Parlamentul European
2019-2024

Document de ședință

B9-0260/2023

22.5.2023

PROIECT DE RECOMANDARE A PARLAMENTULUI EUROPEAN ADRESATĂ CONSILIULUI ȘI COMISIEI

depus în conformitate cu articolul 208 alineatul (12) din Regulamentul de procedură

în urma anchetei privind presupusele încălcări și deficiențe administrative în aplicarea legislației Uniunii în legătură cu utilizarea programului Pegasus și a altor programe de spionaj echivalente
(2023/2500(RSP))

Sophie in ‘t Veld
în numele Comisiei de anchetă pentru examinarea utilizării Pegasus și a altor programe de spionaj echivalente

B9-0260/2023

Proiect de recomandare a Parlamentului European adresată Consiliului și Comisiei în urma anchetei privind presupusele încălcări și deficiențe administrative în aplicarea legislației Uniunii în legătură cu utilizarea programului Pegasus și a altor programe de spionaj echivalente (2023/2500(RSP))

Parlamentul European,

– având în vedere Tratatul privind Uniunea Europeană (TUE), în special articolele 2, 4, 6 și 21,

– având în vedere articolele 16, 223, 225 și 226 din Tratatul privind funcționarea Uniunii Europene (TFUE),

– având în vedere Carta Drepturilor Fundamentale a Uniunii Europene (Carta), în special articolele 7, 8, 11, 17, 21, 41, 42 și 47,

– având în vedere Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice[1] (Directiva asupra confidențialității și comunicațiilor electronice),

– având în vedere Regulamentul (UE) 2016/679 al Parlamentului și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor)[2],

– având în vedere Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului[3],

– având în vedere Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului[4] (Directiva privind criminalitatea informatică),

– având în vedere Regulamentul (UE) 2021/821 al Parlamentului European și al Consiliului din 20 mai 2021 de instituire a unui regim al Uniunii pentru controlul exporturilor, serviciilor de intermediere, asistenței tehnice, tranzitului și transferului de produse cu dublă utilizare[5] (Regulamentul privind produsele cu dublă utilizare),

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

– având în vedere Decizia (PESC) 2019/797 a Consiliului din 17 mai 2019 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre[6], astfel cum a fost modificată de Decizia (PESC) 2021/796 a Consiliului din 17 mai 2021[7],

– având în vedere Actul privind alegerea membrilor Parlamentului European prin vot universal direct[8],

– având în vedere Decizia 95/167/CE, Euratom, CECO a Parlamentului European, a Consiliului și a Comisiei din 6 martie 1995 privind modalitățile detaliate de exercitare a dreptului de anchetă al Parlamentului European[9],

– având în vedere Decizia (UE) 2022/480 a Parlamentului European din 10 martie 2022 privind constituirea, responsabilitățile, componența numerică și durata mandatului Comisiei de anchetă însărcinate cu examinarea utilizării Pegasus și a unor programe spion de supraveghere echivalente[10],

– având în vedere Directiva (UE) 2018/843 a Parlamentului European și a Consiliului din 30 mai 2018 de modificare a Directivei (UE) 2015/849 privind prevenirea utilizării sistemului financiar în scopul spălării banilor sau finanțării terorismului, precum și de modificare a Directivelor 2009/139/CE și 2013/36/UE[11] (Directiva privind combaterea spălării banilor),

– având în vedere propunerea de regulament al Parlamentului European și al Consiliului 16 septembrie 2022 de stabilire a unui cadru comun pentru serviciile mass-media în cadrul pieței interne (Legea europeană privind libertatea mass-mediei) și de modificare a Directivei 2010/13/UE (COM(2022)0457),

– având în vedere articolul 12 din Declarația universală a drepturilor omului,

– având în vedere Hotărârea Curții de Justiție a Uniunii Europene (CJUE) în cauza C-37/20[12] referitoare la Directiva privind combaterea spălării banilor, dispoziția care prevede ca informațiile ce privesc beneficiarii reali ai entităților corporative înregistrate pe teritoriul statelor membre să fie accesibile în toate cazurile oricărui membru al publicului larg este nevalidă,

– având în vedere articolul 17 din Pactul internațional cu privire la drepturile civile și politice,

– având în vedere Carta Organizației Națiunilor Unite și Principiile directoare ale

[6] JO L 129 I, 17.5.2019, p. 13.
[7] JO L 174 I, 18.5.2021, p. 1.
[8] JO L 278, 8.10.1976, p. 5.
[9] JO L 113, 19.5.1995, p. 1.
[10] JO L 98, 25.3.2022, p. 72.
[11] JO L 156, 19.6.2018, p. 43–74.
[12] Hotărârea Curții (Marea Cameră) din 22 noiembrie 2022, C-37/20, WM și Sovim SA/Luxemburg Business Registers, EU:C:2022:912.

Organizației Națiunilor Unite privind afacerile și drepturile omului[13],

– având în vedere declarația Înaltului Comisar al ONU pentru Drepturile Omului, Michelle Bachelet, din 19 iulie 2022 privind „Utilizarea programelor spion pentru supravegherea jurnaliștilor și a apărătorilor drepturilor omului”,

– având în vedere declarația comisarei Consiliului Europei pentru Drepturile Omului, Dunja Mijatović, din 27 ianuarie 2023, intitulată „Programele spion extrem de intruzive pun în pericol esența drepturilor omului”[14],

– având în vedere observațiile preliminare ale Autorității Europene pentru Protecția Datelor (AEPD) din 15 februarie 2022 privind programele spion moderne[15],

– având în vedere Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale, în special articolele 8, 10, 13, 14 și 17 și protocoalele la convenție,

– având în vedere Evaluarea Europol din 2021 a amenințării pe care o reprezintă formele grave de criminalitate și criminalitatea organizată (SOCTA), intitulată „A Corrupting Influence: the Infiltration and Undermining of Europe’s Economy and Society by Organised Crime” (O influență care corupe: infiltrarea criminalității organizate în economia și societatea europene și subminarea acestora),

– având în vedere raportul din 2017 al Agenției pentru Drepturi Fundamentale a Uniunii Europene (FRA) intitulat „Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU” (Supravegherea de către serviciile de informații: garanții și căi de atac privind drepturile fundamentale în UE) și actualizările prezentate la 28 februarie 2023 Comisiei de anchetă pentru examinarea utilizării Pegasus și a altor programe de spionaj echivalente (PEGA),

– având în vedere rezoluția sa din 12 martie 2014 referitoare la programul de supraveghere al Agenției Naționale de Securitate (NSA) a SUA, la organismele de supraveghere din diferite state membre și la impactul acestora asupra drepturilor fundamentale ale cetățenilor UE și asupra cooperării transatlantice în materie de justiție și de afaceri interne[16] și mai ales recomandările incluse în aceasta privind consolidarea securității informatice în instituțiile, organele și agențiile UE,

– având în vedere avizul AEPD 24/2022 din 11 noiembrie 2022 referitor la Legea europeană privind libertatea mass-mediei,

– având în vedere glosarul privind programele rău-intenționate și programele spion realizat de Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA),

– având în vedere Decizia Ombudsmanului European privind modul în care Comisia Europeană a evaluat impactul asupra drepturilor omului înainte de a oferi țărilor africane sprijin pentru dezvoltarea capacităților de supraveghere (cauza

[13] https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf
[14] https://www.coe.int/en/web/commissioner/-/highly-intrusive-spyware-threatens-the-essence-of-human-rights
[15] https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf
[16] JO C 378, 9.11.2017, p. 104.

1904/2021/MHZ),

– având în vedere declarația din 2 februarie 2023 a doamnei Irene Khan, raportoare specială a ONU privind libertatea de opinie și de exprimare, și a domnului Fernand de Varennes, raportor special al ONU pentru chestiuni legate de minorități, prin care se solicită o anchetă asupra presupusului program de spionaj care vizează liderii catalani[17],

– având în vedere raportul Comisiei pentru democrație prin drept (Comisia de la Veneția) privind supravegherea democratică a serviciilor de securitate[18] și avizul său intitulat „Polonia - Aviz privind legea din 15 ianuarie 2016 de modificare a Legii privind poliția și a altor legi specifice”[19],

– având în vedere raportul Comisiei de anchetă pentru examinarea utilizării Pegasus și a altor programe de spionaj echivalente (A9-0189/2023),

– având în vedere articolul 208 alineatul (12) din Regulamentul său de procedură,

A. întrucât, datorită eforturilor CitizenLab și Amnesty Tech și ale multor jurnaliști de investigație, a fost dezvăluit faptul că organisme guvernamentale din mai multe țări, atât din state membre ale UE, cât și din țări din afara UE, au folosit Pegasus și programe spion echivalente împotriva jurnaliștilor, politicienilor, reprezentanților autorităților de aplicare a legii, diplomaților, avocaților, oamenilor de afaceri, actorilor societății civile și altor actori, în scopuri politice și chiar infracționale; întrucât astfel de practici sunt extrem de îngrijorătoare și demonstrează riscul folosirii abuzive a tehnologiilor de supraveghere pentru a submina drepturile fundamentale ale omului, democrația și procesele electorale;

B. întrucât, ori de câte ori sunt menționate în raport, cuvintele „program spion/program de spionaj” înseamnă „Pegasus și programe spion de supraveghere echivalente”, astfel cum sunt definite în decizia Parlamentului de înființare a Comisiei PEGA;

