvloeien”;

X. overwegende dat verschillende sleutelfiguren uit de spyware-industrie de Maltese nationaliteit hebben verworven, waardoor zij gemakkelijker activiteiten kunnen ontplooien in en vanuit de Unie;

Y. overwegende dat veel spyware-ontwikkelaars en -verkopers in een of meer lidstaten ingeschreven staan of worden ingeschreven; overwegende dat NSO Group bijvoorbeeld aanwezig is in Luxemburg, Cyprus, Nederland en Bulgarije; de moedermaatschappij van Intellexa, Thalestris Limited, in Ierland, Griekenland, Zwitserland en Cyprus; DSIRF in Oostenrijk; Amesys en Nexa Technologies in Frankrijk; Tykelab en RCS Lab in Italië, en FinFisher (inmiddels ter ziele) in Duitsland;

Z. overwegende dat de Europese Unie geen partij is in de Overeenkomst van Wassenaar betreffende exportcontrole voor conventionele wapens en goederen en technologieën voor tweeërlei gebruik; overwegende dat alle lidstaten behalve Cyprus deelnemen aan de Overeenkomst van Wassenaar, hoewel Cyprus lang geleden een verzoek heeft ingediend om toe te treden tot de Overeenkomst van Wassenaar; overwegende dat Cyprus gebonden is aan de verordening inzake producten voor tweeërlei gebruik;

AA. overwegende dat de Israëlische uitvoerregeling[20] in beginsel van toepassing is op alle Israëlische burgers, zelfs wanneer zij vanuit de EU opereren; overwegende dat Israël niet deelneemt aan de Overeenkomst van Wassenaar, maar niettemin beweert dat het de normen ervan toepast;

AB. overwegende dat de uitvoer van spyware uit de Unie naar niet-EU-landen is geregeld in de verordening inzake producten voor tweeërlei gebruik, die in 2021 is herzien; overwegende dat de Commissie in september 2022 een eerste uitvoeringsverslag heeft gepubliceerd[21];

AC. overwegende dat sommige producenten van spyware die producten naar derde landen uitvoeren, zich in de Unie vestigen om een respectabel imago te verkrijgen terwijl ze handelen in spyware met repressieve regimes; overwegende dat er vanuit de Unie producten worden uitgevoerd naar repressieve regimes of niet-statelijke actoren, hetgeen in strijd is met de EU-uitvoerregels;

AD. overwegende dat Amesys en Nexa Technologies momenteel in Frankrijk worden vervolgd voor de uitvoer van surveillancetechnologie naar Libië, Egypte en Saudi-Arabië; overwegende dat in Griekenland gevestigde Intellexa-bedrijven naar verluidt hun producten hebben uitgevoerd naar Bangladesh, Sudan, Madagaskar en ten minste één Arabisch land; overwegende dat de software van FinFisher wordt gebruikt door tientallen landen over de hele wereld, waaronder de inlichtingendiensten van Angola, Bahrein, Bangladesh, Egypte, Ethiopië, Gabon, Jordanië, Kazachstan, Myanmar, Oman, Qatar, Saudi-Arabië, Turkije en Marokko, welke door Amnesty International en Forbidden Stories zijn beschuldigd van het gebruik van Pegasus-spyware tegen journalisten, mensenrechtenactivisten, maatschappelijke organisaties en politici; overwegende dat niet bekend is of uitvoervergunningen zijn afgegeven voor de uitvoer

[20] Wet inzake de controle op de uitvoer van defensiematerieel 5766-2007, Israëlisch Ministerie van Defensie.
[21] https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=COM%3A2022%3A434%3AFIN&qid=1662029750223

van spyware naar al deze landen;

AE. overwegende dat uit het aantal deelnemers aan wapenbeurzen en ISSWorld die spywaregerelateerde diensten op de markt brachten, blijkt dat de meeste aanbieders van spyware en aanverwante producten en diensten uit derde landen komen en dat een aanzienlijk aantal van hen in Israël gevestigd is (bijv. NSO Group, Wintego, Quadream en Cellebrite), dat er prominente producenten in India (ClearTrail), het Verenigd Koninkrijk (BAe Systems en Black Cube) en de Verenigde Arabische Emiraten (DarkMatter) zijn en dat ook uit de Amerikaanse "Entity List" van bedrijven waarop handelsbeperkingen van toepassing zijn en waarop spywareproducten uit Israël (NSO Group en Candiru), Rusland (Positive Technologies) en Singapore (Computer Security Initiative Consultancy PTE LTD.) staan, eens te meer blijkt dat spywareproducenten uit allerlei verschillende landen komen; overwegende dat de beurs ook wordt bezocht door een breed scala aan Europese overheidsinstanties, waaronder lokale politiediensten;

AF. overwegende dat in artikel 4, lid 2, VEU is bepaald dat de nationale veiligheid de exclusieve verantwoordelijkheid van elke lidstaat blijft;

AG. overwegende dat het HvJ-EU echter heeft geoordeeld (zaak C-623/17) dat "het immers weliswaar aan de lidstaten [is] om hun wezenlijke veiligheidsbelangen te definiëren en om passende maatregelen te nemen teneinde hun binnenlandse en buitenlandse veiligheid te verzekeren, maar het enkele feit dat een nationale maatregel is genomen met het oog op de bescherming van de nationale veiligheid, niet ertoe [kan] leiden dat het Unierecht niet van toepassing is en dat de lidstaten worden ontheven van de verplichting om dit recht te eerbiedigen";

AH. overwegende dat het HvJ-EU als volgt heeft geoordeeld (zaak C-203/15): "Artikel 15, lid 1, van richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), zoals gewijzigd bij richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009, gelezen tegen de achtergrond van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, moet in die zin worden uitgelegd dat het zich verzet tegen een nationale regeling die, ter bestrijding van criminaliteit, voorziet in algemene en ongedifferentieerde bewaring van alle verkeersgegevens en locatiegegevens van alle abonnees en geregistreerde gebruikers betreffende alle elektronischecommunicatiemiddelen";

AI. overwegende dat het HvJ-EU als volgt heeft geoordeeld (zaak C-203/15): "Artikel 15, lid 1, van richtlijn 2002/58, zoals gewijzigd bij richtlijn 2009/136, gelezen tegen de achtergrond van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, moet in die zin worden uitgelegd dat het zich verzet tegen een nationale regeling die de bescherming en de beveiliging van de verkeersgegevens en de locatiegegevens en in het bijzonder de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens regelt zonder, in het kader van de bestrijding van criminaliteit, te bepalen dat die toegang alleen wordt verleend ter bestrijding van ernstige criminaliteit, dat die toegang aan een voorafgaand toezicht door een rechterlijke instantie of een onafhankelijke bestuurlijke autoriteit is onderworpen, en dat de betrokken gegevens op het grondgebied

van de Unie moeten worden bewaard";

AJ. overwegende dat uit de jurisprudentie van het EHRM duidelijk blijkt dat surveillance altijd in overeenstemming met de wet moet zijn, een legitiem doel moet nastreven en noodzakelijk en evenredig moet zijn; overwegende dat het rechtskader bovendien moet voorzien in gedetailleerde, doeltreffende en omvattende waarborgen met betrekking tot het gelasten en uitvoeren van en het eventueel aanwenden van rechtsmiddelen tegen surveillancemaatregelen, die onderworpen moeten zijn aan adequate rechterlijke toetsing en effectief toezicht[22];

AK. overwegende dat het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (Verdrag 108) van de Raad van Europa, dat onlangs is geactualiseerd in Verdrag 108+, van toepassing is op de verwerking van persoonsgegevens voor (nationale) veiligheidsdoeleinden van de staat, met inbegrip van defensie; overwegende dat alle lidstaten partij zijn bij dit verdrag;

AL. overwegende dat belangrijke aspecten van het gebruik van spyware voor surveillance met het oog op het voorkomen, onderzoeken, opsporen of vervolgen van strafbare feiten en de uitvoering van straffen, met inbegrip van de bescherming tegen en de preventie van bedreigingen, onder het EU-recht vallen;

AM. overwegende dat in het Handvest wordt bepaald welke beperking wordt gesteld aan de uitoefening van grondrechten door te eisen dat deze beperking bij wet wordt voorgeschreven, de wezenlijke inhoud van de desbetreffende rechten en vrijheden eerbiedigt, onderworpen is aan het evenredigheidsbeginsel en alleen wordt opgelegd als dit noodzakelijk is en daadwerkelijk beantwoordt aan door de Unie erkende doelstellingen van algemeen belang of de noodzaak om de rechten en vrijheden van anderen te beschermen; overwegende dat wanneer spyware wordt gebruikt, de mate van inmenging in het recht op privacy zo ernstig kan zijn dat de persoon er feitelijk van wordt beroofd en dat het gebruik niet altijd als evenredig kan worden beschouwd, ongeacht of de maatregel als noodzakelijk kan worden beschouwd om de legitieme doelstellingen van een democratische staat te verwezenlijken;

AN. overwegende dat de e-privacyrichtlijn bepaalt dat de lidstaten de vertrouwelijkheid van communicatie moeten waarborgen; overwegende dat de inzet van surveillance-instrumenten een beperking is van het door de e-privacyrichtlijn gewaarborgde recht op bescherming van randapparatuur; overwegende dat de nationale wetgeving inzake spyware door dergelijke beperkingen onder het toepassingsgebied van de e-privacyrichtlijn vallen, vergelijkbaar met de nationale wetgevingen inzake gegevensbewaring; overwegende dat de frequente inzet van ingrijpende spywaretechnologie niet verenigbaar zou zijn met de rechtsorde van de Unie;

AO. overwegende dat een staat uit hoofde van het internationaal recht alleen het recht heeft om mogelijke misdrijven binnen zijn jurisdictie te onderzoeken en een beroep moet doen op andere staten ingeval het onderzoek in andere staten moet worden uitgevoerd, tenzij het onderzoek in andere rechtsgebieden kan worden uitgevoerd op grond van een internationale overeenkomst of, in het geval van lidstaten, het recht van de Unie;

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

AP. overwegende dat de infectie van een apparaat met spyware en de daaropvolgende verzameling van gegevens plaatsvindt via de servers van mobiele dienstverleners; overwegende dat, aangezien gratis roaming binnen de Unie ertoe heeft geleid dat personen soms mobiele contracten hebben uit andere lidstaten dan die waar zij wonen, er momenteel in het Unierecht geen rechtsgrondslag is voor het verzamelen van gegevens in de andere lidstaat door middel van spyware;

AQ. overwegende dat David Kaye, de voormalige speciale rapporteur van de VN voor de bevordering en bescherming van het recht op vrijheid van mening en meningsuiting[23] en Irene Khan, de huidige speciale VN-rapporteur voor de bevordering en bescherming van het recht op vrijheid van mening en meningsuiting[24], hebben opgeroepen tot een onmiddellijk moratorium op het gebruik, de overdracht en de verkoop van surveillance-instrumenten totdat strenge mensenrechtenwaarborgen zijn ingevoerd om praktijken te reguleren en te waarborgen dat regeringen en niet-statelijke actoren deze instrumenten op legitieme wijze gebruiken;

AR. overwegende dat er gevallen zijn waarin spywarebedrijven, in het bijzonder Intellexa, niet alleen de onderscheppings- en extractietechnologie zelf hebben verkocht, maar ook de volledige dienst, ook wel "hacking als dienst" of "actieve cyberintelligentie" genoemd, waarbij een pakket van surveillance- en onderscheppingstechnieken wordt aangeboden, alsmede opleiding voor het personeel en technische, operationele en methodologische ondersteuning; overwegende dat deze dienst het bedrijf in staat zou kunnen stellen de gehele surveillanceoperatie te controleren en de surveillancegegevens te aggregeren; overwegende dat deze praktijk voor de bevoegde autoriteiten bijna onmogelijk te overzien en te controleren is; overwegende dat dit het moeilijk maakt de beginselen van evenredigheid, noodzakelijkheid, legitimiteit, wettigheid en adequaatheid in acht te nemen; overwegende dat deze dienst niet is toegestaan door het defensie-exportagentschap (DECA) van Israël; overwegende dat Cyprus is gebruikt om de bestaande beperkingen van de Israëlische wet te omzeilen teneinde "hacking als dienst" aan te bieden;

AS. overwegende dat de lidstaten moeten voldoen aan Richtlijn 2014/24/EU en Richtlijn 2009/81/EG betreffende overheidsopdrachten, respectievelijk overheidsopdrachten op defensiegebied; overwegende dat zij afwijkingen uit hoofde van artikel 346, lid 1, punt b), VWEU naar behoren moeten rechtvaardigen, aangezien Richtlijn 2009/81/EG uitdrukkelijk rekening houdt met de gevoelige kenmerken van overheidsopdrachten op defensiegebied, en dat zij de Overeenkomst inzake overheidsopdrachten van de WTO, zoals gewijzigd op 30 maart 2012[25] moeten naleven, indien zij partij zijn bij die overeenkomst;

AT. overwegende dat de Europese Toezichthouder voor gegevensbescherming heeft benadrukt dat de lidstaten het Europees Verdrag tot bescherming van de rechten van de mens en de jurisprudentie van het EHRM, waarin grenzen worden gesteld aan surveillanceactiviteiten met het oog op de nationale veiligheid, moeten eerbiedigen; en

[23] "Surveillance and human rights", rapport van de speciale rapporteur van de VN voor de bevordering en bescherming van het recht op vrijheid van mening en meningsuiting, A/HRC/41/35, 2019.
[24] Bureau van de Hoge Commissaris van de VN voor de mensenrechten, "Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech".
[25] https://www.wto.org/english/tratop_e/gproc_e/gpa_1994_e.htm

overwegende dat surveillance, wanneer het plaatsvindt in het kader van de rechtshandhaving, in overeenstemming moet zijn met het EU-recht en met name met het Handvest en de richtlijnen van de EU op dit gebied, zoals de e-privacyrichtlijn en de richtlijn gegevensbescherming bij rechtshandhaving;

AU. overwegende dat naar verluidt grote financiële instellingen geprobeerd hebben producenten van spyware ervan te weerhouden passende mensenrechtennormen en zorgvuldigheidseisen toe te passen en hebben aangespoord spyware te blijven verkopen aan repressieve regimes;

AV. overwegende dat Israël in het Horizon 2020-programma de derde plaats inneemt onder de geassocieerde landen voor de totale deelname aan het programma; overwegende dat de Horizon Europa-overeenkomst met Israël voor 2021-2027 een totale begroting heeft van 95,5 miljard EUR[26]; overwegende dat via deze Europese programma's middelen ter beschikking zijn gesteld van Israëlische militaire en beveiligingsondernemingen[27];

AW. overwegende dat het belangrijkste wetgevingsinstrument voor het ontwikkelingsbeleid van de Unie Verordening (EU) 2021/947[28] ("Europa in de wereld"-verordening) is en de financiering van de Unie kan worden verstrekt via de soorten financiering waarin het Financieel Reglement voorziet; overwegende dat de bijstand kan worden opgeschort in geval van verslechtering van de democratie, de mensenrechten of de rechtsstaat in derde landen;

1. benadrukt het onmiskenbare belang van de bescherming van de persoonlijke levenssfeer, het recht op waardigheid, privé- en gezinsleven, vrijheid van meningsuiting en van informatie, vrijheid van vergadering en vereniging, en het recht op een eerlijk proces, met name in een steeds digitalere wereld waarin een groeiend aantal van onze activiteiten online plaatsvindt;

2. is sterk van mening dat inbreuken op deze grondrechten en fundamentele vrijheden van essentieel belang zijn voor de eerbiediging van de gemeenschappelijke rechtsbeginselen die in de Verdragen en in andere bronnen zijn vastgelegd, en merkt op dat de democratie zelf op het spel staat, aangezien het gebruik van spyware op politici, maatschappelijke organisaties en journalisten een remmend effect heeft en het recht op vreedzame vergadering, de vrijheid van meningsuiting en de inspraak van het publiek ernstig aantast;

3. veroordeelt ten stelligste het gebruik van spyware door regeringen van lidstaten en leden van regeringsinstanties of staatsinstellingen met het oog op het controleren, chanteren, intimideren, manipuleren en in diskrediet brengen van leden van de oppositie, critici en het maatschappelijk middenveld, het uitschakelen van

---

[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_en

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

[28] Verordening (EU) 2021/947 van het Europees Parlement en de Raad van 9 juni 2021 tot vaststelling van het instrument voor nabuurschapsbeleid, ontwikkeling en internationale samenwerking – Europa in de wereld, tot wijziging en intrekking van Besluit nr. 466/2014/EU van het Europees Parlement en de Raad en tot intrekking van Verordening (EU) 2017/1601 van het Europees Parlement en de Raad en Verordening (EG, Euratom) nr. 480/2009 van de Raad, PB L 209 van 14.6.2021.

democratische controle en persvrijheid, het manipuleren van verkiezingen en het ondermijnen van de rechtsstaat door rechters, aanklagers en advocaten voor politieke doeleinden als doelwit te nemen;

4. wijst erop dat dit onrechtmatige gebruik van spyware door nationale regeringen en regeringen van niet-EU-landen directe en indirecte gevolgen heeft voor de instellingen van de Unie en het besluitvormingsproces, waardoor de integriteit van de democratie van de Europese Unie wordt ondermijnd;

5. stelt met grote bezorgdheid vast dat de huidige bestuursstructuur van de Unie fundamenteel ontoereikend is om te reageren op aanvallen op de democratie, grondrechten en de rechtsstaat van binnen de Unie, en dat veel lidstaten te weinig maatregelen nemen; stelt vast dat wanneer zij in één lidstaat worden bedreigd, de gehele Unie in gevaar komt;

6. benadrukt dat digitale normen voor technologische ontwikkelingen in de Unie de grondrechten in acht moeten nemen;

7. is er stellig van overtuigd dat de uitvoer van spyware uit de Unie naar dictaturen en repressieve regimes met een slechte staat van dienst op het gebied van mensenrechten, waar dergelijke instrumenten worden gebruikt tegen mensenrechtenactivisten, journalisten en critici van de regering, een ernstige schending van de in het Handvest verankerde grondrechten vormt en een grove schending van de uitvoerregels van de Unie;

8. uit voorts zijn bezorgdheid over het onrechtmatige gebruik van en de illegale handel in spyware door de lidstaten, die samen de Unie tot een bestemming voor de spyware-industrie maken;

9. uit zijn bezorgdheid over het feit dat prominente personen, mensenrechtenactivisten en journalisten in de Unie door niet-EU-landen met spyware worden aangevallen;

10. is evenzeer bezorgd over de duidelijke terughoudendheid om misbruik van spyware te onderzoeken, zowel in gevallen waarin de verdachte een overheidsinstantie van een lidstaat of een niet-EU-land is; wijst op de zeer trage vooruitgang en het gebrek aan transparantie in het gerechtelijk onderzoek naar spywaremisbruik jegens regeringsleiders en ministers van EU-lidstaten en de Commissie, evenals jegens leden van het maatschappelijk middenveld, journalisten of politieke tegenstanders;

11. merkt op dat het rechtskader van sommige lidstaten niet voorziet in nauwkeurige, doeltreffende en alomvattende waarborgen voor het ordonneren en uitvoeren van en de mogelijke verhaalmechanismen tegen surveillancemaatregelen; merkt op dat dergelijke maatregelen een legitiem doel moeten dienen en noodzakelijk en evenredig moeten zijn;

12. betreurt het dat de regeringen van de lidstaten, de Raad en de Commissie niet volledig met het onderzoek hebben meegewerkt en niet alle relevante en betekenisvolle informatie hebben gedeeld om de Enquêtecommissie te helpen haar taken te vervullen, zoals in haar mandaat staat; erkent dat een deel van deze informatie onderworpen kan zijn aan strikte wettelijke voorschriften inzake geheimhouding en vertrouwelijkheid; is van mening dat het collectieve antwoord van de Raad volstrekt ontoereikend is en in

strijd is met het beginsel van loyale samenwerking zoals vastgelegd in artikel 4, lid 3, VEU;

13. concludeert dat noch de lidstaten, noch de Raad, noch de Commissie er ook maar enig belang in leken te stellen om hun inspanningen om het misbruik van spyware volledig te onderzoeken, te maximaliseren en aldus willens en wetens regeringen van de Unie te beschermen die de mensenrechten binnen en buiten de Unie schenden;

14. concludeert dat er in Polen sprake is geweest van grove inbreuken en wanbeheer bij de uitvoering van het recht van de Unie;

15. verzoekt Polen om:

a) er bij de procureur-generaal op aan te dringen een onderzoek in te stellen naar het misbruik van spyware;

b) dringend voldoende institutionele en juridische waarborgen te herstellen, met inbegrip van doeltreffende, bindende controles vooraf en achteraf, alsmede onafhankelijke toezichtmechanismen, onder meer gerechtelijke toetsing van surveillanceactiviteiten; benadrukt dat in het kader van een doeltreffende controle vooraf het verzoek aan de rechter om operationele surveillance, alsook het rechterlijk bevel tot die surveillance, een duidelijke rechtvaardiging en vermelding van de voor de surveillance te gebruiken technische middelen moeten bevatten, en dat in het kader van een doeltreffende controle achteraf een verplichting moet worden vastgesteld om de aan de surveillance onderworpen persoon in te lichten over het feit, de duur, de omvang en de wijze van verwerking van de tijdens de operationele surveillance verkregen gegevens;

c) coherente wetgeving in te voeren om burgers te beschermen, ongeacht het feit of het operationele toezicht wordt verricht door het openbaar ministerie, de geheime diensten of andere overheidsinstanties;

d) de uitspraak van het Constitutioneel Hof over de politiewet van 1990 na te leven;

e) te voldoen aan het advies van de Commissie van Venetië over de politiewet van 2016;

f) te voldoen aan de verschillende arresten van het EHRM, zoals het arrest in de zaak *Roman Zakharov*/*Rusland* in 2015, waarin de noodzaak wordt onderstreept van strikte surveillancecriteria, behoorlijke rechterlijke toestemming en rechterlijk toezicht, de onmiddellijke vernietiging van irrelevante gegevens, rechterlijke toetsing van spoedprocedures en de verplichting om de betrokken personen te informeren, alsook de uitspraak in de zaak *Klass e.a.*/*Duitsland* uit 1978, waarin wordt gesteld dat de surveillance van voldoende belang moet zijn om een dergelijke inbreuk op de privacy noodzakelijk te maken;

g) te voldoen aan alle uitspraken van het HvJ-EU en het EHRM met betrekking tot de onafhankelijkheid van de rechterlijke macht en de voorrang van het EU-recht;

h) artikel 168 bis van de herschreven Wet tot wijziging van het Wetboek van Strafvordering van 2016 in te trekken;

i) de volledige onafhankelijkheid van de rechterlijke macht te herstellen en de statutaire bevoegdheden van alle relevante toezichthoudende instanties te eerbiedigen, zoals de Ombudsman, de president van het Bureau voor de bescherming van persoonsgegevens en de Hoge Rekenkamer, om ervoor te zorgen dat alle toezichthoudende instanties volledige medewerking en toegang tot informatie krijgen, en om alle personen die doelwit zijn volledige informatie te verstrekken;

j) met spoed te zorgen voor de willekeurige toewijzing van zaken aan de rechters van de rechtbanken voor elk verzoek dat wordt ingediend, zelfs tijdens het weekend en buiten de normale kantooruren, om te voorkomen dat de geheime diensten "bevriende rechters" selecteren, en om de transparantie van een dergelijk systeem te waarborgen, onder meer door het algoritme op basis waarvan een zaak willekeurig aan een rechter wordt toegewezen openbaar te maken;

k) het traditionele systeem van parlementair toezicht te herstellen, waarbij de oppositiepartij het voorzitterschap van de parlementaire commissie voor bijzondere diensten (KSS) op zich neemt;

l) dringend duidelijkheid te verschaffen over de situatie rond het misbruik van spyware in Polen, zodat de integriteit van de komende verkiezingen geenszins in twijfel kan worden getrokken;

m) Richtlijn (EU) 2016/680 (de richtlijn wetshandhaving) naar behoren uit te voeren en te handhaven, en ervoor te zorgen dat de gegevensbeschermingsautoriteit de bevoegdheid heeft om toezicht te houden op de verwerking van persoonsgegevens door onder meer autoriteiten als het centrale corruptiebestrijdingsbureau en het bureau voor interne veiligheid;

n) de klokkenluidersrichtlijn om te zetten;

o) geen bepalingen in nieuwe wetten inzake elektronische communicatie aan te nemen die in strijd zijn met het Europees Verdrag voor de rechten van de mens (EVRM);

p) de beschikbaarheid van doeltreffende rechtsmiddelen te waarborgen voor Poolse burgers die nadelen ondervinden van de uitvoering van wetten die in strijd zijn met de Poolse grondwet en het EVRM;

q) Europol te vragen alle gevallen van vermeend misbruik van spyware te onderzoeken;

r) de onafhankelijke grondwettelijke toetsing van de wetten in Polen te waarborgen;

s) de onafhankelijkheid van de rol van de procureur-generaal ten opzichte van de minister van Justitie te herstellen om te waarborgen dat onderzoeken naar vermeende schendingen van de grondrechten vrij zijn van politieke overwegingen;