C. întrucât s-a observat că actorii statali au folosit în mod deliberat programe spion într-o manieră înșelătoare, recurgând la programe spion care se pot ascunde sub formă de program, fișier sau conținut legitim („troian”), cum ar fi mesaje false din partea unor instituții publice; întrucât în unele cazuri, autoritățile publice au folosit operatori de telefonie pentru a transmite conținut rău-intenționat pe dispozitivul persoanei vizate; întrucât programele spion pot fi utilizate prin exploatarea vulnerabilităților de ziua zero, fără interacțiunea țintei cu conținutul infectat, pot elimina toate urmele prezenței lor după dezinstalare și pot anonimiza legătura dintre operatorii de la distanță și server;

D. întrucât, la începutul comunicațiilor mobile, ascultarea conversațiilor avea loc prin interceptarea apelurilor și, ulterior, a mesajelor text în format simplu;

E. întrucât apariția aplicațiilor de comunicații mobile criptate a dus la emergența industriei programelor spion care profită de vulnerabilitățile existente în sistemele de operare ale telefoanelor inteligente cu scopul de a instala software care importă programe spion în

[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

telefon, infectându-le inclusiv fără a se face clic (zero-click), fără ca utilizatorul să știe sau să acționeze în vreun fel, permițând extragerea datelor înainte de criptare; întrucât, prin însăși concepția lor, aceste programe spion zero-click fac ca un control eficient și semnificativ al utilizării lor să fie foarte dificil;

F. întrucât cunoștințele despre vulnerabilitățile sistemelor software sunt tranzacționate direct între părți sau sunt facilitate de intermediari; întrucât aceste tranzacții includ actori nestatali și grupuri infracționale organizate;

G. întrucât achiziționarea, tranzacționarea și acumularea vulnerabilităților de ziua zero subminează fundamental integritatea și securitatea comunicațiilor și securității cibernetice a cetățenilor UE;

H. întrucât supravegherea prin programe spion ar trebui să rămână o excepție și să necesite întotdeauna o autorizație judiciară prealabilă eficace, obligatorie și semnificativă din partea unei autorități judiciare imparțiale și independente, care trebuie să se asigure că măsura este necesară și proporțională și se limitează strict la cazurile care afectează securitatea națională sau implică terorism și infracțiuni grave; întrucât tehnicile de supraveghere sunt susceptibile de a fi folosite abuziv în medii unde nu există un sistem de control și echilibru eficient;

I. întrucât orice supraveghere prin programe spion trebuie să fie verificată de o autoritate independentă de supraveghere ex post, care trebuie să se asigure că orice supraveghere autorizată este efectuată cu respectarea drepturilor fundamentale și în conformitate cu condițiile stabilite de CJUE, de Curtea Europeană a Drepturilor Omului (CEDO) și de Comisia de la Veneția; întrucât această autoritate de supraveghere ex post ar trebui să dispună imediat încetarea supravegherii dacă se constată că aceasta este incompatibilă cu drepturile și condițiile menționate mai sus;

J. întrucât supravegherea prin programe spion care nu îndeplinește cerințele prevăzute în dreptul Uniunii și în jurisprudența CJUE și a CEDO contravine valorilor consacrate la articolul 2 din TUE și drepturilor fundamentale consacrate în Cartă, în special la articolele 7, 8, 11, 17, 21 și 47, care recunosc drepturi, libertăți și principii specifice, cum ar fi respectarea vieții private și de familie, protecția datelor cu caracter personal, libertatea de exprimare și de informare, dreptul la proprietate, dreptul la nediscriminare, precum și dreptul la o cale de atac eficientă, la un proces echitabil și la prezumția de nevinovăție;

K. întrucât drepturile persoanelor vizate sunt prevăzute în Cartă și în convențiile internaționale, în special dreptul la viață privată și dreptul la un proces echitabil, precum și în normele Uniunii privind drepturile persoanelor suspectate și acuzate; întrucât aceste drepturi au fost confirmate de jurisprudența CJUE și a CEDO;

L. întrucât impactul supravegherii țintite asupra femeilor poate fi deosebit de grav, deoarece autoritățile pot utiliza controlul social sporit la care sunt supuse femeile pentru a folosi împotriva lor datele private și intime extrase cu ajutorul programelor spion pentru campanii de defăimare;

M. întrucât este clar din mărturiile persoanelor vizate că deși există pe hârtie, căile de atac și drepturile civile, devin în general nule în fața obstrucționării de către organismele

guvernamentale, a absenței sau a nepunerii în aplicare a dreptului persoanelor vizate de a fi informate și a obstacolelor administrative în calea demersului de a demonstra statutul de persoană vizată; întrucât chiar și în sisteme cu proceduri rapide și deschise, natura programelor spion face să fie foarte greu să se dovedească cine este autorul, natura situației și gradul în care o persoană a fost vizată;

N. întrucât instanțele nu au acceptat probele criminalistice ale experților independenți, ci doar probe bazate pe examinarea autorităților, a serviciilor de securitate sau a autorităților de aplicare a legii care se presupune că se află în spatele unui atac; întrucât acest lucru face ca persoanele vizate să se afle într-o situație paradoxală fără nicio opțiune viabilă de a dovedi o infectare cu programe spion;

O. întrucât guvernul polonez a slăbit și a eliminat garanțiile instituționale și juridice, inclusiv procedurile adecvate de supraveghere și control, lăsând efectiv persoanele vizate fără nicio cale de atac semnificativă; întrucât programul spion Pegasus a fost utilizat ilegal în scopuri politice pentru a spiona jurnaliști, politicieni din opoziție, avocați, procurori și actori ai societății civile;

P. întrucât guvernul ungar a slăbit și a eliminat garanțiile instituționale și juridice, inclusiv procedurile adecvate de supraveghere și control, lăsând efectiv persoanele vizate fără nicio cale de atac semnificativă; întrucât programul spion Pegasus a fost utilizat ilegal în scopuri politice pentru a spiona jurnaliști, politicieni din opoziție, avocați, procurori și actori ai societății civile;

Q. întrucât s-a confirmat oficial că un deputat în Parlamentul European (deputat în PE) din partea Greciei și un jurnalist grec au fost atât interceptați de Serviciul național elen de informații (EYP), cât și vizați de programul spion Predator; întrucât un fost angajat eleno-american al Meta a fost în același timp interceptat de EYP și vizat de programul spion Predator, a cărui utilizare este ilegală în temeiul legislației elene; întrucât potrivit relatărilor din mass-media, și deputați din opoziție și din partidul aflat la guvernare în Grecia, activiști de partid și jurnaliști au fost, se pare, vizați fie prin programul spion Predator, fie prin interceptarea convențională de către EYP sau prin ambele metode; întrucât guvernul elen neagă achiziționarea sau utilizarea Predator, însă este foarte probabil ca acesta să fi fost folosit de persoane foarte apropiate de cabinetul prim-ministrului sau în numele lor; întrucât guvernul elen a recunoscut că a acordat licențe de export companiei Intellexa pentru vânzarea programului spion Predator unor guverne represive, cum ar fi Madagascar și Sudan; întrucât guvernul a răspuns la scandal introducând modificări legislative care reduc și mai mult drepturile persoanelor vizate de a fi informate după ce a avut loc supravegherea și îngreunează și mai mult activitatea autorităților independente;

R. întrucât dezvăluirile au identificat două categorii de persoane vizate de programele spion în Spania; întrucât prima categorie include prim-ministrul și ministrul apărării, ministrul de interne și alți înalți funcționari; întrucât a doua categorie ține de ceea ce organizația Citizen Lab numește „CatalanGate” și include 65 de persoane vizate, inclusiv personalități politice din guvernul regional al Cataloniei, membri ai mișcării pro-catalane de independență, deputați în Parlamentul European, avocați, cadre universitare și actori ai societății civile; întrucât în mai 2022, autoritățile spaniole au recunoscut vizarea a 18 persoane, cu autorizație judiciară, deși până în prezent nu au

făcut publice mandatele sau orice alte informații, invocând securitatea națională, atunci când au justificat utilizarea programelor spion în Spania; întrucât alte 47 de persoane au fost, se pare, de asemenea vizate, dar nu au primit alte informații decât cele de la Citizen Lab;

S. întrucât în Cipru nu au fost confirmate acuzații de infectare cu programe spion; întrucât Cipru este un important centru european de export pentru industria de supraveghere și un loc atractiv pentru întreprinderile care vând tehnologii de supraveghere;

T. întrucât există indicii puternice că guvernele din Maroc și Rwanda, printre altele, au vizat cu programe spion cetățeni de marcă ai Uniunii, între aceștia aflându-se președintele Franței, prim-ministrul, ministrul apărării și ministrul de interne din Spania, prim-ministrul de atunci al Belgiei, fostul președinte al Comisiei și fostul prim-ministru al Italiei, precum și Carine Kanimba, fiica lui Paul Rusesabagina;

U. întrucât se poate presupune în siguranță că toate statele membre au achiziționat sau au utilizat unul sau mai multe sisteme de spionaj; întrucât majoritatea guvernelor din Uniunea Europeană se vor abține de la utilizarea nelegitimă a programelor spion, dar riscul de utilizare abuzivă este foarte ridicat în absența unui cadru juridic solid care să includă garanții și supraveghere și având în vedere dificultățile tehnice în detectarea și urmărirea infectărilor;

V. întrucât majoritatea guvernelor și parlamentelor statelor membre nu au furnizat Parlamentului European informații semnificative cu privire la cadrele lor juridice care reglementează utilizarea programelor spion în afară de ceea ce se cunoștea deja în mod public, în pofida obligației de a face acest lucru în temeiul articolului 3 alineatul (4) din Decizia Parlamentului European, a Consiliului și a Comisiei din 6 martie 1995 privind modalitățile detaliate de exercitare a dreptului de anchetă al Parlamentului European; întrucât este dificil să se evalueze aplicarea legislației Uniunii și garanțiile, supravegherea și căile de atac, ceea ce împiedică o protecție adecvată a drepturilor fundamentale ale cetățenilor;

W. întrucât articolul 4 alineatul (3) din TUE statuează că „[î]n temeiul principiului cooperării loiale, Uniunea și statele membre se respectă și se ajută reciproc în îndeplinirea misiunilor care decurg din tratate”;

X. întrucât mai multe persoane importante din sectorul programelor spion au obținut cetățenia malteză, ceea ce le facilitează activitatea în interiorul Uniunii și dinspre Uniune;

Y. întrucât mulți dezvoltatori și vânzători de programe spion sunt sau au fost înregistrați într-unul sau în mai multe state membre; întrucât printre aceștia se numără NSO Group cu sedii în Luxemburg, Cipru, Țările de Jos și Bulgaria, societatea-mamă a Intellexa, Thalestris Limited, în Irlanda, Grecia, Elveția și Cipru, DSIRF în Austria, Amesys și Nexa Technologies în Franța, Tykelab și RCS Lab în Italia și FinFisher (care nu mai există) în Germania;

Z. întrucât Uniunea Europeană nu participă la Aranjamentul de la Wassenaar pentru controlul exporturilor de arme convenționale și produse și tehnologii cu dublă utilizare; întrucât toate statele membre, cu excepția Ciprului, participă la Aranjamentul de la

Wassenaar, deși Cipru a depus o cerere de aderare la Aranjamentul de la Wassenaar cu mult timp în urmă; întrucât Cipru are obligații în temeiul Regulamentului privind produsele cu dublă utilizare;

AA. întrucât regimul de export al Israelului[20] se aplică, în principiu, tuturor cetățenilor israelieni, chiar și atunci când operează din UE; întrucât Israelul nu participă la Aranjamentul de la Wassenaar, dar susține că aplică totuși standardele acestuia;

AB. întrucât exportul de programe spion din Uniune către țări din afara UE este reglementat de Regulamentul privind produsele cu dublă utilizare, care a fost revizuit în 2021; întrucât Comisia a publicat un prim raport de punere în aplicare în septembrie 2022[21];

AC. întrucât unii producători de programe spion care exportă în țări terțe se stabilesc în Uniune pentru a câștiga respectabilitate în timp ce vând programe spion regimurilor represive; întrucât au loc exporturi din Uniune către regimuri represive sau actori nestatali, încălcându-se normele UE privind exporturile;

AD. întrucât Amesys și Nexa Technologies sunt în prezent urmărite penal în Franța pentru exportul de tehnologie de supraveghere către Libia, Egipt și Arabia Saudită; întrucât se pare că societățile Intellexa cu sediul în Grecia și-au exportat produsele în Bangladesh, Sudan, Madagascar și cel puțin o țară arabă; întrucât software-ul FinFisher este folosit de zeci de țări din întreaga lume, inclusiv de Angola, Bahrain, Bangladesh, Egipt, Etiopia, Gabon, Iordania, Kazahstan, Myanmar, Oman, Qatar, Arabia Saudită, Turcia și serviciile de informații din Maroc, care au fost acuzate de Amnesty International și de Forbidden Stories că folosesc programul spion Pegasus împotriva jurnaliștilor, a apărătorilor drepturilor omului, a societății civile și a politicienilor; întrucât nu se știe dacă au fost acordate licențe de export pentru exportul de programe spion către toate aceste țări;

AE. întrucât numărul de participanți la târgurile de armament și ISSWorld care comercializau capacități de programe spion demonstrează predominanța furnizorilor de programe spion și de produse și servicii conexe din țări terțe, un număr semnificativ dintre ei având sediul în Israel (de exemplu, NSO Group, Wintego, Quadream și Cellebrite), și aduc în lumină producători importanți din India (ClearTrail), Regatul Unit (BAe Systems și Black Cube) și Emiratele Arabe Unite (DarkMatter), în timp ce introducerea pe lista neagră, de către lista de entități din Statele Unite, a producătorilor de programe spion situați în Israel (NSO Group și Candiru), în Rusia (Positive Technologies) și în Singapore (Computer Security Initiative Consultancy PTE LTD.) evidențiază și mai mult originile diverse ale producătorilor de programe spion; întrucât la târg participă și o gamă largă de autorități publice europene, printre care forțele de poliție locale;

AF. întrucât articolul 4 alineatul (2) din TUE prevede că securitatea națională rămâne responsabilitatea exclusivă a fiecărui stat membru;

AG. întrucât, cu toate acestea, CJUE a statuat (cauza C-623/17) că „deși este de competența statelor membre să își definească interesele esențiale de securitate și să adopte măsurile

[20] Legea privind controlul exporturilor în sectorul apărării 5766-2007, Ministerul Apărării din Israel.
[21] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=COM%3A2022%3A434%3AFIN&qid=1662029750223.

apte să asigure securitatea lor internă și externă, simplul fapt că o măsură națională a fost adoptată în vederea protejării securității naționale nu poate să determine inaplicabilitatea dreptului Uniunii și nici să absolve statele membre de necesitatea de a respecta acest drept”;

AH. întrucât CJUE a statuat (cauza C-203/15) că „[a]rticolul 15 alineatul (1) din Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice), astfel cum a fost modificată prin Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009, lecturat în lumina articolelor 7[, 8 și 11], precum și a articolului 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene, trebuie interpretat în sensul că se opune unei reglementări naționale care prevede, în scopul combaterii infracționalității, o păstrare generalizată și nediferențiată a ansamblului datelor de transfer și al datelor de localizare ale tuturor abonaților și utilizatorilor înregistrați în ceea ce privește toate mijloacele de comunicare electronică”;

AI. întrucât CJUE a statuat (cauza C-203/15) că „[a]rticolul 15 alineatul (1) din Directiva 2002/58, astfel cum a fost modificată prin Directiva 2009/136/CE, lecturat în lumina articolelor 7[, 8 și 11], precum și a articolului 52 alineatul (1) din Carta drepturilor fundamentale, trebuie interpretat în sensul că se opune unei reglementări naționale care guvernează protecția și securitatea datelor de transfer și a datelor de localizare, în special accesul autorităților naționale competente la datele păstrate, fără a limita acest acces, în cadrul combaterii infracționalității, numai la combaterea infracționalității grave, fără a supune respectivul acces unui control prealabil din partea unei instanțe sau a unei autorități administrative independente, și fără a impune ca datele în cauză să fie păstrate pe teritoriul Uniunii”;

AJ. întrucât jurisprudența CEDO arată clar că orice supraveghere trebuie să aibă loc în conformitate cu legea, să servească unui scop legitim și să fie necesară și proporțională; întrucât, în plus, cadrul juridic trebuie să ofere garanții precise, eficiente și cuprinzătoare privind ordonarea, executarea și posibilele căi de atac împotriva măsurilor de supraveghere, care trebuie să facă obiectul unui control judiciar adecvat și al unei supravegheri eficace[22];

AK. întrucât Convenția Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (Convenția 108), modernizată recent sub numele de Convenția 108+, se aplică prelucrării datelor cu caracter personal în scopuri legate de securitatea statului (națională), inclusiv în scopuri de apărare; întrucât toate statele membre sunt părți la această convenție;

AL. întrucât aspecte importante ale utilizării de programe spion pentru prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor și executarea sancțiunilor penale, inclusiv apărarea împotriva amenințărilor la adresa siguranței publice și prevenirea lor, intră în domeniul de aplicare al dreptului UE;

AM. întrucât Carta stabilește condițiile în care poate fi limitată exercitarea drepturilor fundamentale, impunând ca limitarea să fie prevăzută prin lege, să respecte substanța

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

drepturilor și libertăților în cauză, să facă obiectul principiului proporționalității și să fie impusă numai dacă este necesară și răspunde efectiv obiectivelor de interes general recunoscute de Uniune sau necesității protejării drepturilor și libertăților celorlalți; întrucât atunci când se folosesc programe spion, nivelul de interferență cu dreptul la viață privată este atât de grav încât persoana este, de fapt, privată de acesta, iar utilizarea nu poate fi considerată întotdeauna proporțională, indiferent dacă măsura poate fi considerată necesară pentru atingerea obiectivelor legitime ale unui stat democratic;

AN. întrucât Directiva asupra confidențialității și comunicațiilor electronice prevede că statele membre trebuie să asigure confidențialitatea comunicațiilor; întrucât utilizarea instrumentelor de supraveghere constituie o restricționare a dreptului la protecția echipamentelor terminale prevăzut de Directiva asupra confidențialității și comunicațiilor electronice; întrucât aceste restricționări fac ca legislațiile naționale privind programele spion să intre în domeniul de aplicare al Directivei asupra confidențialității și comunicațiilor electronice la fel ca în cazul legislațiilor naționale privind păstrarea datelor; întrucât utilizarea frecventă a tehnologiei de spionaj intruzive nu ar fi compatibilă cu ordinea juridică a Uniunii;