16. dringt er bij de Commissie op aan de verenigbaarheid van de Poolse wet van 2018 inzake de bescherming van persoonsgegevens die worden verwerkt in het kader van de voorkoming en bestrijding van criminaliteit, met de EU-richtlijn inzake wetshandhaving te beoordelen en, indien nodig, een inbreukprocedure in te leiden;

17. concludeert dat er in Hongarije sprake is geweest van grove inbreuken en wanbeheer bij de uitvoering van het recht van de Unie;

18. verzoekt Hongarije om:

a) dringend voldoende institutionele en juridische waarborgen te herstellen, met inbegrip van doeltreffende, bindende controles vooraf en achteraf, alsmede onafhankelijke toezichtmechanismen; waaronder rechterlijke toetsing van surveillanceactiviteiten; benadrukt dat in het kader van een doeltreffende controle vooraf het verzoek aan de rechter om operationele surveillance, alsook het rechterlijk bevel tot die surveillance, een duidelijke rechtvaardiging en vermelding van de voor de surveillance te gebruiken technische middelen moeten bevatten, en dat in het kader van een doeltreffende controle achteraf een verplichting moet worden vastgesteld om de aan de surveillance onderworpen persoon in te lichten over het feit, de duur, de omvang en de wijze van verwerking van de tijdens de operationele surveillance verkregen gegevens;

b) te voldoen aan de verschillende arresten van het EHRM, zoals het arrest in de zaak *Roman Zakharov*/*Rusland* in 2015, waarin de noodzaak wordt onderstreept van strikte surveillancecriteria, behoorlijke rechterlijke toestemming en rechterlijk toezicht, de onmiddellijke vernietiging van irrelevante gegevens, rechterlijke toetsing van spoedprocedures en de verplichting om de betrokken personen te informeren, alsook de uitspraak in de zaak *Klass e.a.*/*Duitsland* in 1978, waarin wordt gesteld dat de surveillance van voldoende belang moet zijn om een dergelijke inbreuk op de privacy noodzakelijk te maken, alsook dat de betrokkenen in kennis moeten worden gesteld;

c) te voldoen aan alle uitspraken van het HvJ-EU en het EHRM met betrekking tot de onafhankelijkheid van de rechterlijke macht en de voorrang van het EU-recht;

d) onafhankelijke toezichthoudende instanties te herstellen overeenkomstig het arrest van het EHRM in de zaak Hüttl/Hongarije, waarin de rechtbank verklaart dat de nationale autoriteit voor gegevensbescherming en vrijheid van informatie (NAIH) niet in staat is onafhankelijk toezicht uit te oefenen op het gebruik van spyware, aangezien de geheime diensten het recht hebben om toegang tot bepaalde documenten te weigeren op basis van geheimhouding;

e) de volledige onafhankelijkheid van de rechterlijke macht en alle relevante toezichthoudende instanties, zoals de Ombudsman en de gegevensbeschermingsautoriteiten, te herstellen om ervoor te zorgen dat alle toezichthoudende instanties volledige medewerking en toegang tot informatie krijgen, en om alle personen die doelwit zijn volledige informatie te verstrekken;

f) onafhankelijke werknemers opnieuw aan te stellen in bestuursfuncties in toezichthoudende organen zoals het Grondwettelijk Hof, het Hooggerechtshof, de Rekenkamer, het openbaar ministerie, de Nationale Bank van Hongarije en de Nationale Verkiezingscommissie;

g) de klokkenluidersrichtlijn om te zetten;

h) Europol te vragen alle gevallen van vermeend misbruik van spyware te onderzoeken;

i) geen bepalingen in nieuwe wetten inzake elektronische communicatie aan te nemen die in strijd zijn met het EVRM;

j) de beschikbaarheid van doeltreffende rechtsmiddelen te waarborgen voor Hongaarse burgers die nadelen ondervinden van de uitvoering van wetten die in strijd zijn met de Hongaarse grondwet en het EVRM;

19. concludeert dat er in Griekenland sprake is geweest van inbreuken en wanbeheer bij de uitvoering van het recht van de Unie;

20. verzoekt Griekenland om:

a) dringend de institutionele en juridische waarborgen te herstellen, met inbegrip van doeltreffende controles vooraf en achteraf, alsmede onafhankelijke toezichtmechanismen;

b) met spoed alle uitvoervergunningen in te trekken die niet volledig in overeenstemming zijn met de verordening inzake producten voor tweeërlei gebruik en de beschuldigingen van illegale uitvoer, onder meer naar Sudan, te onderzoeken;

c) ervoor te zorgen dat de autoriteiten alle beschuldigingen van het gebruik van spyware vrij en ongehinderd kunnen onderzoeken;

d) amendement 826/145 van Wet 2472/1997, waarbij de Griekse autoriteit voor beveiliging en privacy van de communicatie (ADAE) niet langer in staat is burgers op de hoogte te stellen van de opheffing van de vertrouwelijkheid van communicatie, in te trekken; wet 5002/2022 te wijzigen om het recht van de beoogde personen op onmiddellijke informatie, op verzoek, zodra de surveillance is voltooid, te herstellen, en andere bepalingen die de waarborgen, de controle en de verantwoordingsplicht verzwakken, te corrigeren;

e) de volledige onafhankelijkheid van de rechterlijke macht en alle relevante toezichthoudende instanties, zoals de Ombudsman en de gegevensbeschermingsautoriteiten, te herstellen en de onafhankelijkheid van de ADAE volledig te eerbiedigen om ervoor te zorgen dat alle controlerende en toezichthoudende instanties volledige medewerking en toegang tot informatie krijgen, en om alle personen die doelwit zijn volledige informatie te verstrekken;

f) ervoor te zorgen dat de ADAE een elektronisch archief kan opzetten om haar taak te kunnen uitvoeren;

g) dringend duidelijkheid te verschaffen over de situatie rond het misbruik van spyware in Griekenland, zodat de integriteit van de komende verkiezingen geenszins in twijfel kan worden getrokken;

h) de wetswijziging van 2019 waarbij de nationale inlichtingendienst (EYP) onder de rechtstreekse controle van de premier werd geplaatst, terug te draaien; grondwettelijke garanties in te voeren en parlementaire controle op haar activiteiten mogelijk te maken, zonder het voorwendsel van vertrouwelijkheid van informatie;

i) de onafhankelijkheid van het leiderschap van de nationale transparantie-autoriteit (EAD) te waarborgen;

j) ervoor te zorgen dat de rechterlijke macht over alle nodige middelen en ondersteuning beschikt voor het onderzoek naar aanleiding van het vermeende misbruik van spyware en de hand te leggen op het fysieke bewijsmateriaal van gelieerde personen, makelaars en spywareverkopers die in verband wordt gebracht met de infecties van spyware;

k) Europol te verzoeken onmiddellijk aan het onderzoek deel te nemen;

l) zich te onthouden van politieke inmenging in het werk van de hoofdaanklager;

21. concludeert dat het regelgevingskader in Spanje in het algemeen voldoet aan de eisen van de Verdragen; wijst er echter op dat er enkele hervormingen nodig zijn en dat de uitvoering in de praktijk volledig in overeenstemming moet zijn met de grondrechten en de bescherming van de inspraak van het publiek moet waarborgen;

22. verzoekt daarom Spanje om:

a) een volledig, eerlijk en doeltreffend onderzoek te verrichten, waarbij volledige duidelijkheid wordt verschaft over alle vermeende gevallen van het gebruik van spyware, met inbegrip van de 47 gevallen waarvoor het onduidelijk blijft of de betrokken personen al dan niet met een gerechtelijk bevel door de Spaanse nationale inlichtingendienst (CNI) doelwit zijn geweest, dan wel of een andere autoriteit een gerechtelijk bevel had gekregen om hen legaal in het oog te houden, alsmede over het gebruik van spyware tegen de minister-president en leden van de regering, en de bevindingen zo breed mogelijk te presenteren, overeenkomstig de toepasselijke wetgeving;

b) de beoogde personen adequate toegang te verschaffen tot de door het Hooggerechtshof aan de CNI verleende rechterlijke machtiging om 18 personen als doelwit te nemen;

c) samen te werken met de rechtbanken om ervoor te zorgen dat personen die het doelwit zijn van spyware toegang hebben tot een reëel en zinvol rechtsmiddel, en dat gerechtelijke onderzoeken onverwijld op onpartijdige en grondige wijze worden afgerond, waarvoor voldoende middelen moeten worden uitgetrokken;

d) te beginnen met de hervorming van het rechtskader van de CNI, zoals aangekondigd in mei 2022;

e) Europol, die met technische expertise zou kunnen bijdragen, te verzoeken zich bij de onderzoeken aan te sluiten;

23. concludeert dat er bewijs is dat er in Cyprus sprake is geweest van wanbeheer bij de uitvoering van de EU-verordening inzake producten voor tweeërlei gebruik, hetgeen grondig onderzocht moet worden;

24. verzoekt Cyprus om:

a) alle voor spyware afgegeven uitvoervergunningen grondig te beoordelen en in

voorkomend geval in te trekken;

b) de verzending van spywarematériaal binnen de interne markt van de EU tussen de lidstaten aan een grondige beoordeling te onderwerpen en de verschillende Israëlische bedrijven of de bedrijven die eigendom zijn van en bestuurd worden door Israëlische burgers, in Cyprus geregistreerd staan en bij dergelijke activiteiten betrokken zijn, in kaart te brengen;

c) het verslag van de speciale onderzoeker over de zaak “spywarebestelwagen” vrij te geven, waarom is verzocht door de commissie tijdens haar werkbezoek aan Cyprus;

d) met de hulp van Europol alle beschuldigingen van het onrechtmatige gebruik en de uitvoer van spyware grondig te onderzoeken, met name tegen journalisten, advocaten, actoren uit het maatschappelijk middenveld en Cypriotische burgers;

25. is van mening dat de situatie in sommige andere lidstaten ook reden tot zorg is, met name gezien de aanwezigheid van een lucratieve en groeiende spywaresector die profiteert van de goede reputatie, de interne markt en het vrije verkeer van de Unie, waardoor sommige lidstaten zoals Cyprus en Bulgarije een exportknooppunt voor spyware kunnen worden naar repressieve regimes over de hele wereld;

26. is van mening dat het verzuim of de weigering van sommige nationale autoriteiten om de burgers van de Unie naar behoren te beschermen, met inbegrip van lacunes in de regelgeving en fatsoenlijke rechtsinstrumenten, ondubbelzinnig aantoont dat optreden op het niveau van de Unie onontbeerlijk is om ervoor te zorgen dat de letter van de Verdragen wordt nageleefd en dat de wetgeving van de Unie in acht wordt genomen, zodat het recht van de burgers op een leven in een veilige omgeving, menselijke waardigheid, privéleven, persoonsgegevens en eigendom wordt geëerbiedigd, zoals vereist door Richtlijn 2012/29/EU op grond waarvan elk slachtoffer van een misdrijf het recht heeft op steun en bescherming volgens zijn individuele behoeften;

27. concludeert dat er ernstige tekortkomingen bij de toepassing van het Unierecht hebben plaatsgevonden toen de Commissie en de Europese Dienst voor extern optreden (EDEO) steun verleenden aan niet-EU-landen, waaronder maar niet beperkt tot tien van dergelijke landen in de Sahel, teneinde hen in staat te stellen surveillancecapaciteit te ontwikkelen[29];

28. is van mening dat de handel in en het gebruik van spyware strikt moeten worden gereguleerd; erkent echter dat het wetgevingsproces tijd kan vergen, terwijl misbruik onmiddellijk moet worden gestopt; vraagt om de vaststelling van voorwaarden voor het legale gebruik en de legale verkoop, verwerving en overdracht van spyware; dringt erop aan dat de lidstaten voor het verdere gebruik van spyware uiterlijk op 31 december 2023 aan alle onderstaande voorwaarden voldoen:

a) alle gevallen van vermeend misbruik van spyware worden grondig onderzocht en onverwijld door de bevoegde rechtshandhavings-, vervolgings- en gerechtelijke autoriteiten opgelost;