AO. întrucât în temeiul dreptului internațional, un stat are dreptul de a investiga posibile infracțiuni doar în jurisdicția sa și trebuie să recurgă la asistența altor state dacă ancheta trebuie să aibă loc în alte state, cu excepția cazului în care există o bază pentru desfășurarea anchetelor în cealaltă jurisdicție în virtutea unui acord internațional sau, în cazul statelor membre, a dreptului Uniunii;

AP. întrucât infectarea unui dispozitiv cu un program spion și colectarea ulterioară a datelor au loc prin intermediul serverelor furnizorilor de servicii mobile; întrucât roamingul gratuit în interiorul Uniunii a făcut ca uneori clienții să aibă contracte de telefonie mobilă din alte state membre decât cel în care își au reședința, dar în prezent nu există niciun temei juridic în dreptul Uniunii pentru colectarea de date în celălalt stat membru prin utilizarea programelor spion;

AQ. întrucât David Kaye, fostul raportor special al ONU privind promovarea și apărarea dreptului la libertatea de exprimare[23], și Irene Khan, actuala raportoare specială a ONU privind promovarea și apărarea dreptului la libertatea de exprimare[24], au solicitat un moratoriu imediat asupra utilizării, transferului și vânzării de instrumente de supraveghere până la instituirea de garanții riguroase privind drepturile omului pentru a reglementa practicile și a garanta că guvernele și actorii nestatali folosesc aceste instrumente în moduri legitime;

AR. întrucât există cazuri în care societățile din sectorul programelor spion, în special Intellexa, au vândut nu numai tehnologia de interceptare și extragere propriu-zisă, ci și întregul serviciu, denumit și „piraterie informatică ca serviciu” sau „inteligență cibernetică activă”, oferind un pachet de metode tehnologice de supraveghere și interceptare, precum și formare pentru personal și sprijin tehnic, operațional și

[23] „Surveillance and human rights” (Supravegherea și drepturile omului), raport al raportorului special al ONU privind promovarea și apărarea dreptului la libertatea de opinie și de exprimare, A/HRC/41/35, 2019.
[24] Oficiul Înaltului Comisar al ONU pentru Drepturile Omului, „Spyware scandal: UN experts call for moratorium on sale of «life threatening' surveillance tech»” (Scandalul programelor spion: experții ONU solicită un moratoriu asupra vânzării de tehnologie de supraveghere care „pune viața în pericol”).

metodologic; întrucât acest serviciu ar putea permite companiei să dețină controlul asupra întregii operațiuni de supraveghere și să agrege datele de supraveghere; întrucât această practică este aproape imposibil de supravegheat și controlat de către autoritățile competente; întrucât acest lucru îngreunează respectarea principiilor proporționalității, necesității, legitimității, legalității și adecvării; întrucât acest serviciu nu este permis de agenția israeliană pentru export în domeniul apărării (DECA); întrucât Cipru a fost folosit pentru a eluda limitările existente în temeiul legislației israeliene în scopul de a furniza pirateria informatică ca serviciu;

AS. întrucât statele membre trebuie să respecte Directiva 2014/24/UE și Directiva 2009/81/CE privind achizițiile publice și, respectiv, achizițiile în domeniul apărării; întrucât statele membre trebuie să justifice cum se cuvine derogările în temeiul articolului 346 alineatul (1) litera (b) din TFUE, dat fiind că Directiva 2009/81/CE ia în considerare în mod explicit caracteristicile sensibile ale achizițiilor publice din domeniul apărării, precum și să respecte Acordul OMC privind achizițiile publice, astfel cum a fost modificat la 30 martie 2012[25], dacă sunt parte la acesta;

AT. întrucât AEPD a subliniat că statele membre trebuie să respecte Convenția Europeană a Drepturilor Omului și jurisprudența CEDO, care stabilește limite pentru activitățile de supraveghere pentru securitatea națională; întrucât, în plus, atunci când este utilizată în scopuri de asigurare a respectării legii, supravegherea trebuie să respecte legislația UE și în special Carta și directivele UE, cum ar fi Directiva asupra confidențialității și comunicațiilor electronice și Directiva privind protecția datelor în materie de asigurare a respectării legii;

AU. întrucât există informații potrivit cărora instituții financiare mari au încercat să încurajeze producătorii de programe spion să nu aplice standarde adecvate în materie de drepturile omului și obligația de diligență și să continue să vândă programe spion regimurilor represive;

AV. întrucât Israelul se situează pe locul al treilea printre țările asociate la programul Orizont 2020 în ceea ce privește participarea globală la program; întrucât Acordul cu Israelul privind programul Orizont Europa are un buget total de 95,5 miliarde EUR pentru perioada 2021-2027[26]; întrucât au fost puse fonduri la dispoziția companiilor israeliene militare și din domeniul securității prin intermediul acestor programe europene[27];

AW. întrucât principalul instrument legislativ pentru politicile de dezvoltare ale Uniunii este Regulamentul (UE) 2021/947[28] („Regulamentul privind Europa globală”), iar finanțarea din partea Uniunii poate fi oferită prin modurile de finanțare prevăzute de Regulamentul financiar; întrucât asistența poate fi suspendată în cazul degradării democrației, a

[25] https://www.wto.org/english/tratop_e/gproc_e/gpa_1994_e.htm.
[26] https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/israel-joins-horizon-europe-research-and-innovation-programme-2021-12-06_en.
[27] https://webgate.ec.europa.eu/dashboard/extensions/CountryProfile/CountryProfile.html?Country=Israel https://elbitsystems.com/products/comercial-aviation/innovation-rd/.
28 Regulamentul (UE) 2021/947 al Parlamentului European și al Consiliului din 9 iunie 2021 de instituire a Instrumentului de vecinătate, cooperare pentru dezvoltare și cooperare internațională – „Europa globală”, de modificare și abrogare a Deciziei nr. 466/2014/UE a Parlamentului European și a Consiliului și de abrogare a Regulamentului (UE) 2017/1601 al Parlamentului European și al Consiliului și a Regulamentului (CE, Euratom) nr. 480/2009 al Consiliului (JO L 209, 14.6.2021).

drepturilor omului sau a statului de drept în țările terțe,

1. evidențiază importanța incontestabilă a protecției vieții private, a dreptului la demnitate, a vieții private și de familie, a libertății de exprimare și de informare, a libertății de întrunire și de asociere și a dreptului la un proces echitabil, mai ales într-o lume din ce în ce mai digitală, în care tot mai multe din activitățile noastre se desfășoară în mediul online;

2. este ferm convins că încălcările acestor drepturi și libertăți fundamentale sunt esențiale în ceea ce privește respectarea principiilor juridice comune prevăzute în tratate și în alte surse și observă că însăși democrația este în joc, deoarece folosirea programelor spion împotriva politicienilor, societății civile și jurnaliștilor are un efect de intimidare și afectează grav dreptul la întrunire pașnică, libertatea de exprimare și participarea publicului;

3. condamnă cu fermitate folosirea programelor spion de către guvernele statelor membre și de către membrii autorităților guvernamentale sau ai instituțiilor statului în scopul de a monitoriza, șantaja, intimida, manipula și discredita membrii opoziției, criticii și societatea civilă, de a elimina controlul democratic și presa liberă, de a manipula alegerile și a submina statul de drept prin vizarea judecătorilor, a procurorilor și a avocaților în scopuri politice;

4. atrage atenția că această utilizare nelegitimă a programelor spion de către guvernele naționale și din afara UE afectează direct și indirect instituțiile Uniunii și procesul decizional, subminând astfel integritatea democrației Uniunii Europene;

5. constată cu profundă îngrijorare inadecvarea fundamentală a actualei structuri de guvernanță a Uniunii pentru a răspunde atacurilor din interiorul Uniunii la adresa democrației, a drepturilor fundamentale și a statului de drept și faptul că multe state membre nu iau măsuri; menționează că atunci când aceste drepturi sunt amenințate într-un stat membru, întreaga Uniune este pusă în pericol;

6. accentuează că standardele digitale care reglementează evoluțiile tehnologice din Uniune trebuie să respecte drepturile fundamentale;

7. are părerea fermă că exportul de programe spion din Uniune către dictaturi și regimuri represive cu rezultate slabe în domeniul drepturilor omului, unde astfel de instrumente sunt folosite împotriva activiștilor pentru drepturile omului, a jurnaliștilor și a criticilor guvernului, reprezintă o încălcare gravă a drepturilor fundamentale consacrate în Cartă și o încălcare flagrantă a normelor Uniunii privind exporturile;

8. își exprimă, de asemenea, îngrijorarea cu privire la utilizarea nelegitimă și comercializarea ilicită a programelor spion de către alte state membre, care, împreună, transformă Uniunea într-o destinație pentru industria programelor spion;

9. își exprimă îngrijorarea cu privire la vizarea de către țări din afara UE a unor personalități importante, apărători ai drepturilor omului și jurnaliști din Uniune cu programe spion;

10. este, de asemenea, îngrijorat de reticența evidentă de a investiga folosirea abuziva a

programelor spion, atât în cazul în care suspectul este un stat membru, cât și atunci când este un organism guvernamental dintr-o țară din afara UE; observă progresele foarte lente și absența transparenței în anchetele judiciare privind folosirea abuzivă a programelor spion împotriva liderilor de guvern și a miniștrilor din statele membre ale UE și a Comisiei, precum și împotriva membrilor societății civile, a jurnaliștilor sau a opozanților politici;