[29] Besluit in zaak 1904/2021/MHZ, beschikbaar op https://www.ombudsman.europa.eu/nl/decision/nl/163491

b) zij tonen aan dat het kader voor het gebruik van spyware in overeenstemming is met de normen van de Commissie van Venetië en de desbetreffende jurisprudentie van het HvJ-EU en het EHRM;

c) zij gaan een uitdrukkelijke verbintenis aan om Europol overeenkomstig de artikelen 4 tot en met 6 van de verordening betreffende Europol te betrekken bij onderzoeken naar beschuldigingen van onrechtmatig gebruik van spyware; en dat

d) alle uitvoervergunningen die niet volledig in overeenstemming zijn met de verordening inzake producten voor tweeërlei gebruik worden ingetrokken;

29. is van mening dat de Commissie uiterlijk op 30 november 2023 moet beoordelen of aan de voorwaarden is voldaan; is voorts van mening dat de bevindingen van de beoordeling in een verslag bekendgemaakt moeten worden;

30. benadrukt dat de bestrijding van zware criminaliteit en terrorisme en het besef dat het vermogen daartoe weliswaar van cruciaal belang zijn voor de lidstaten, maar dat de bescherming van de grondrechten en de democratie essentieel is; benadrukt voorts dat het gebruik van spyware door de lidstaten evenredig moet zijn, niet willekeurig mag zijn en surveillance alleen mag worden toegestaan onder vooraf strikt bepaalde omstandigheden; is van mening dat doeltreffende mechanismen vooraf om rechterlijk toezicht te waarborgen, van cruciaal belang zijn voor de bescherming van individuele vrijheden; bevestigt nogmaals dat individuele rechten niet in gevaar mogen worden gebracht door vrije toegang tot surveillance toe te staan; onderstreept dat ook het vermogen van de rechterlijke macht om zinvol en doeltreffend toezicht achteraf uit te oefenen op verzoeken om surveillance ten behoeve van de nationale veiligheid belangrijk is, om ervoor te zorgen dat onevenredig gebruik van spyware door regeringen kan worden aangevochten;

31. onderstreept dat het gebruik van spyware voor rechtshandhaving rechtstreeks moet worden geregeld via maatregelen op basis van hoofdstuk 4 van titel 5 VWEU inzake justitiële samenwerking in strafzaken; benadrukt dat de configuratie van spyware die in de EU wordt ingevoerd en anderszins op de markt wordt gebracht, moet worden geregeld door middel van een maatregel op basis van artikel 114 VWEU; merkt op dat het gebruik van spyware voor nationale veiligheidsdoeleinden slechts indirect kan worden geregeld via bijvoorbeeld de grondrechten en de regels inzake gegevensbescherming;

32. is van mening dat, gezien de transnationale en EU-dimensie van het gebruik van spyware, een gecoördineerde en transparante controle op EU-niveau noodzakelijk is om niet alleen de bescherming van EU-burgers, maar ook de geldigheid van door middel van spyware verzameld bewijsmateriaal in grensoverschrijdende zaken te waarborgen, en dat er duidelijk behoefte is aan gemeenschappelijke EU-normen op basis van hoofdstuk 4 van titel 5 VWEU ter regulering van het gebruik van spyware door organen van de lidstaten, op basis van normen die zijn vastgesteld door het HvJ-EU, het EHRM, de Commissie van Venetië en het Bureau voor de grondrechten[30]; is van mening dat

[30] Bureau voor de grondrechten, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Volume II Summary*, 2017, https://fra.europa.eu/nl/publication/2017/surveillance-intelligence-services-fundamental-rights-safeguards-and-remedies-eu

dergelijke EU-normen ten minste de volgende elementen moeten omvatten:

a) het beoogde gebruik van spyware mag alleen in uitzonderlijke en specifieke gevallen worden toegestaan om de nationale veiligheid te beschermen en moet onderworpen zijn aan een doeltreffende, bindende en betekenisvolle voorafgaande rechterlijke toestemming van een onpartijdige en onafhankelijke rechterlijke instantie of een andere onafhankelijke democratische toezichthoudende instantie, die toegang heeft tot alle relevante informatie en de noodzaak en evenredigheid van de beoogde maatregel aantoont;

b) spyware mag niet langer worden ingezet dan strikt noodzakelijk is, in de rechterlijke toestemming vooraf moet voor elk apparaat waartoe toegang wordt verkregen de precieze reikwijdte en duur zijn bepaald en de hacking mag alleen worden verlengd wanneer verdere rechterlijke toestemming voor een andere gespecificeerde periode is verleend, gezien de aard van spyware en de mogelijkheid van surveillance met terugwerkende kracht; de autoriteiten van de lidstaten mogen bovendien alleen individuele apparaten of accounts van eindgebruikers targeten en mogen geen aanbieders van internet- en technologiediensten hacken, om te voorkomen dat gebruikers die geen doelwit zijn, daar gevolgen van ondervinden;

c) de toestemming voor het gebruik van spyware mag alleen in uitzonderlijke gevallen worden verleend voor onderzoeken naar een beperkte en gesloten lijst van duidelijk en nauwkeurig omschreven ernstige misdrijven die een reële bedreiging voor de nationale veiligheid vormen, en spyware mag alleen worden gebruikt bij personen ten aanzien van wie er voldoende aanwijzingen zijn dat zij ernstige misdrijven hebben gepleegd of voornemens zijn te plegen;

d) gegevens die worden beschermd door voorrechten of immuniteiten die betrekking hebben op categorieën personen (zoals politici, artsen enz.) of specifiek beschermde relaties (zoals vertrouwelijkheid van de communicatie tussen advocaat en cliënt) of regels betreffende de vaststelling en beperking van strafrechtelijke aansprakelijkheid met betrekking tot de persvrijheid en de vrijheid van meningsuiting in andere media, mogen niet met spyware worden opgevraagd, tenzij onder gerechtelijk toezicht voldoende gronden zijn vastgesteld die hun betrokkenheid bij criminele activiteiten of aangelegenheden van nationale veiligheid bevestigen, waarvoor een gemeenschappelijk kader moet gelden;

e) er moeten specifieke regels worden opgesteld voor surveillance op basis van spywaretechnologie, aangezien hiermee onbeperkte toegang met terugwerkende kracht kan worden verkregen tot berichten, bestanden en metagegevens;

f) de lidstaten moeten ten minste het aantal goedgekeurde en afgewezen verzoeken om surveillance en het soort en het doel van het onderzoek bekendmaken en elk onderzoek anoniem registreren in een nationaal register met een unieke identificatiecode, zodat het kan worden onderzocht in geval van vermeend misbruik;

g) de nationale controleorganen moeten verslag uitbrengen aan de lidstaten, en de lidstaten moeten deze informatie vervolgens regelmatig aan de Commissie meedelen; de Commissie moet deze informatie in haar jaarlijks verslag over de rechtsstaat gebruiken om het gebruik van spyware in de lidstaten te kunnen vergelijken;

h) het recht van kennisgeving aan de beoogde persoon: na afloop van de surveillance moeten de autoriteiten de persoon in kennis stellen van het feit dat de autoriteiten spyware hebben gebruikt, met inbegrip van informatie over de datum en de duur van de surveillance, het voor de surveillance uitgevaardigde bevel, de verkregen gegevens, informatie over hoe die gegevens zijn gebruikt en door welke actoren, de datum van de verwijdering van de gegevens en het recht en de praktische regelingen om bij de bevoegde autoriteiten administratieve en gerechtelijke beroepsprocedures in te stellen; merkt op dat deze kennisgeving onverwijld moet worden verzonden, tenzij een onafhankelijke rechterlijke autoriteit uitstel van de kennisgeving toestaat in het geval dat onmiddellijke kennisgeving het doel van de surveillance ernstig in gevaar zou brengen;

i) het recht van kennisgeving aan niet-beoogde personen tot wier gegevens toegang is verkregen: na afloop van de periode waarvoor de surveillance was toegestaan, moeten de autoriteiten de personen wier recht op privacy ernstig is geschonden door het gebruik van spyware, maar die niet het doelwit van de operatie waren, daarvan in kennis stellen; de autoriteiten moeten deze persoon in kennis stellen van het feit dat zijn gegevens door de autoriteiten zijn bekeken, informatie verstrekken over de datum en de duur van de surveillance, het voor de surveillance uitgevaardigde bevel, de verkregen gegevens, informatie over hoe die gegevens zijn gebruikt en door welke actoren, en de datum van de verwijdering van de gegevens; merkt op dat deze kennisgeving onverwijld moet worden verzonden, tenzij een onafhankelijke rechterlijke autoriteit uitstel van de kennisgeving toestaat in het geval dat onmiddellijke kennisgeving het doel van de surveillance ernstig in gevaar zou brengen;

j) effectief, bindend en onafhankelijk toezicht achteraf op het gebruik van spyware, waarbij de daarvoor verantwoordelijke instanties over alle nodige middelen en bevoegdheden moeten beschikken om betekenisvol toezicht uit te oefenen en gekoppeld moeten worden aan parlementair toezicht op basis van partijoverschrijdend lidmaatschap met een passende machtiging en met volledige toegang tot voldoende informatie om zich ervan te vergewissen dat de surveillance rechtmatig en evenredig is uitgevoerd, en parlementair toezicht op gevoelige vertrouwelijke informatie moet worden vergemakkelijkt door middel van de nodige infrastructuur, processen en veiligheidsmachtigingen; ongeacht de definitie of afbakening van het begrip nationale veiligheid, moeten de nationale toezichthoudende instanties bevoegd zijn voor de volledige reikwijdte van de nationale veiligheid;

k) fundamentele beginselen van behoorlijke rechtsgang en rechterlijk toezicht moeten centraal staan in de regeling rond surveillancespyware;

l) een zinvol rechtsmiddel voor directe en indirecte doelwitten en voor personen die beweren dat zij nadeel ondervinden van het toezicht, moet toegang bieden tot verhaal via een onafhankelijke instantie; dringt daarom aan op de invoering van een kennisgevingsverplichting voor overheidsinstanties, met inbegrip van passende termijnen voor kennisgeving, waarbij deze plaatsvindt zodra de bedreiging voor de veiligheid voorbij is;

m) rechtsmiddelen moeten zowel rechtens als feitelijk doeltreffend zijn, alsook bekend en toegankelijk; benadrukt dat dergelijke rechtsmiddelen een snel, grondig en onpartijdig

onderzoek door een onafhankelijke toezichthoudende instantie vereisen en dat deze instantie toegang, alsmede de deskundigheid en technische capaciteiten moet hebben om alle relevante gegevens te verwerken teneinde te kunnen bepalen of de veiligheidsbeoordeling door de autoriteiten van een persoon betrouwbaar en evenredig is; in gevallen waarin misbruik is vastgesteld, moeten passende sancties van strafrechtelijke of administratieve aard worden opgelegd, overeenkomstig het toepasselijke nationale recht van de lidstaten;

n) de verbetering van de kosteloze toegang van de betrokkenen tot technologische expertise in dit stadium, aangezien de grotere beschikbaarheid en betaalbaarheid van technologische processen, zoals forensische analyse, de betrokkenen in staat zou stellen om in rechte sterkere argumenten aan te voeren en de vertegenwoordiging van de betrokkenen in rechte zou verbeteren door technologische capaciteitsopbouw van de juridische vertegenwoordiging en de rechterlijke macht om de betrokkenen beter te adviseren, schendingen vast te stellen en het toezicht op en de verantwoording voor misbruik van spyware te verbeteren;

o) de versterking van de rechten van de verdediging en het recht op een eerlijk proces door ervoor te zorgen dat personen die van strafbare feiten worden beschuldigd, de juistheid, authenticiteit, betrouwbaarheid en zelfs de wettigheid van het tegen hen gebruikte bewijsmateriaal mogen en kunnen controleren, waarmee een algemene toepassing van de nationale regels inzake het defensiegeheim wordt afgewezen;

p) tijdens het toezicht moeten de autoriteiten alle gegevens wissen die irrelevant zijn voor het toegestane onderzoek en na de beëindiging van de surveillance en het onderzoek waarvoor de vergunning is verleend, moeten de autoriteiten de gegevens en alle daarmee verband houdende documenten verwijderen, zoals aantekeningen die tijdens die periode zijn gemaakt, en deze verwijdering moet worden geregistreerd en controleerbaar zijn;

q) relevante informatie die door spyware wordt verkregen, mag alleen toegankelijk zijn voor bevoegde autoriteiten en alleen ten behoeve van een operatie; deze toegang moet worden beperkt tot een bepaalde, in de gerechtelijke procedure vastgestelde periode;

r) er moeten minimumnormen worden vastgesteld voor de rechten van personen in strafprocedures met betrekking tot de toelaatbaarheid van bewijsmateriaal dat met behulp van spyware is verzameld; de mogelijkheid dat door de inzet van spyware valse of gemanipuleerde informatie wordt geproduceerd (nabootsing) moet in het strafprocesrecht worden opgenomen;

s) de lidstaten moeten elkaar in kennis stellen in het geval van surveillance van burgers of ingezetenen van een andere lidstaat of van een mobiel nummer van een aanbieder in een andere lidstaat;

t) in de surveillancesoftware moet een marker worden opgenomen zodat de toezichthoudende instanties in geval van een vermoeden van misbruik de gebruiker ondubbelzinnig kunnen identificeren; de verplichte handtekening voor elke inzet van spyware moet bestaan uit een individueel label voor de optredende autoriteit, het gebruikte type spyware en een geanonimiseerd zaaknummer;