11. observă că cadrul juridic al unor state membre nu oferă garanții precise, eficace și cuprinzătoare privind dispozițiile, executarea și eventualele căi de atac împotriva măsurilor de supraveghere; constată că astfel de măsuri trebuie să servească unui scop legitim și să fie necesare și proporționale;

12. regretă că guvernele statelor membre, Consiliul și Comisia nu au reușit să coopereze pe deplin în cadrul anchetei și să împărtășească toate informațiile pertinente și semnificative pentru a ajuta comisia de anchetă să își îndeplinească sarcinile așa cum sunt prevăzute în mandat; recunoaște că unele dintre aceste informații pot face obiectul unor cerințe legale stricte în materie de secret și confidențialitate; consideră că răspunsul colectiv al Consiliului este complet inadecvat și contrar principiului cooperării loiale, astfel cum este consacrat la articolul 4 alineatul (3) din TUE;

13. conchide că nici statele membre, nici Consiliul și nici Comisia nu au părut să fie deloc interesate să depună eforturi maxime pentru a ancheta pe deplin folosirea abuzivă a programelor spion, protejând astfel cu bună știință guvernele Uniunii care încalcă drepturile omului în interiorul și în afara Uniunii;

14. concluzionează că în Polonia au avut loc cazuri majore de încălcare a normelor de drept și de administrare defectuoasă în punerea în aplicare a dreptului Uniunii;

15. invită Polonia:

(a) să îndemne procurorul general să lanseze anchete privind folosirea abuzivă a programelor spion;

(b) să restabilească de urgență garanții instituționale și juridice suficiente, inclusiv controale *ex ante* și *ex post* eficace și obligatorii, precum și mecanisme de supraveghere independente, printre care controlul judiciar asupra activităților de supraveghere; accentuează că în contextul unui control *ex ante* eficace, cererea de supraveghere operațională adresată instanței și ordinul judecătoresc pentru o astfel de supraveghere ar trebui să conțină o justificare clară și o indicație a mijloacelor tehnice care trebuie folosite pentru supraveghere și că, în contextul unui control *ex post* eficace, ar trebui introdusă obligația de a informa persoana care face obiectul supravegherii cu privire la acest fapt, la durata, la domeniul de aplicare și la modul de prelucrare a datelor obținute în timpul supravegherii operaționale;

(c) să introducă o legislație consecventă care să protejeze cetățenii, indiferent dacă supravegherea operațională este efectuată de către parchet, serviciile secrete sau orice alt organism de stat;

(d) să respecte hotărârea Curții Constituționale referitoare la Legea privind poliția din 1990;

(e) să respecte avizul Comisiei de la Veneția referitor la Legea privind poliția din 2016;

(f) să respecte diferitele hotărâri ale CEDO, cum ar fi hotărârea pronunțată în cauza Roman Zaharov/Rusia din 2015, în care se subliniază că sunt necesare criterii stricte privind supravegherea, o autorizare și supraveghere judiciară adecvată, distrugerea imediată a datelor irelevante, controlul judiciar asupra procedurilor de urgență și o cerință privind notificarea persoanelor vizate, precum și hotărârea în cauza Klass și alții/Germania din 1978, în care se prevede că supravegherea trebuie să fie suficient de importantă pentru a necesita o astfel de încălcare a vieții private;

(g) să respecte toate hotărârile CJUE și CEDO referitoare la independența sistemului judiciar și la supremația dreptului Uniunii;

(h) să retragă articolul 168a din Legea reformulată de modificare a Codului de procedură penală din 2016;

(i) să restabilească independența deplină a sistemului judiciar și să respecte competențele statutare ale tuturor organismelor de supraveghere pertinente, cum ar fi Avocatul Poporului, președintele Biroului pentru protecția datelor cu caracter personal și instituția supremă de conturi, pentru a se asigura că toate organismele de supraveghere beneficiază de cooperare și acces deplin la informații și pentru a furniza informații complete tuturor persoanelor vizate;

(j) să introducă de urgență alocarea aleatorie a cauzelor către judecătorii din instanțe pentru fiecare cerere depusă, chiar și la sfârșit de săptămână și în afara programului normal de lucru, pentru a se evita selectarea „judecătorilor prieteni” de către serviciile secrete și să asigure transparența unui astfel de sistem, printre altele, punând la dispoziția publicului algoritmul pe baza căruia sunt atribuite în mod aleatoriu cauzele judecătorilor;

(k) să reinstituie sistemul tradițional de control parlamentar în care partidul de opoziție preia președinția Comisiei parlamentare de supraveghere a serviciilor speciale (KSS);

(l) să clarifice urgent situația privind folosirea abuzivă a programelor spion în Polonia, pentru a nu exista nicio îndoială cu privire la integritatea alegerilor viitoare;

(m) să pună în aplicare cum se cuvine și să asigure respectarea Directivei (UE) 2016/680 (Directiva privind protecția datelor în materie de asigurare a respectării legii) și să se asigure că autoritatea pentru protecția datelor are competența de a supraveghea prelucrarea datelor cu caracter personal, printre altele, de către autorități precum Biroul Central Anticorupție și Agenția pentru Securitate Internă;

(n) să pună în aplicare Directiva privind avertizorii;

(o) să se abțină de la adoptarea în noile legi privind comunicațiile electronice a unor prevederi care contravin Convenției europene a drepturilor omului (CEDO);

(p) să asigure disponibilitatea unor căi de atac eficace pentru cetățenii Poloniei afectați de punerea în aplicare a legilor care contravin Constituției Poloniei și CEDO;

(q) să invite Europol să investigheze toate cazurile de presupusă folosire abuzivă a

programelor spion;

(r) să garanteze controlul constituțional independent al legilor în Polonia;

(s) să restabilească independența rolului procurorului general în raport cu ministrul justiției pentru a garanta că anchetele privind presupusele încălcări ale drepturilor fundamentale nu sunt influențate de considerente politice;

16. îndeamnă Comisia să evalueze compatibilitatea Legii polone din 2018 privind protecția datelor cu caracter personal prelucrate în legătură cu prevenirea și combaterea infracționalității cu Directiva UE privind protecția datelor în materie de asigurare a respectării legii și, dacă este necesar, să demareze o procedură de constatare a neîndeplinirii obligațiilor;

17. concluzionează că în Ungaria au avut loc cazuri majore de încălcare a normelor de drept și de administrare defectuoasă în punerea în aplicare a dreptului Uniunii;

18. invită Ungaria:

(a) să restabilească de urgență garanții instituționale și juridice suficiente, inclusiv controale *ex ante* și *ex post* eficace și obligatorii, precum și mecanisme de supraveghere independente, printre care controlul judiciar asupra activităților de supraveghere; accentuează că în contextul unui control *ex ante* eficace, cererea de supraveghere operațională adresată instanței și ordinul judecătoresc pentru o astfel de supraveghere ar trebui să conțină o justificare clară și o indicație a mijloacelor tehnice care trebuie folosite pentru supraveghere și că, în contextul unui control *ex post* eficace, ar trebui introdusă obligația de a informa persoana care face obiectul supravegherii cu privire la acest fapt, la durata, la domeniul de aplicare și la modul de prelucrare a datelor obținute în timpul supravegherii operaționale;

(b) să respecte diferitele hotărâri ale CEDO, cum ar fi hotărârea pronunțată în cauza Roman Zaharov/Rusia din 2015, în care se subliniază că sunt necesare criterii stricte privind supravegherea, o autorizare și supraveghere judiciară adecvată, distrugerea imediată a datelor irelevante, controlul judiciar asupra procedurilor de urgență și o cerință privind notificarea persoanelor vizate, precum și hotărârea în cauza Klass și alții/Germania din 1978, în care se prevede că supravegherea trebuie să fie suficient de importantă pentru a necesita o astfel de încălcare a vieții private și cerința de notificare a persoanelor supravegheate;

(c) să respecte toate hotărârile CJUE și CEDO referitoare la independența sistemului judiciar și la supremația dreptului Uniunii;

(d) să reinstituie organisme de supraveghere independente, în conformitate cu hotărârea CEDO în cauza Hüttl/Ungaria, în care instanța afirmă că Autoritatea Națională pentru Protecția Datelor și Libertatea de Informare (NAIH) nu este în măsură să efectueze o supraveghere independentă a utilizării programelor spion, având în vedere că serviciile secrete au dreptul de a refuza accesul la anumite documente din motive de confidențialitate;

(e) să restabilească independența deplină a sistemului judiciar și a tuturor organismelor de

supraveghere relevante, cum ar fi Avocatul Poporului și autoritățile pentru protecția datelor, pentru a se asigura că toate organismele de supraveghere beneficiază de cooperare și acces deplin la informații și pentru a furniza informații complete tuturor persoanelor vizate;

(f) să reintegreze angajați independenți în funcții de conducere în cadrul organismelor de supraveghere, cum ar fi Curtea Constituțională, Curtea Supremă, Curtea de Conturi, Parchetul, Banca Națională a Ungariei și Comisia Electorală Națională;

(g) să pună în aplicare Directiva privind avertizorii;

(h) să invite Europol să investigheze toate cazurile de presupusă folosire abuzivă a programelor spion;

(i) să se abțină de la adoptarea în noile legi privind comunicațiile electronice a unor prevederi care contravin CEDO;

(j) să asigure disponibilitatea unor căi de atac eficace pentru cetățenii Ungariei afectați de punerea în aplicare a legilor care contravin Constituției Ungariei și CEDO;

19. concluzionează că în Grecia au avut loc cazuri de încălcare a normelor de drept și de administrare defectuoasă în punerea în aplicare a dreptului Uniunii;

20. invită Grecia:

(a) să restabilească și să consolideze de urgență garanțiile instituționale și juridice, inclusiv controale *ex ante* și *ex post* eficace, precum și mecanisme de supraveghere independente;

(b) să abroge de urgență toate licențele de export care nu respectă pe deplin Regulamentul privind produsele cu dublă utilizare și să investigheze acuzațiile de exporturi ilegale, printre altele către Sudan;

(c) să se asigure că autoritățile pot investiga în mod liber și neîngrădit toate acuzațiile privind folosirea programelor spion;

(d) să retragă de urgență amendamentul 826/145 la Legea nr. 2472/1997, care a anulat capacitatea Autorității Elene pentru Securitatea și Confidențialitatea Comunicațiilor (ADAE) de a informa cetățenii cu privire la ridicarea confidențialității comunicațiilor; să modifice Legea nr. 5002/2022 pentru a restabili dreptul persoanelor vizate de a fi informate imediat, la cerere, de îndată ce supravegherea a fost finalizată, și pentru a corecta alte dispoziții care slăbesc garanțiile, controlul și tragerea la răspundere;

(e) să restabilească independența deplină a sistemului judiciar și a tuturor organismelor de supraveghere relevante, cum ar fi Avocatul Poporului și autoritățile pentru protecția datelor, și să respecte pe deplin independența ADAE, pentru a se asigura că toate organismele de supraveghere și control beneficiază de cooperare și acces deplin la informații și pentru a furniza informații complete tuturor persoanelor vizate;

(f) să se asigure că ADAE poate crea o arhivă electronică pentru a-și putea îndeplini

sarcina;

(g) să clarifice urgent situația privind folosirea abuzivă a programelor spion în Grecia, pentru a nu exista nicio îndoială cu privire la integritatea alegerilor viitoare;

(h) să anuleze amendamentul legislativ din 2019 care a plasat Serviciul național de informații (EYP) sub controlul direct al prim-ministrului; să instituie garanții constituționale și să permită controlul parlamentar al operațiilor serviciului respectiv, fără pretextul confidențialității informațiilor;

(i) să asigure independența conducerii Autorității naționale pentru transparență (EAD);

(j) să se asigure că sistemul judiciar dispune de toate mijloacele necesare pentru anchetă în urma presupusei folosiri abuzive de programe spion și să confișteprobele fizice ale mandatarilor, ale societăților de intermediere și ale vânzătorilor de programe spion care sunt legate de infectările cu programe spion;

(k) să invite Europol să se alăture imediat anchetelor;

(l) să renunțe la amestecul politic în activitatea procurorului-șef;

21. concluzionează că, în general, cadrul de reglementare din Spania este în conformitate cu cerințele prevăzute în tratate; atrage atenția totuși că sunt necesare unele reforme, iar punerea în practică trebuie să respecte pe deplin drepturile fundamentale și să asigure protecția participării publicului;

22. invită, prin urmare, Spania:

(a) să efectueze o anchetă completă, echitabilă și eficace, în care să se ofere claritate deplină cu privire la toate presupusele cazuri de utilizare a programelor spion, inclusiv cele 47 de cazuri în care nu este clar dacă persoanele în cauză au fost vizate sau nu de Agenția Națională de Informații (CNI) din Spania printr-un ordin judecătoresc sau dacă o altă autoritate a primit ordine judecătorești pentru a le viza în mod legal, precum și cu privire la folosirea programelor spion împotriva prim-ministrului și a membrilor guvernului, și să prezinte constatările cât mai pe larg posibil, în conformitate cu legislația aplicabilă;

(b) să asigure accesul adecvat al persoanelor vizate la autorizația judiciară eliberată de Curtea Supremă către CNI pentru a viza 18 persoane;

(c) să coopereze cu instanțele pentru a se asigura că persoanele vizate de programe spion au acces la căi de atac reale și semnificative și că anchetele judiciare sunt finalizate fără întârziere, în mod imparțial și aprofundat, alocându-se resurse suficiente în acest sens;

(d) să înceapă reforma cadrului juridic al CNI, astfel cum a anunțat în mai 2022;

(e) să invite Europol, care ar putea contribui cu cunoștințe tehnice de specialitate, să se alăture anchetelor;

23. concluzionează că în Cipru există dovezi cu privire la cazuri de încălcare a normelor de drept și de administrare defectuoasă în punerea în aplicare a Regulamentului privind

produsele cu dublă utilizare care necesită control atent;

24. invită Ciprul:

(a) să evalueze în detaliu toate licențele de export eliberate pentru programele spion și să le abroge, dacă este cazul;

(b) să evalueze în detaliu transportul de materiale de spionaj pe piața internă a UE între statele membre și să cartografieze diferitele societăți israeliene sau societăți deținute și conduse de cetățeni israelieni care sunt înregistrate în Cipru și care sunt implicate în astfel de activități;

(c) să publice raportul anchetatorului special privind cazul „Spyware Van”, conform solicitării formulate de comisie în timpul misiunii sale oficiale în Cipru;

(d) să ancheteze temeinic, cu asistența Europol, toate acuzațiile de utilizare și export ilegale ale programelor spion, în special cu privire la jurnaliști, avocați, actori ai societății civile și cetățeni ciprioți;

25. consideră că și situația din câteva alte state membre este îngrijorătoare, în special având în vedere prezența unei industrii lucrative și în expansiune a programelor spion, care profită de buna reputație, de piața unică și de libera circulație din Uniune, permițând unor state membre precum Cipru și Bulgaria să devină un centru de export al programelor spion către regimuri represive din întreaga lume;

26. consideră că incapacitatea sau refuzul unor autorități naționale de a asigura protecția corespunzătoare a cetățenilor Uniunii, inclusiv lacune în reglementare și instrumente juridice adecvate, demonstrează cu toată claritatea necesară că acțiunea la nivelul Uniunii este indispensabilă pentru a asigura respectarea literei tratatelor și a legislației Uniunii, astfel încât dreptul cetățenilor de a trăi într-un mediu sigur în care sunt respectate demnitatea umană, viața privată, datele cu caracter personal și proprietatea, conform dispozițiilor Directivei 2012/29/UE, potrivit căreia fiecare victimă a unei infracțiuni are dreptul de a primi sprijin și protecție în conformitate cu nevoile sale individuale;

27. conchide că s-au înregistrat deficiențe grave în punerea în aplicare a dreptului Uniunii atunci când Comisia și Serviciul European de Acțiune Externă (SEAE) au acordat sprijin unor țări din afara UE, printre care, dar nu numai, 10 țări din Sahel, pentru a le permite să își dezvolte capacitățile de supraveghere[29];

28. consideră că comerțul cu programe spion și utilizarea acestora trebuie reglementate în mod strict; recunoaște, cu toate acestea, că procesul legislativ poate dura, în timp ce abuzurile trebuie oprite imediat; solicită adoptarea unor condiții pentru utilizarea, vânzarea, achiziționarea și transferul de programe spion în mod legal; insistă ca, pentru a utiliza în continuare programele spion, statele membre să îndeplinească toate condițiile următoare până la 31 decembrie 2023:

[29] Decizia în cazul 1904/2021/MHZ, disponibilă la adresa https://www.ombudsman.europa.eu/ro/decision/ro/163491.

(a) toate cazurile de presupusă utilizare abuzivă a programelor spion sunt pe deplin investigate și soluționate fără întârziere de către autoritățile competente de aplicare a legii, de urmărire penală și judiciare

(b) demonstrează că cadrul care reglementează utilizarea programelor spion este în conformitate cu standardele stabilite de Comisia de la Veneția și cu jurisprudența relevantă a CJUE și a CEDO;

(c) își asumă angajamentul explicit de a implica Europol, în temeiul articolelor 4, 5 și 6 din Regulamentul Europol, în anchetele privind acuzațiile de utilizare ilegală a programelor spion; și

(d) toate licențele de export care nu sunt în deplină conformitate cu Regulamentul privind dubla utilizare sunt abrogate;

29. consideră că îndeplinirea acestor condiții trebuie evaluată de Comisie până la 30 noiembrie 2023; consideră, de asemenea, că concluziile evaluării se prezintă într-un raport public;

30. subliniază că, deși combaterea infracțiunilor grave și a terorismului, precum și recunoașterea faptului că posibilitatea de a face acest lucru sunt extrem de importante pentru statele membre, protecția drepturilor fundamentale și a democrației este esențială; accentuează, de asemenea, că utilizarea programelor spion de către statele membre trebuie să fie proporțională, nu trebuie să fie arbitrară, iar supravegherea trebuie să fie autorizată numai în circumstanțe strict definite și prestabilite; consideră că mecanismele ex-ante eficace de asigurare a supravegherii judiciare sunt esențiale pentru protejarea libertăților individuale; reafirmă că drepturile individuale nu pot fi expuse riscurilor prin permiterea accesului neîngrădit la supraveghere; evidențiază că capacitatea sistemului judiciar de a efectua o supraveghere ex-post semnificativă și eficace în domeniul cererilor de supraveghere pentru securitatea națională este, de asemenea, importantă, pentru a se asigura că utilizarea disproporționată a programelor spion de către guverne poate fi contestată;