33. verzoekt de lidstaten openbare raadplegingen te houden met belanghebbenden, de transparantie van het wetgevingsproces te waarborgen en EU-normen en -waarborgen op te nemen bij het opstellen van nieuwe wetgeving inzake het gebruik en de verkoop van spyware;

34. benadrukt dat alleen spyware die zodanig is ontworpen dat deze de werking van spyware mogelijk maakt en vergemakkelijkt overeenkomstig het wetgevingskader zoals uiteengezet in paragraaf 29, op de interne markt mag worden gebracht, ontwikkeld of gebruikt in de Unie; bevestigt dat een dergelijke verordening inzake het op de markt brengen van spyware die voorziet in een "rule-of-law-by-design" op basis van artikel 114 VWEU, de burgers van de Unie een hoog beschermingsniveau moet bieden; acht het ongerechtvaardigd dat, terwijl de verordening inzake producten voor tweeërlei gebruik sinds 2021 burgers van niet-EU-landen bescherming biedt tegen de uitvoer van spyware uit de EU, EU-burgers geen gelijkwaardige bescherming wordt geboden;

35. is van oordeel dat alleen onderscheppings- en extractietechnologie door bedrijven in de EU mag worden verkocht en door de lidstaten mag worden verworven, en niet "hacking als dienst", dat de levering van technische, operationele en methodologische ondersteuning van surveillancetechnologie omvat en de aanbieder toegang geeft tot een onevenredige hoeveelheid gegevens die onverenigbaar is met de beginselen van evenredigheid, noodzakelijkheid, rechtmatigheid, wettigheid en adequaatheid; vraagt de Commissie een wetsvoorstel in deze zin te doen;

36. benadrukt dat spyware alleen in de handel mag worden gebracht voor verkoop aan en gebruik door overheidsinstanties, op basis van een gesloten lijst, die onder meer tot taak hebben misdrijven te onderzoeken of de nationale veiligheid te beschermen waarvoor het gebruik van spyware kan worden toegestaan; is van mening dat veiligheidsdiensten alleen spyware mogen gebruiken wanneer alle aanbevelingen van het Bureau voor de grondrechten zijn uitgevoerd[31];

37. benadrukt dat er een spywareversie moet worden gebruikt die zodanig is ontworpen dat de toegang tot alle op een apparaat opgeslagen gegevens tot een minimum wordt beperkt, maar die zodanig is ontworpen dat de toegang tot gegevens wordt beperkt tot het minimum dat strikt noodzakelijk is voor het doel van het toegestane onderzoek;

38. concludeert dat wanneer een lidstaat spyware heeft gekocht, de aankoop moet kunnen worden gecontroleerd door een onafhankelijk, onpartijdig auditorgaan met een passende veiligheidsmachtiging;

39. benadrukt dat alle entiteiten die spyware op de interne markt brengen, moeten voldoen aan strikte zorgvuldigheidseisen, en dat bedrijven die zich als leverancier inschrijven op een openbare aanbesteding, moeten worden doorgelicht, waarbij onder meer wordt nagegaan hoe het bedrijf reageert op mensenrechtenschendingen die met hun software zijn begaan, en of de technologie gebaseerd is op gegevens die zijn verzameld in het kader van ondemocratische en onrechtmatige surveillancepraktijken; benadrukt dat de bevoegde nationale toezichthoudende autoriteiten jaarlijks aan de Commissie verslag

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

moeten uitbrengen over de naleving;

40. benadrukt dat bedrijven die surveillancetechnologieën of -diensten aan overheidsactoren aanbieden, de aard van de uitvoervergunningen aan de bevoegde nationale toezichthoudende autoriteiten moeten meedelen;

41. onderstreept dat de lidstaten een afkoelingsperiode moeten instellen, waardoor voormalige werknemers van overheidsinstanties of -agentschappen tijdelijk niet voor spywarebedrijven kunnen gaan werken;

Noodzaak van grenzen aan de nationale veiligheid

42. is bezorgd over gevallen waarin ten onrechte een beroep wordt gedaan op "nationale veiligheid" om de inzet en het gebruik van spyware te rechtvaardigen en te zorgen voor absolute geheimhouding en het ontbreken van verantwoordingsplicht; is ingenomen met de verklaring van de Commissie, in overeenstemming met de jurisprudentie van het HvJ-EU[32], dat enkel en alleen een verwijzing naar de nationale veiligheid niet kan worden geïnterpreteerd als een onbeperkte uitzondering van de toepassing van het EU-recht en een duidelijke rechtvaardiging moet vereisen, en verzoekt de Commissie follow-up te geven aan deze verklaring ingeval er aanwijzingen zijn van misbruik; is van mening dat in een democratische, transparante samenleving die zich aan de rechtsstaat houdt, dergelijke beperkingen in naam van de nationale veiligheid eerder uitzondering dan regel zullen zijn;

43. is van mening dat het begrip nationale veiligheid moet worden afgezet tegen de beperktere reikwijdte ten opzichte van het begrip binnenlandse veiligheid, dat een ruimer toepassingsgebied heeft, waaronder het voorkomen van risico's voor burgers en met name de handhaving van het strafrecht;

44. betreurt de moeilijkheden die voortvloeien uit het ontbreken van een gemeenschappelijke juridische definitie van nationale veiligheid, waarin criteria zijn vastgelegd om te bepalen welke wettelijke regeling van toepassing kan zijn op het gebied van de nationale veiligheid, alsook van een duidelijke afbakening van het gebied waarop een dergelijke bijzondere regeling van toepassing kan zijn;

45. is van mening dat het gebruik van spyware een beperking van de grondrechten vormt; is voorts van mening dat wanneer een begrip in een juridische context wordt gebruikt, hetgeen de overdracht van rechten en het opleggen van verplichtingen (en met name beperkingen van de grondrechten van personen) met zich meebrengt, het begrip duidelijk en voorzienbaar moet zijn voor alle personen die erdoor worden getroffen; herinnert eraan dat in het Handvest van de grondrechten is bepaald dat elke beperking van de grondrechten overeenkomstig artikel 52, lid 1, bij wet moet worden vastgelegd; acht het daarom noodzakelijk dat "nationale veiligheid" duidelijk wordt gedefinieerd; benadrukt dat, ongeacht de precieze afbakening, het domein van de nationale veiligheid

[32] Arrest van 6 oktober 2020, zaak C-623/17, *Privacy International*/*Secretary of State for Foreign and Commonwealth Affairs en anderen*, EU:C:2020:790, punt 44 en arresten van 6 oktober 2020, gevoegde zaken C-511/18, C-512/18 en C-520/18, *La Quadrature du Net en anderen*/*Premier ministre en anderen*, EU:C:2020:791, punt 99: "het enkele feit dat een nationale maatregel is genomen met het oog op de bescherming van de nationale veiligheid, [kan er] niet [toe] leiden dat het Unierecht niet van toepassing is en dat de lidstaten worden ontheven van de verplichting om dit recht te eerbiedigen".

in zijn geheel onderworpen moet zijn aan onafhankelijk, bindend en doeltreffend toezicht;

46. benadrukt dat indien de autoriteiten redenen van nationale veiligheid aanvoeren om het gebruik van spyware te rechtvaardigen, zij, in aanvulling op het in paragraaf 29 vastgestelde kader, moeten aantonen dat zij het EU-recht in acht nemen, met inbegrip van de beginselen van evenredigheid, noodzakelijkheid, rechtmatigheid, wettigheid en adequaatheid; benadrukt dat de rechtvaardiging gemakkelijk toegankelijk moet zijn en ter beoordeling aan een nationaal controleorgaan ter beschikking moet worden gesteld;

47. herhaalt in deze context dat alle lidstaten Verdrag 108+ hebben ondertekend, waarin normen en verplichtingen zijn vastgelegd voor de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, ook voor doeleinden van nationale veiligheid; wijst erop dat Verdrag 108+ een bindend Europees kader is voor de verwerking van gegevens door inlichtingen- en veiligheidsdiensten; dringt er bij alle lidstaten op aan dit Verdrag onverwijld te ratificeren en de normen ervan reeds in nationaal recht om te zetten en dienovereenkomstig te handelen op het gebied van de nationale veiligheid;

48. benadrukt dat uitzonderingen en beperkingen op een beperkt aantal bepalingen van het verdrag alleen zijn toegestaan indien zij in overeenstemming zijn met de vereisten van artikel 11 van het Verdrag, wat betekent dat bij de uitvoering van Verdrag 108+ elke specifieke uitzondering en beperking bij wet moet worden vastgesteld en de wezenlijke inhoud van de grondrechten en de fundamentele vrijheden moet eerbiedigen en dat moet worden gerechtvaardigd dat de uitzondering “in een democratische samenleving een noodzakelijke en evenredige maatregel vormt” om een van de in artikel 11[33] genoemde legitieme redenen, en dat die uitzonderingen en beperkingen geen belemmering mogen vormen voor onafhankelijke en doeltreffende toetsing en toezicht overeenkomstig de binnenlandse wetgeving van de respectieve partij;

49. merkt voorts op dat Verdrag 108+ benadrukt dat het toezicht over onderzoeks- en interventiebevoegdheden beschikt; is van mening dat voor doeltreffende toetsing en toezicht bindende bevoegdheden nodig zijn waar de gevolgen voor de grondrechten het grootst zijn, met name in de toegangs-, analyse- en opslagfase van de verwerking van persoonsgegevens;

50. is van mening dat het ontbreken van bindende bevoegdheden van toezichthoudende instanties op het gebied van de nationale veiligheid onverenigbaar is met het in Verdrag 108+ neergelegde criterium dat dit in een democratische samenleving een noodzakelijke en evenredige maatregel vormt;

51. wijst erop dat Verdrag 108+ een zeer beperkt aantal uitzonderingen op artikel 15 toestaat, maar dergelijke uitzonderingen met name niet toestaat op lid 2 [bewustmakingsplicht], lid 3 [raadpleging over wettelijke en bestuursrechtelijke

[33] In deze beoordeling is voorzien in de jurisprudentie van het EHRM, waarin de bewijslast bij de staat/wetgever wordt gelegd. De betreffende jurisprudentie van het EHRM omvat: *Roman Zakharov*/*Rusland* (verzoek nr. 47143/06), 4 december 2015; *Szabó en Vissy*/*Hongarije* (verzoek nr. 37138/14), 12 januari 2016; *Big Brother Watch e.a.*/*Verenigd Koninkrijk* (aanvraag nrs. 58170/13, 62322/14 en 24969/15), 25 mei 2021 en *Centrum för rättvisa*/*Zweden* (aanvraag nr. 35252/08), 25 mei 2021.

maatregelen], lid 4 [verzoeken en klachten van personen], lid 5 [onafhankelijkheid en onpartijdigheid], lid 6 [noodzakelijke middelen voor een doeltreffende uitvoering van de taken], lid 7 [periodieke verslaglegging], lid 8 [vertrouwelijkheid], lid 9 [beroepsmogelijkheid] en lid 10 [geen bevoegdheid ten aanzien van instanties die in hun hoedanigheid van rechter optreden];

Betere uitvoering en handhaving van bestaande wetgeving

52. onderstreept de tekortkomingen in de nationale rechtskaders en de noodzaak van een betere handhaving van de bestaande Uniewetgeving om deze tekortkomingen aan te pakken; stelt vast dat de volgende wetgeving van de Unie relevant is, maar te vaak onjuist wordt uitgevoerd en/of gehandhaafd: de antiwitwasrichtlijn, de richtlijn gegevensbescherming bij rechtshandhaving, de aanbestedingsregels, de verordening inzake producten voor tweeërlei gebruik, de jurisprudentie (uitspraken over surveillance en nationale veiligheid) en de klokkenluidersrichtlijn; verzoekt de Commissie de tekortkomingen in de uitvoering en handhaving te onderzoeken en hierover verslag uit te brengen en een routekaart voor te stellen om deze uiterlijk op 1 augustus 2023 te verhelpen;