31. subliniază că folosirea programelor spion pentru aplicarea legii ar trebui reglementată direct prin măsuri bazate pe titlul 5 capitolul 4 din TFUE privind cooperarea judiciară în materie penală; subliniază că configurația programelor spion importate în UE și introduse în alt mod pe piață ar trebui reglementată printr-o măsură bazată pe articolul 114 din TFUE; ia act de faptul că utilizarea programelor spion în scopuri de securitate națională poate fi reglementată doar indirect, de exemplu, prin intermediul drepturilor fundamentale și al normelor privind protecția datelor;

32. consideră că, având în vedere dimensiunea transnațională și europeană a utilizării programelor spion, este necesar un control coordonat și transparent la nivelul UE pentru a asigura nu numai protecția cetățenilor UE, ci și valabilitatea probelor colectate prin intermediul programelor spion în cazurile transfrontaliere și că sunt necesare în mod clar standarde comune la nivelul UE în temeiul titlului 5 capitolul 4 din TFUE care reglementează utilizarea programelor spion de către organismele statelor membre, pe baza standardelor stabilite de CJUE, CEDO, Comisia de la Veneția și Agenția pentru

Drepturi Fundamentale[30]; consideră că astfel de standarde ale UE ar trebui să acopere cel puțin următoarele elemente:

(a) utilizarea preconizată a programelor spion trebuie să fie autorizată numai în cazuri excepționale și specifice, pentru a proteja securitatea națională, și să facă obiectul unei autorizații judiciare ex ante eficace, obligatorii și semnificative din partea unei autorități judiciare imparțiale și independente sau a altui organism independent de supraveghere democratică, care să aibă acces la toate informațiile relevante și să demonstreze necesitatea și proporționalitatea măsurii avute în vedere;

(b) vizarea cu programe spion ar trebui să dureze numai atât timp cât este strict necesar, autorizația judiciară prealabilă ar trebui să definească domeniul de aplicare și durata exactă pentru fiecare dispozitiv accesat, iar pirateria informatică poate fi prelungită numai atunci când se acordă o autorizație judiciară suplimentară pentru o altă durată specificată, având în vedere natura programelor spion și posibilitatea unei supravegheri retroactive; în plus, autoritățile statelor membre ar trebui să vizeze numai dispozitivele sau conturile individuale ale utilizatorilor finali și să se abțină de la piratarea furnizorilor de servicii de internet și tehnologie, pentru a evita afectarea utilizatorilor nevizați;

(c) autorizația de utilizare a programelor spion poate fi acordată în cazuri excepționale numai în ceea ce privește anchetele privind o listă limitată și închisă de infracțiuni grave, definite clar și precis, care reprezintă o amenințare reală la adresa securității naționale, iar programele spion pot fi utilizate numai în cazul persoanelor în legătură cu care există suficiente indicii că au comis sau intenționează să comită astfel de infracțiuni grave;

(d) datele protejate de privilegii sau imunități care se referă la categorii de persoane (cum ar fi politicienii, medicii etc.) sau la relații protejate în mod specific (cum ar fi secretul profesional al avocatului) ori de norme privind determinarea și limitarea răspunderii penale referitoare la libertatea presei și la libertatea de exprimare în alte mijloace de comunicare nu trebuie să fie vizate de programele spion, cu excepția cazului în care există motive suficiente, stabilite sub supraveghere judiciară, care să confirme implicarea în activități infracționale sau în chestiuni de securitate națională, care ar trebui să facă obiectul unui cadru comun;

(e) trebuie elaborate norme specifice pentru supravegherea cu ajutorul tehnologiei spion, având în vedere că aceasta permite un acces retroactiv nelimitat la mesaje, fișiere și metadate;

(f) statele membre ar trebui să publice cel puțin numărul de cereri de supraveghere aprobate și respinse, precum și tipul și scopul investigației și să înregistreze în mod anonim fiecare investigație într-un registru național cu un identificator unic, astfel încât aceasta să poată fi investigată în cazul unor suspiciuni de abuz;

[30] Agenția pentru Drepturi Fundamentale a Uniunii Europene, „Supravegherea de către serviciile de informații: măsurile de protecție și căile de recuperare a prejudiciului privind drepturile fundamentale în Uniunea Europeană – volumul II – Rezumat”, 2017 https://fra.europa.eu/en/publication/2017/surveillance-intelligence-services-fundamental-rights-safeguards-and-remedies-eu.

(g) organismele naționale de control ar trebui să raporteze statelor membre, iar statele membre ar trebui să notifice ulterior Comisiei aceste informații în mod regulat; Comisia ar trebui să utilizeze aceste informații în raportul său anual privind statul de drept pentru a permite compararea utilizării programelor spion în statele membre;

(h) dreptul de notificare al persoanei vizate: după încheierea supravegherii, autoritățile ar trebui să notifice persoanei faptul că a făcut obiectul utilizării de programe spion de către autorități și să îi furnizeze informații privind data și durata supravegherii, mandatul emis pentru operațiunea de supraveghere, datele obținute, informații cu privire la modul în care au fost utilizate aceste date și de către ce actori, data la care datele au fost șterse, precum și dreptul și aspectele practice de exercitare a căilor de atac administrative și judiciare în fața autorităților competente; consideră că această notificare ar trebui trimisă fără întârzieri nejustificate, cu excepția cazului în care o autoritate judiciară independentă dispune întârzierea notificării, deoarece notificarea imediată ar periclita grav scopul supravegherii;

(i) dreptul de notificare al persoanelor nevizate ale căror date au fost accesate: după încheierea perioadei pentru care supravegherea a fost autorizată, autoritățile ar trebui să notifice persoanele al căror drept la viața privată a fost grav afectat prin utilizarea programelor spion, dar care nu au fost ținta operațiunii; autoritățile ar trebui să notifice aceste persoane cu privire la faptul că datele lor au fost accesate de autorități, să le furnizeze informații privind data și durata supravegherii, mandatul emis pentru operațiunea de supraveghere, datele obținute, informații cu privire la modul în care au fost utilizate aceste date și de către ce actori, precum și data la care datele au fost șterse; consideră că această notificare ar trebui trimisă fără întârzieri nejustificate, cu excepția cazului în care o autoritate judiciară independentă dispune întârzierea notificării, deoarece notificarea imediată ar periclita grav scopul supravegherii;

(j) o supraveghere ex post eficace, obligatorie și independentă a utilizării programelor spion, organismele responsabile care trebuie să dispună de toate mijloacele și competențele necesare pentru a exercita o supraveghere semnificativă și să fie însoțită de o supraveghere parlamentară la care să participe mai multe partide, cu autorizația adecvată, cu acces deplin la suficiente informații pentru a confirma că supravegherea a fost efectuată în mod legal și proporțional, și o supraveghere parlamentară a informațiilor confidențiale sensibile, care ar trebui să fie facilitată de infrastructura, procesele și autorizațiile de securitate necesare; indiferent de definiția sau delimitarea conceptului de securitate națională, organismele naționale de supraveghere trebuie să fie competente pentru domeniul de aplicare complet al securității naționale;

(k) regimul de reglementare a programelor spion de supraveghere trebuie să se bazeze pe principiile fundamentale ale respectării garanțiilor procedurale și ale controlului judiciar;

(l) o cale de atac eficientă pentru persoanele care au fost vizate direct și indirect; persoanele care susțin că sunt afectate negativ de supraveghere trebuie să aibă acces la căi de atac prin intermediul unui organism independent; solicită, prin urmare, introducerea unei obligații de notificare pentru autoritățile de stat și a unor termene adecvate pentru notificare, care să prevadă că notificarea trebuie să aibă loc odată ce amenințarea la adresa securității a trecut;

(m) căile de atac legale trebuie să fie eficiente atât în drept, cât și în fapt și să fie cunoscute și accesibile; subliniază că aceste căi de atac necesită o anchetă rapidă, aprofundată și imparțială din partea unui organism independent de supraveghere și că acest organism ar trebui să aibă acces, precum și expertiză și capacități tehnice pentru a gestiona toate datele relevante pentru a putea stabili dacă evaluarea de securitate efectuată de autorități asupra unei persoane este fiabilă și proporțională; în cazurile în care au fost confirmate abuzuri, ar trebui să se aplice sancțiuni adecvate de natură penală sau administrativă, în conformitate cu dreptul național relevant din statele membre;

(n) îmbunătățirea accesului gratuit al persoanelor vizate de expertiza tehnologică în această etapă, deoarece creșterea disponibilității și a accesibilității proceselor tehnologice, cum ar fi analiza criminalistică, ar permite persoanelor vizate să prezinte cauze mai puternice în instanță și ar îmbunătăți reprezentarea persoanelor vizate în instanță prin consolidarea capacității tehnologice a reprezentării juridice și a sistemului judiciar pentru a consilia mai bine persoanele vizate, a identifica încălcările, a îmbunătăți supravegherea și răspunderea pentru abuzul de programe spion;

(o) consolidarea dreptului la apărare și a dreptului la un proces echitabil prin garantarea faptului că persoanele acuzate de infracțiuni au dreptul și posibilitatea de a verifica acuratețea, autenticitatea, fiabilitatea și chiar legalitatea probelor folosite împotriva lor și, prin urmare, de a respinge orice aplicare generală a normelor de secretizare prin invocarea apărării naționale;

(p) în timpul supravegherii, autoritățile ar trebui să șteargă toate datele care sunt irelevante pentru investigația autorizată și, după încheierea supravegherii și a investigației pentru care a fost acordată autorizația, autoritățile ar trebui să șteargă datele și orice documente conexe, cum ar fi notele care au fost luate în perioada respectivă, iar ștergerea trebuie să fie înregistrată și să poată fi auditată;