53. is van mening dat de correcte toepassing en de strikte handhaving van het rechtskader van de Unie inzake gegevensbescherming, met name de richtlijn wetshandhaving, de algemene verordening gegevensbescherming en de e-privacyrichtlijn, van cruciaal belang zijn; acht het evenzeer van belang dat de desbetreffende arresten van het HvJ-EU volledig ten uitvoer worden gelegd, wat in verschillende lidstaten nog steeds niet het geval is; herinnert eraan dat de Commissie een centrale rol speelt door het handhaven van het EU-recht en het waarborgen van de uniforme toepassing ervan in de hele Unie, en dat zij gebruik moet maken van alle beschikbare instrumenten, met inbegrip van inbreukprocedures in geval van aanhoudende niet-naleving;

54. dringt erop aan dat de Overeenkomst van Wassenaar een bindende overeenkomst wordt voor alle deelnemers, met als doel het tot een internationaal verdrag te maken;

55. dringt erop aan dat Cyprus en Israël deelnemende staten van de Overeenkomst van Wassenaar worden; herinnert de lidstaten eraan dat alles in het werk moet worden gesteld om Cyprus en Israël in staat te stellen toe te treden tot de Overeenkomst van Wassenaar;

56. benadrukt dat de Overeenkomst van Wassenaar een mensenrechtenkader moet omvatten waarin de afgifte van vergunningen voor spywaretechnologieën is geïntegreerd, de naleving van bedrijven die spywaretechnologieën produceren wordt beoordeeld en geëvalueerd, en dat de deelnemende partijen de aankoop van surveillancetechnologieën moeten verbieden door staten die geen deel uitmaken van de overeenkomst;

57. benadrukt dat de Commissie en de lidstaten in het licht van de onthullingen van spyware een diepgaand onderzoek moeten instellen naar uitvoervergunningen die zijn verleend voor het gebruik van spyware in het kader van de verordening inzake producten voor tweeërlei gebruik, en dat de Commissie de resultaten van dit onderzoek met het Parlement moet delen;

58. onderstreept de noodzaak van traceerbaarheid van en verantwoording voor de uitvoer

van spyware en herinnert eraan dat EU-bedrijven alleen spyware mogen uitvoeren die voldoende traceerbaar is om ervoor te zorgen dat de verantwoordelijkheid altijd kan worden toegewezen;

59. benadrukt dat de Commissie de herschikte verordening inzake producten voor tweeërlei gebruik regelmatig moet controleren en naar behoren moet handhaven om "export regime shopping" (gebruikmaking van landen met gunstige uitvoerregelingen) in de hele Unie te voorkomen, zoals momenteel het geval is in Bulgarije en Cyprus, en dat de Commissie over voldoende middelen moet beschikken om deze taak uit te voeren;

60. verzoekt de Commissie te zorgen voor voldoende personeelscapaciteit voor de eenheden die verantwoordelijk zijn voor het toezicht op en de handhaving van de verordening inzake producten voor tweeërlei gebruik;

61. dringt aan op wijzigingen van de verordening inzake producten voor tweeërlei gebruik om in artikel 15 te verduidelijken dat uitvoervergunningen voor goederen voor tweeërlei gebruik niet mogen worden afgegeven wanneer goederen bestemd zijn of kunnen zijn voor binnenlandse repressie en/of het plegen van ernstige inbreuken op de mensenrechten en het internationaal humanitair recht; dringt aan op de volledige uitvoering van mensenrechten- en zorgvuldigheidscontroles in het vergunningsproces en op verdere verbeteringen, zoals remediëring voor doelwitten van mensenrechtenschendingen en transparante verslaglegging over de toegepaste zorgvuldigheid;

62. dringt aan op wijzigingen van de verordening inzake producten voor tweeërlei gebruik om te waarborgen dat doorvoer wordt verboden in gevallen waarin goederen bestemd zijn of kunnen zijn voor binnenlandse repressie en/of het plegen van ernstige inbreuken op de mensenrechten en het internationaal humanitair recht;

63. benadrukt dat bij een toekomstige wijziging van de verordening inzake producten voor tweeërlei gebruik de aangewezen nationale autoriteiten die verantwoordelijk zijn voor de goedkeuring en weigering van uitvoervergunningen voor producten voor tweeërlei gebruik gedetailleerde verslagen moeten verstrekken, met inbegrip van informatie over het product voor tweeërlei gebruik in kwestie; het aantal aangevraagde vergunningen; de naam van het land van uitvoer; een beschrijving van het exportbedrijf en of dit bedrijf een dochteronderneming is; een beschrijving van de eindgebruiker en de bestemming; de waarde van de uitvoervergunning; en de reden waarom de uitvoervergunning is goedgekeurd dan wel is geweigerd; benadrukt dat deze verslagen elk kwartaal openbaar moeten worden gemaakt; dringt aan op de oprichting van een speciale vaste parlementaire commissie met toegang tot gerubriceerde informatie van de Commissie, met het oog op parlementair toezicht;

64. benadrukt dat bij een toekomstige wijziging van de verordening inzake producten voor tweeërlei gebruik de uitzondering op de verplichting om de Commissie informatie te verstrekken om redenen die verband houden met commerciële gevoeligheid, defensie, buitenlands beleid of nationale veiligheid moet worden afgeschaft; is van mening dat de Commissie, om te voorkomen dat gevoelige informatie beschikbaar komt voor niet-EU-landen, in plaats daarvan kan besluiten bepaalde informatie in haar jaarverslag te rubriceren;

65. benadrukt dat de definitie van producten voor cybersurveillance in de herschikte verordening inzake producten voor tweeërlei gebruik niet restrictief mag worden geïnterpreteerd, maar alle technologieën op dit gebied moet omvatten, zoals interceptie of verstoring van mobieletelefooncommunicatie; inbraakprogrammatuur; surveillancesystemen of -apparatuur voor netwerkcommunicaties van het internetprotocol; programmatuur, speciaal ontworpen of aangepast voor monitoring of analyse door rechtshandhavingsinstanties; laser-akoestische detectieapparatuur; forensische instrumenten waarmee ruwe gegevens uit een computer of communicatieapparaat worden geëxtraheerd en de "authenticatie-" of autorisatiecontroles van het apparaat worden omzeild; elektronische systemen of apparatuur ontworpen voor de bewaking en monitoring van het elektromagnetisch spectrum voor militaire inlichtingen- of veiligheidsdoeleinden; en onbemande luchtvaartuigen die surveillance kunnen uitvoeren;

66. dringt aan op aanvullende Europese wetgeving op grond waarvan bedrijfsactoren die surveillancetechnologieën produceren en/of uitvoeren, mensenrechten- en zorgvuldigheidskaders moeten opnemen in overeenstemming met de leidende beginselen van de VN inzake bedrijfsleven en mensenrechten (UNGP's);

Internationale samenwerking ter bescherming van burgers

67. pleit voor een gezamenlijke EU-VS-spionagesoftwarestrategie, met inbegrip van een gezamenlijke witte en/of zwarte lijst van verkopers van spyware wier instrumenten zijn misbruikt of dreigen te worden misbruikt om overheidsfunctionarissen, journalisten en het maatschappelijk middenveld kwaadaardig te treffen, en die tegen het veiligheids- en buitenlands beleid van de Unie opereren, door buitenlandse regeringen met een slechte reputatie op het gebied van mensenrechten, die (geen) toestemming hebben om aan overheidsinstanties te verkopen, gemeenschappelijke criteria voor verkopers om op een van beide lijsten te worden opgenomen, regelingen voor gemeenschappelijke rapportage van de EU en de VS over de sector, gemeenschappelijk toezicht, gemeenschappelijke zorgvuldigheidsverplichtingen voor verkopers en de strafbaarstelling van de verkoop van spyware aan niet-overheidsactoren;

68. verzoekt de Handels- en Technologieraad EU-VS breed en openlijk overleg te plegen met het maatschappelijk middenveld over de ontwikkeling van de gezamenlijke strategie en normen van de EU en de VS, met inbegrip van de gezamenlijke witte en/of zwarte lijst;

69. dringt aan op onderhandelingen met andere landen, met name Israël, om een kader voor het in de handel brengen van spyware en uitvoervergunningen vast te stellen, met inbegrip van regels inzake transparantie, een lijst van in aanmerking komende landen met betrekking tot mensenrechtennormen en zorgvuldigheidsregelingen;

70. merkt op dat in vergelijking met de VS, waar NSO snel op de zwarte lijst werd geplaatst en de president van de VS een presidentieel besluit heeft ondertekend waarin staat dat het bedrijf geen operationeel gebruik mag maken van commerciële spyware die significante contra-inlichtingen of veiligheidsrisico's voor de regering van de Verenigde Staten oplevert of significante risico's van oneigenlijk gebruik door een buitenlandse regering of een buitenlandse persoon, op EU-niveau niet voldoende is opgetreden wat

betreft de invoer van spyware en de handhaving van de exportregels;

71. concludeert dat de uitvoerregels van de Unie en de handhaving daarvan moeten worden versterkt met het oog op de bescherming van de mensenrechten in niet-EU-landen en dat deze regels moeten worden voorzien van de nodige instrumenten om de bepalingen ervan doeltreffend uit te voeren; herinnert eraan dat de EU samen met de VS en andere bondgenoten moet trachten de handel in spyware te reguleren en hun gecombineerde marktmacht moet gebruiken om veranderingen af te dwingen en strenge normen vast te stellen voor transparantie, traceerbaarheid en verantwoordingsplicht voor het gebruik van surveillancetechnologie, hetgeen moet uitmonden in een initiatief op het niveau van de Verenigde Naties;

Zeroday-kwetsbaarheden

72. dringt aan op een regeling voor het opsporen, delen, herstellen en exploiteren van kwetsbaarheden, alsmede van de openbaarmakingsprocedures, en vult daarmee de in Richtlijn (EU) 2022/2555[34] (NIS 2-richtlijn) en het voorstel voor de verordening cyberweerbaarheid[35] vastgestelde basis aan;

73. is van mening dat onderzoekers kwetsbaarheden moeten kunnen onderzoeken en hun resultaten moeten kunnen delen zonder civiele en strafrechtelijke aansprakelijkheid uit hoofde van onder meer de richtlijn cybercriminaliteit en de auteursrechtenrichtlijn;

74. roept de belangrijkste spelers uit de sector op om onderzoekers te stimuleren deel te nemen aan kwetsbaarheidsonderzoek, door te investeren in kwetsbaarheidsbehandelingsplannen en in openbaarmakingspraktijken binnen de sector en het maatschappelijk middenveld, en om “bug bounty”-programma’s uit te voeren;

75. verzoekt de Commissie haar steun en financiering te verhogen voor zogeheten bug bounties (premies voor het opsporen van programmeerfouten) en andere projecten die zich richten op het zoeken naar en herstellen van kwetsbaarheden op het gebied van veiligheid, en een gecoördineerde aanpak van verplichte openbaarmaking van kwetsbaarheden op te zetten tussen de lidstaten;

76. vraagt om een verbod op de verkoop van kwetsbaarheden in een systeem voor andere doeleinden dan het versterken van de veiligheid van dat systeem, en een verplichting om de bevindingen van al het onderzoek naar kwetsbaarheden bekend te maken op een gecoördineerde en verantwoorde wijze die de openbare veiligheid bevordert en het risico van uitbuiting van de kwetsbaarheid tot een minimum beperkt;

77. vraagt openbare en particuliere entiteiten een openbaar toegankelijk contactpunt op te zetten waar kwetsbaarheden op gecoördineerde en verantwoorde wijze kunnen worden gemeld en verzoekt organisaties die informatie over kwetsbaarheden in hun systeem

[34] Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972, en tot intrekking van Richtlijn (EU) 2016/1148, PB L 333 van 27.12.2022, blz. 80.

[35] Voorstel van 15 september 2022 voor een verordening van het Europees Parlement en de Raad betreffende horizontale cyberbeveiligingseisen voor producten met digitale bestanddelen, en tot wijziging van Verordening (EU) 2019/1020 (COM(2022) 0454).

ontvangen, onmiddellijk op te treden om deze te verhelpen; is van mening dat, wanneer een patch beschikbaar is, organisaties moeten worden verplicht om passende maatregelen te nemen om een snelle en gegarandeerde toepassing te waarborgen als onderdeel van een gecoördineerd en verantwoord openbaarmakingsproces;

78. is van mening dat de lidstaten voldoende financiële, technische en personele middelen moeten uittrekken voor veiligheidsonderzoek en het herstellen van kwetsbaarheden;

79. verzoekt de lidstaten bij wet voorgeschreven "vulnerabilities equities"-processen te ontwikkelen, waarin wordt bepaald dat kwetsbaarheden standaard openbaar moeten worden gemaakt en niet mogen worden uitgebuit, en dat elk besluit om hiervan af te wijken een uitzondering moet zijn en moet worden getoetst aan de eisen van noodzakelijkheid en evenredigheid, met inbegrip van de overweging of de door de kwetsbaarheid getroffen infrastructuur door een groot deel van de bevolking wordt gebruikt, en moet worden onderworpen aan strikt toezicht door een onafhankelijke toezichthoudende instantie, alsmede aan transparante procedures en besluiten;

Telecomnetwerken

80. wijst erop dat de vergunning van elke dienstverlener die onrechtmatige toegang tot nationale en/of internationale mobiele signaleringsinfrastructuur voor alle generaties (momenteel 2G tot en met 5G) faciliteert, moet worden ingetrokken;

81. benadrukt dat de processen waarmee nieuwe telefoonnummers uit de hele wereld kunnen worden gecreëerd door kwaadwillige actoren, beter moeten worden gereguleerd zodat het moeilijker wordt om illegale activiteiten te verbergen;

82. wijst erop dat telecomaanbieders ervoor moeten zorgen dat zij de capaciteit hebben om potentieel misbruik van toegang tot, controle op of daadwerkelijk eindgebruik van signaleringsinfrastructuur door derden via commerciële of andere overeenkomsten in de lidstaat waar zij actief zijn, op te sporen;

83. verzoekt de lidstaten ervoor te zorgen dat de bevoegde nationale autoriteiten, overeenkomstig de bepalingen van de NIS 2-richtlijn, evalueren in hoeverre telecomaanbieders bestand zijn tegen ongeoorloofde inbraken;

84. verzoekt telecomaanbieders krachtige en aantoonbare maatregelen te nemen tegen de verschillende vormen van het zonder toestemming nabootsen van de herkomst van telecomverkeer door een netwerkelement om toegang te krijgen tot gegevens of diensten die voor de legitieme gebruiker bestemd waren, en andere activiteiten waarbij de normale activiteiten van mobiele netwerkelementen en infrastructuur worden gemanipuleerd voor surveillancedoeleinden door kwaadwillige actoren, waaronder actoren op staatsniveau en criminele groepen;

85. verzoekt de lidstaten maatregelen te nemen om ervoor te zorgen dat overheidsactoren van buiten de EU die de grondrechten niet eerbiedigen, geen controle op of daadwerkelijk eindgebruik hebben van strategische infrastructuur en geen invloed hebben op besluiten in verband met strategische infrastructuur binnen de Unie, met inbegrip van telecommunicatie-infrastructuur;

86. verzoekt alle lidstaten prioriteit te geven aan meer investeringen in de bescherming van kritieke infrastructuur, zoals nationale telecommunicatiesystemen, om lacunes in de bescherming tegen inbreuken op de persoonlijke levenssfeer, het uitlekken van gegevens en ongeoorloofde inbraken aan te pakken, teneinde de grondrechten van de burgers te verdedigen;

87. verzoekt de bevoegde nationale autoriteiten zich actief in te zetten voor de versterking van de capaciteiten van providers, alsmede van de reactiecapaciteiten, om de identificatie van personen die illegaal doelwit zijn geworden, de meldingen en de incidentenmelding beter te ondersteunen, teneinde permanente, meetbare zekerheid te bieden en de uitbuiting van lacunes in de beveiliging door kwaadwillende actoren van buiten en binnen de EU te beperken;

E-privacy

88. dringt aan op de snelle goedkeuring van de e-privacyverordening op een wijze die volledig aansluit bij de jurisprudentie inzake de beperkingen voor de nationale veiligheid en de noodzaak om het misbruik van surveillancetechnologieën te voorkomen, en die het grondrecht op privacy versterkt en voorziet in sterke waarborgen en effectieve handhaving; wijst erop dat de reikwijdte van de rechtmatige onderschepping niet verder mag gaan dan de e-privacyrichtlijn (Richtlijn 2002/58/EG);

89 dringt aan op de bescherming van alle elektronische communicatie, inhoud en metagegevens tegen misbruik van persoonsgegevens en privécommunicatie door particuliere bedrijven en overheidsinstanties; wijst erop dat digitale hulpmiddelen voor ingebouwde veiligheid, zoals end-to-endencryptie, niet mogen worden verzwakt;

90. verzoekt de Commissie de uitvoering van de e-privacyrichtlijn door de lidstaten in de hele EU te beoordelen en inbreukprocedures in te leiden wanneer zich schendingen voordoen;

De rol van Europol

91. merkt op dat de PEGA-commissie in een brief van Europol van april 2023 aan de voorzitter van de commissie op de hoogte wordt gebracht van het feit dat Europol contact heeft opgenomen met Griekenland, Hongarije, Bulgarije, Spanje en Polen om na te gaan of er strafrechtelijke onderzoeken of andere onderzoeken lopen of gepland zijn op grond van de toepasselijke bepalingen van nationaal recht dat door Europol kan worden ondersteund; benadrukt dat het verlenen van bijstand aan de lidstaten niet neerkomt op het instellen, voeren of coördineren van een strafrechtelijk onderzoek als bedoeld in artikel 6;

92. verzoekt Europol ten volle gebruik te maken van zijn nieuwe bevoegdheden uit hoofde van artikel 6, lid 1 bis van Verordening (EU) 2022/991, op grond waarvan Europol de bevoegde autoriteiten van de betrokken lidstaten in voorkomend geval kan voorstellen een onderzoek in te stellen, uit te voeren of te coördineren; wijst erop dat het krachtens artikel 6 aan de lidstaten is om een dergelijk voorstel te verwerpen;

93. verzoekt alle lidstaten zich er ten aanzien van het Europees Parlement en de Raad toe te verplichten om Europol te betrekken bij onderzoeken naar beschuldigingen van

onrechtmatig gebruik van spyware op nationaal niveau, met name wanneer een voorstel uit hoofde van artikel 6, lid 1 bis, van Verordening (EU) nr. 2022/991 is gedaan;

94. verzoekt de lidstaten om binnen Europol een register op te zetten van nationale rechtshandhavingsoperaties waarbij gebruik wordt gemaakt van spyware en waarin elke operatie moet worden aangemerkt met een code, en het gebruik van spyware door regeringen op te nemen in de jaarlijkse dreigingsevaluatie van de georganiseerde internetcriminaliteit van Europol;

95. is van mening dat er moet worden nagedacht over de rol van Europol in gevallen waarin de nationale autoriteiten falen of weigeren onderzoek te doen en er duidelijke bedreigingen zijn voor de belangen en de veiligheid van de EU;

Ontwikkelingsbeleid van de Unie

96. verzoekt de Commissie en de EDEO striktere controlemechanismen in te voeren om ervoor te zorgen dat met de ontwikkelingshulp van de Unie, met inbegrip van de donatie van surveillancetechnologie en opleiding in het gebruik van surveillancesoftware, geen instrumenten en activiteiten worden gefinancierd of gefaciliteerd die afbreuk kunnen doen aan de beginselen van democratie, goed bestuur, de rechtsstaat en eerbiediging van de mensenrechten, of die een bedreiging vormen voor de internationale veiligheid of de essentiële veiligheid van de Unie en haar leden; merkt op dat de beoordeling door de Commissie van de naleving van het Unierecht, met name het Financieel Reglement, specifieke controlecriteria en handhavingsmechanismen moet bevatten om dergelijk misbruik te voorkomen, met inbegrip van de mogelijke tijdelijke opschorting van specifieke projecten indien een inbreuk op deze beginselen wordt geconstateerd;

97. verzoekt de Commissie en de EDEO om in elke effectbeoordeling voor de mensenrechten en de grondrechten een controleprocedure op te nemen inzake mogelijk misbruik van surveillance, die ten volle rekening houdt met artikel 51 van het Handvest van de grondrechten en wel binnen één jaar [na de publicatie van de aanbevelingen van PEGA]; wijst erop dat deze procedure aan het Parlement en de Raad moet worden voorgelegd en dat deze effectbeoordeling moet worden uitgevoerd voordat steun aan niet-EU-landen wordt verleend;

98. verzoekt de EDEO om in het jaarverslag van de EU over mensenrechten en democratie verslag uit te brengen over het misbruik van spyware tegen mensenrechtenverdedigers;

Financiële regels van de Unie

99. benadrukt dat de eerbiediging van de mensenrechten door de financiële sector moet worden verbeterd; benadrukt dat de “UNGP 10+”-aanbevelingen moeten worden omgezet in Unierecht en dat de zorgvuldigheidsrichtlijn volledig van toepassing moet zijn op de financiële sector, teneinde de eerbiediging van de democratie, de mensenrechten en de rechtsstaat in de financiële sector te waarborgen;

100. is bezorgd over de gevolgen van het besluit van het HvJ-EU met betrekking tot Richtlijn (EU) 2018/843 inzake de voorkoming van het gebruik van het financiële

stelsel voor het witwassen van geld of terrorismefinanciering[36], waarbij informatie over de uiteindelijk begunstigden van vennootschappen en juridische entiteiten die zijn opgenomen in een nationaal publiek toegankelijk register van uiteindelijk begunstigden (UBO) ongeldig is verklaard[37]; wijst erop dat de toekomstige richtlijn, rekening houdend met het arrest van het HvJ-EU, een zo groot mogelijke openbaarheid mogelijk moet maken, zodat het moeilijker wordt om aankopen of verkopen van spyware via gelieerde personen en makelaars te verbergen;

Follow-up van de resoluties van het Parlement

101. pleit voor de dringende follow-up van zijn resolutie van 12 maart 2014 over het surveillanceprogramma van de NSA in de VS, toezichthoudende instanties in verschillende lidstaten en gevolgen voor de grondrechten van EU-burgers en voor de trans-Atlantische samenwerking op het gebied van justitie en binnenlandse zaken; benadrukt dat de aanbevelingen daarin dringend moeten worden uitgevoerd;

102. wijst erop dat, ondanks het feit dat het toezicht op de activiteiten van de inlichtingendiensten gebaseerd moet zijn op zowel democratische legitimiteit (sterk rechtskader, toestemming vooraf en verificatie achteraf) als adequate technische capaciteit en deskundigheid; de meeste van de huidige toezichthoudende instanties in de EU en de VS een dramatisch tekort aan beide hebben, met name aan technische capaciteit;

103. verzoekt, zoals het in het geval van Echelon heeft gedaan, alle nationale parlementen die dit nog niet hebben gedaan doelmatig toezicht op inlichtingenactiviteiten door parlementsleden of deskundigenorganen met wettelijke onderzoeksbevoegdheden in te stellen; verzoekt de nationale parlementen ervoor te zorgen dat deze toezichtscommissies/-organen over voldoende middelen, technische deskundigheid en juridische middelen, waaronder het recht om controles ter plaatse te verrichten, beschikken om doeltreffend toezicht uit te kunnen oefenen op inlichtingendiensten;

104. pleit voor de oprichting van een groep op hoog niveau die op transparante wijze en in samenwerking met de parlementen aanbevelingen zou moeten uitbrengen voor nadere stappen die moeten worden genomen voor verscherpt democratisch toezicht, ook parlementair toezicht, op inlichtingendiensten, en voor nauwere samenwerking op het gebied van toezicht in de EU, met name ten aanzien van de grensoverschrijdende dimensie;

105. stelt dat deze groep op hoog niveau:

a) bindende Europese minimumnormen of richtsnoeren inzake toezicht vooraf en achteraf op inlichtingendiensten moet vaststellen op grond van bestaande goede praktijken en aanbevelingen van internationale organen, zoals de VN en de Raad van Europa, met inbegrip van de kwestie dat toezichtsorganen als derde partij worden beschouwd, volgens de derdepartijregel of het beginsel van de controle door afzender, met het oog op de controleerbaarheid en de verantwoording van inlichtingen uit derde landen;

[36] Arrest van 22 november 2022, gevoegde zaken C-37/20 en C-601/20, EU:C:2022:912.
[37] HvJ-EU. Persbericht nr. 188/22, arrest van het Hof in de gevoegde zaken C-37/20 en C-601/20.

b) criteria voor een grotere transparantie moet ontwikkelen, voortbouwend op het algemene beginsel van toegang tot informatie en de zogenaamde Tshwane-beginselen[38];

106. is voornemens om een conferentie met nationale toezichtsorganen, zowel parlementaire als onafhankelijke, te organiseren;

107. roept de lidstaten op voort te bouwen op hun goede praktijken om de toegang van hun toezichtsorganen tot informatie over inlichtingenactiviteiten, waaronder begrepen gerubriceerde informatie en informatie van andere diensten, te verbeteren en te voorzien in de bevoegdheid om bezoeken ter plaatse te brengen, een solide pakket bevoegdheden voor verhoor, adequate middelen en technische deskundigheid, strikte onafhankelijkheid ten opzichte van hun regering en een rapportageverplichting jegens hun parlement;

108. roept de lidstaten op samenwerking tussen toezichtsorganen te ontwikkelen;

109. roept de Commissie op een voorstel in te dienen voor een veiligheidsmachtigingsprocedure van de Unie voor alle beklеders van een openbaar ambt in de Unie, aangezien het huidige systeem, dat gebaseerd is op de door de lidstaat van herkomst uitgevoerde veiligheidsmachtiging, voorziet in verschillende vereisten en lengtes van de procedures binnen de nationale systemen, en zodoende leidt tot een verschillende behandeling van Parlementsleden en hun personeel al naargelang hun nationaliteit;

110. herinnert aan de bepalingen van de interinstitutionele overeenkomst tussen het Europees Parlement en de Raad betreffende het doorzenden aan en verwerken door het Europees Parlement van gerubriceerde informatie waarover de Raad beschikt met betrekking tot aangelegenheden die niet vallen onder het gemeenschappelijk buitenlands en veiligheidsbeleid, die moeten worden gebruikt om het toezicht op EU-niveau te verbeteren;

Onderzoeksprogramma's van de Unie

111. pleit voor de invoering van strengere en doeltreffendere controlemechanismen om ervoor te zorgen dat de onderzoeksfondsen van de Unie geen instrumenten financieren of faciliteren, met inbegrip van spyware en surveillance-instrumenten, die indruisen tegen de waarden van de EU; merkt op dat de beoordeling door de Commissie van de naleving van het Unierecht specifieke controlecriteria moet bevatten om dergelijk misbruik te voorkomen; dringt aan op de stopzetting van onderzoeksfondsen van de Unie aan entiteiten die betrokken zijn of zijn geweest bij de directe of indirecte facilitering van mensenrechtenschendingen met surveillance-instrumenten;

112. benadrukt het feit dat EU-financiering voor onderzoek, zoals de Horizon Europa-overeenkomsten met niet-EU-landen, niet mag worden gebruikt om bij te dragen aan de ontwikkeling van spyware en gelijkwaardige technologieën;

[38] The Global Principles on National Security and the Right to Information (Mondiale beginselen betreffende nationale veiligheid en het recht op informatie), juni 2013.

Technologielaboratorium van de EU

113. verzoekt de Commissie onverwijld een begin te maken met de oprichting van een onafhankelijk geleid Europees interdisciplinair onderzoeksinstituut dat zich richt op onderzoek en ontwikkeling op het gebied van informatie- en communicatietechnologie, grondrechten en veiligheid; wijst erop dat dit instituut moet samenwerken met deskundigen, academici en vertegenwoordigers van het maatschappelijk middenveld, en openstaan voor deelname van deskundigen en instellingen van de lidstaten;

114. wijst erop dat het instituut zou bijdragen tot een betere bewustwording, attributie en aflegging van verantwoording in en buiten Europa, en tot een bredere Europese talentenbasis en een beter inzicht in de wijze waarop spywareverkopers hun diensten ontwikkelen, onderhouden, verkopen en leveren aan derden;

115. is van mening dat het instituut tot taak moet krijgen het onwettige gebruik van software voor illegale surveillancedoeleinden op te sporen en aan het licht te brengen, toegankelijke en gratis juridische en technologische ondersteuning te bieden, met inbegrip van smartphonescreenings voor personen die vermoeden dat zij het doelwit zijn van spyware en de instrumenten die nodig zijn om spyware op te sporen, forensisch analytisch onderzoek te verrichten voor gerechtelijke onderzoeken en regelmatig verslag uit te brengen over het gebruik en misbruik van spyware in de EU, rekening houdend met technologische updates; is van mening dat dit verslag jaarlijks beschikbaar moet worden gesteld en aan de Commissie, het Parlement en de Raad moet worden toegezonden;

116. beveelt de Commissie aan het technologielaboratorium van de EU op te zetten in nauwe samenwerking met het computercrisisresponsteam voor de instellingen, organen en instanties van de Europese Unie (CERT-EU) en Enisa, en bij de oprichting van het technologielaboratorium van de EU overleg te plegen met relevante deskundigen om te leren van de beste praktijken op academisch gebied;

117. benadrukt dat het van belang is te zorgen voor passende financiering voor het technologielaboratorium van de EU;

118. beveelt de Commissie aan een certificeringsregeling voor te stellen voor de analyse en authenticatie van forensisch materiaal;

119. verzoekt de Commissie de capaciteit van het maatschappelijk middenveld wereldwijd te ondersteunen teneinde de weerbaarheid tegen spyware-aanvallen en de verlening van bijstand en diensten aan burgers te versterken;

De rechtsstaat

120. benadrukt dat de gevolgen van het onrechtmatige gebruik van spyware veel duidelijker zijn in lidstaten waar de autoriteiten die gewoonlijk belast zijn met onderzoek, het bieden van verhaal aan personen die doelwit zijn en het waarborgen van de verantwoordingsplicht, door de staat worden gegijzeld en dat wanneer er sprake is van een rechtsstaatcrisis en de onafhankelijkheid van de rechterlijke macht in gevaar is, geen beroep kan worden gedaan op de nationale autoriteiten;

121. verzoekt de Commissie daarom te zorgen voor een effectieve uitvoering van haar instrumentarium voor de rechtsstaat, met name door:

a) een uitgebreidere monitoring van de rechtsstaat in te voeren, met inbegrip van landspecifieke aanbevelingen in verband met het onrechtmatige gebruik van spyware door de lidstaten in het jaarlijks verslag over de rechtsstaat van de Commissie, met een beoordeling van de mate waarin overheidsinstellingen bereid zijn verhaal te bieden aan personen die doelwit zijn, en door het toepassingsgebied van haar jaarverslag over de rechtsstaat te verruimen en er alle uitdagingen voor de democratie, de rechtsstaat en de grondrechten in op te nemen, zoals opgenomen in artikel 2 VEU, zoals herhaaldelijk gevraagd door het Parlement;

b) proactief inbreukprocedures te starten en te bundelen tegen lidstaten wegens tekortkomingen op het gebied van de rechtsstaat, zoals bedreigingen voor de onafhankelijkheid van de rechterlijke macht en de doeltreffende werking van de politie en het openbaar ministerie, in het kader van de samenwerking van politie en justitie in strafzaken;

Uniefonds voor geschillen

122. dringt aan op de oprichting, zonder onnodige vertraging, van een Uniefonds voor geschillenbeslechting om de werkelijke proceskosten te dekken en de personen die doelwit zijn van spyware in staat te stellen passende schadeloosstelling te eisen, met inbegrip van een vergoeding voor het onrechtmatige gebruik van spyware tegen hen, in overeenstemming met de voorbereidende actie die het Parlement in 2017 heeft vastgesteld, om een “EU-fonds voor financiële steun voor het procederen in zaken die verband houden met schendingen van de democratie, rechtsstaat en grondrechten” in het leven te roepen;

EU-instellingen

123. uit zijn bezorgdheid over het gebrek aan maatregelen van de Commissie tot dusver en dringt er bij de Commissie op aan ten volle gebruik te maken van al haar bevoegdheden als hoedster van de Verdragen en een uitgebreid en diepgaand onderzoek in te stellen naar het misbruik van en de handel in spyware in de Unie;

124. dringt er bij de Commissie op aan een uitgebreid onderzoek in te stellen naar alle beschuldigingen en vermoedens van het gebruik van spyware tegen haar ambtenaren, en waar nodig verslag uit te brengen aan het Parlement en aan de verantwoordelijke rechtshandhavingsinstanties;

125. verzoekt de Commissie een speciale taskforce op te richten, met medewerking van de nationale kiescommissies, voor de bescherming van de Europese verkiezingen van 2024 in de hele Unie; herinnert eraan dat niet alleen buitenlandse, maar ook interne inmenging een bedreiging vormt voor de Europese verkiezingsprocessen; wijst erop dat bij misbruik van pervasieve surveillance-instrumenten, zoals Pegasus, de verkiezingen in het gedrang kunnen komen;

126. merkt op dat de commissie PEGA pas vlak voor de publicatie van het ontwerpverslag, ongeveer vier maanden nadat het Parlement brieven had verzonden, een collectief

antwoord van de Raad heeft ontvangen op de vragen van het Europees Parlement aan alle afzonderlijke lidstaten; spreekt zijn afkeuring uit over het gebrek aan actie van de Europese Raad en de Raad van Ministers, en dringt aan op een speciale top van de Europese Raad, gezien de omvang van de bedreiging voor de democratie in Europa;

127. verzoekt de Raad van de EU ontwikkelingen in verband met het gebruik van spyware en de gevolgen daarvan voor de in artikel 2 VEU verankerde waarden te behandelen in het kader van hoorzittingen op grond van artikel 7, lid 1, VEU;

128. is van mening dat het Parlement over volledige onderzoeksbevoegdheden moet beschikken, met inbegrip van betere toegang tot gerubriceerde en niet-gerubriceerde informatie, de bevoegdheid om getuigen op te roepen, hen formeel te verplichten onder ede te getuigen en de gevraagde informatie binnen specifieke termijnen te verstrekken; herhaalt het standpunt van het Parlement in zijn voorstel van 23 mei 2012 voor een verordening van het Europees Parlement tot vaststelling van de wijze van uitoefening van het enquêterecht van het Europees Parlement en tot intrekking van Besluit 95/167/EG, Euratom, EGKS van het Europees Parlement, de Raad en de Commissie[39]; verzoekt de Raad onmiddellijk maatregelen te nemen met betrekking tot dit voorstel voor een verordening om het Europees Parlement een passend enquêterecht te bieden;

129. erkent de inspanningen van het Parlement om spyware-infecties op te sporen; is evenwel van mening dat de bescherming van het personeel moet worden versterkt, rekening houdend met de voorrechten en immuniteiten van bespioneerden; herinnert eraan dat elke aanval op de politieke rechten van de leden een aanval is op de onafhankelijkheid en soevereiniteit van de instelling, alsook een aanval op de rechten van de kiezer;

130. verzoekt het Bureau van het Parlement een protocol vast te stellen voor gevallen waarin leden of personeelsleden van het Parlement direct of indirect doelwit van spyware zijn geworden en onderstreept dat alle gevallen door het Parlement moeten worden gemeld aan de verantwoordelijke rechtshandhavingsinstanties; wijst erop dat het Parlement in dergelijke gevallen juridische en technische bijstand moet verlenen;

131. besluit het initiatief te nemen om een interinstitutionele conferentie te organiseren waarin het Parlement, de Raad en de Commissie streven naar bestuurshervormingen die de institutionele capaciteit van de Unie versterken om adequaat te reageren op aanvallen op de democratie en de rechtsstaat van binnenuit en ervoor te zorgen dat de Unie beschikt over doeltreffende supranationale methoden om de Verdragen en het afgeleide recht te handhaven in geval van niet-naleving door de lidstaten;

132. dringt aan op de spoedige goedkeuring van het voorstel van de Commissie voor een verordening van het Europees Parlement en de Raad betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de instellingen, organen en instanties van de Unie (COM(2022)0122) en op snelle uitvoering en strikte handhaving daarna, om het risico op spyware-infecties van apparaten en systemen die door personeel en politici van de EU-instellingen worden gebruikt, te verminderen;

[39] PB C 264 E van 13.9.2013, blz. 41.

133. dringt erop aan dat de EU Verdrag 108+ ondertekent;

134. verzoekt de Europese Ombudsman om binnen het Europees netwerk van ombudsmannen besprekingen op gang te brengen over de gevolgen van misbruik van wijdverbreid toezicht op democratische processen en burgerrechten; verzoekt het netwerk aanbevelingen te ontwikkelen over doeltreffende en zinvolle verhaalmiddelen in de hele EU;

Wetgevende maatregelen

135. verzoekt de Commissie onverwijld met wetgevingsvoorstellen te komen op basis van deze aanbeveling;

°

° °

136. verzoekt zijn Voorzitter deze resolutie te doen toekomen aan de lidstaten, de Raad, de Commissie en Europol.