(q) informațiile relevante obținute prin intermediul programelor spion ar trebui să fie accesibile numai autorităților autorizate și numai în scopul unei operațiuni; acest acces ar trebui să fie limitat la o anumită perioadă, astfel cum se specifică în procesul judiciar;

(r) trebuie stabilite standarde minime privind drepturile persoanelor în cadrul procedurilor penale privind admisibilitatea probelor colectate cu ajutorul programelor spion; riscul de informații false sau manipulate ca urmare a implementării programelor spion (fals privind identitatea, bazat pe asemănare) trebuie să fie inclus în dreptul procesual penal;

(s) statele membre trebuie să se informeze reciproc în cazul supravegherii cetățenilor sau rezidenților unui alt stat membru sau a unui număr mobil al unui operator dintr-un alt stat membru;

(t) în software-ul de supraveghere trebuie inclus un identificator, astfel încât organismele de supraveghere să poată identifica în mod clar utilizatorul în caz de suspiciune de abuz; semnătura obligatorie pentru fiecare instalare de programe spion ar trebui să fie compusă dintr-o etichetă individuală pentru autoritatea care acționează, tipul de program spion utilizat și un număr de caz anonimizat;

33. invită statele membre să organizeze consultări publice cu părțile interesate, să asigure transparența procesului legislativ și să includă standardele și garanțiile UE atunci când

elaborează o nouă legislație privind utilizarea și vânzarea de programe spion;

34. subliniază că numai programele spion proiectate astfel încât să permită și să faciliteze funcționalitatea programelor spion în conformitate cu cadrul legislativ prevăzut la alineatul (29) pot fi introduse pe piața internă, dezvoltate sau utilizate în Uniune; afirmă că un astfel de regulament privind introducerea pe piață a programelor spion, care prevede „statul de drept începând cu momentul conceperii”, în temeiul articolului 114 din TFUE, ar trebui să acorde cetățenilor Uniunii un nivel ridicat de protecție; consideră că este nejustificat ca, deși Regulamentul privind produsele cu dublă utilizare a oferit cetățenilor țărilor terțe protecție împotriva exporturilor de programe spion din UE începând din 2021, cetățenilor UE nu li se oferă o protecție echivalentă;

35. consideră că numai tehnologia de interceptare și extracție poate fi vândută de întreprinderile din UE și achiziționată de statele membre, și nu „pirateria informatică ca serviciu”, care include furnizarea de sprijin tehnic, operațional și metodologic pentru tehnologia de supraveghere și permite accesul furnizorului la un volum disproporționat de date care este incompatibil cu principiile proporționalității, necesității, legitimității, legalității și adecvării; invită Comisia să formuleze o propunere legislativă în această privință;

36. subliniază că programele spion pot fi introduse pe piață pentru vânzare și utilizare, pe baza unei liste închise, de către autoritățile publice care au ca instrucțiuni să realizeze anchete privind infracțiuni sau protecția securității naționale pentru care poate fi autorizată utilizarea programelor spion; consideră că agențiile de securitate ar trebui să utilizeze programe spion numai după ce toate recomandările formulate de Agenția pentru Drepturi Fundamentale au fost puse în aplicare[31];

37. subliniază obligația de a utiliza o versiune de programe spion care este concepută astfel încât să reducă la minimum accesul la toate datele stocate pe un dispozitiv, dar care ar trebui concepută astfel încât să limiteze accesul la date la strictul necesar în sensul investigației autorizate;

38. concluzionează că, atunci când un stat membru achiziționează programe spion, achiziția trebuie să poată fi auditată de un organism de audit independent și imparțial care deține autorizația corespunzătoare;

39. subliniază că toate entitățile care introduc programe spion pe piața internă ar trebui să respecte cerințe stricte privind diligența necesară, iar întreprinderile care depun o cerere în cadrul unui proces de achiziții publice pentru a fi furnizori ar trebui să fie supuse unui proces de verificare care include răspunsul întreprinderii la încălcările drepturilor omului comise cu ajutorul software-ului lor și dacă tehnologia se bazează pe date colectate în cadrul unor practici de supraveghere nedemocratice și abuzive; subliniază că autoritățile naționale de supraveghere competente ar trebui să raporteze anual Comisiei cu privire la conformitate;

40. subliniază că întreprinderile care oferă tehnologii sau servicii de supraveghere actorilor statali ar trebui să dezvăluie autorităților naționale de supraveghere competente natura

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

licențelor de export;

41. accentuează că statele membre ar trebui să stabilească o perioadă de incompatibilitate care să împiedice temporar foștii angajați ai organismelor sau ai agențiilor guvernamentale să lucreze pentru companiile de programe spion;

Necesitatea unor limite ale securității naționale

42. este îngrijorat de cazurile de invocare nejustificată a „securității naționale” pentru a justifica desfășurarea și utilizarea programelor spion, precum și pentru a asigura secretul absolut și lipsa de răspundere; salută declarația Comisiei, care corespunde jurisprudenței CJUE[32], potrivit căreia simpla referire la securitatea națională nu poate fi interpretată ca fiind o excepție nelimitată de la aplicarea dreptului UE și ar trebui să necesite o justificare clară și invită Comisia să susțină această declarație în cazurile în care există indicii că există abuzuri; consideră că într-o societate transparentă democratică care respectă statul de drept, astfel de limitări în numele securității naționale vor fi mai degrabă excepția decât regula;

43. consideră că noțiunea de securitate națională trebuie analizată în lumina noțiunii mai restrânse de securitate internă, aceasta din urmă având un domeniu de aplicare mai larg, incluzând prevenirea riscurilor pentru cetățeni și, în special, aplicarea dreptului penal;

44. regretă dificultățile provocate de lipsa unei definiții juridice comune a securității naționale, care să stabilească criterii pentru determinarea regimului juridic aplicabil în materie de securitate națională, precum și o delimitare clară a zonei în care se poate aplica un astfel de regim special;

45. consideră că utilizarea programelor spion constituie o limitare a drepturilor fundamentale; consideră, de asemenea, că, în cazul în care un concept este utilizat într-un context juridic care implică transferul de drepturi și impunerea de obligații (și, în special, limitări ale drepturilor fundamentale ale persoanelor), conceptul trebuie să fie clar și previzibil pentru toate persoanele afectate de acesta; reamintește că Carta drepturilor fundamentale prevede că orice limitare a drepturilor fundamentale în conformitate cu articolul 52 alineatul (1) trebuie să fie prevăzută prin lege; consideră, prin urmare, că este necesar să se definească în mod clar „securitatea națională”; subliniază că, indiferent de delimitarea precisă, domeniul securității naționale trebuie să facă obiectul unei supravegheri independente, obligatorii și eficace în toate elementele sale;

46. subliniază că, în cazul în care autoritățile invocă motive de securitate națională pentru a justifica utilizarea programelor spion, acestea ar trebui, în plus față de cadrul stabilit la punctul 29, să demonstreze conformitatea cu legislația UE, inclusiv respectarea principiilor proporționalității, necesității, legitimității, legalității și adecvării; subliniază că justificarea ar trebui să fie ușor accesibilă și pusă la dispoziția unui organism național

[32] Hotărârea din 6 octombrie 2020, Privacy International/Secretary of State for Foreign and Commonwealth Affairs și alții, C-623/17, EU:C:2020:790, punctul 44 și hotărârile din 6 octombrie 2020, cauzele conexate C-511/18, C-512/18 și C-520/18, La Quadrature du Net și alții/Premier ministre și alții, EU:C:2020:791, punctul 99: „simplul fapt că o măsură națională a fost adoptată în vederea protejării securității naționale nu poate să determine inaplicabilitatea dreptului Uniunii și nici să absolve statele membre de necesitatea de a respecta acest drept”.

de control pentru evaluare;

47. reiterează, în acest context, faptul că toate statele membre au semnat Convenția 108+, care stabilește standarde și obligații pentru protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, inclusiv în scopuri de securitate națională; subliniază că Convenția 108+ este un cadru european obligatoriu privind prelucrarea datelor de către serviciile de informații și de securitate; îndeamnă toate statele membre să ratifice fără întârziere această convenție, să pună deja în aplicare standardele sale în legislația națională și să acționeze în consecință cu privire la securitatea națională;

48. subliniază că excepțiile și restricțiile la un număr limitat de dispoziții ale convenției sunt permise numai atunci când sunt în conformitate cu cerințele menționate la articolul 11 din convenție, ceea ce înseamnă că, atunci când se pune în aplicare Convenția 108+, fiecare excepție și restricție specifică trebuie să fie prevăzută de lege, trebuie să respecte esența drepturilor și libertăților fundamentale și trebuie să justifice faptul că „constituie o măsură necesară și proporțională într-o societate democratică” pentru unul dintre motivele legitime enumerate la articolul 11[33] și că aceste excepții și restricții nu trebuie să afecteze „examinarea și supravegherea independente și eficace în temeiul legislației interne a părții respective”;

49. constată, de asemenea, că Convenția 108 + subliniază că supravegherea „are competențe de investigare și de intervenție”; consideră că o revizuire și o supraveghere eficace implică competențe obligatorii atunci când impactul asupra drepturilor fundamentale este cel mai mare, în special în fazele de accesare, analiză și stocare a datelor cu caracter personal;

50. consideră că lipsa unor competențe obligatorii ale organismelor de supraveghere din domeniul securității naționale este incompatibilă cu criteriul stabilit în Convenția 108 +, potrivit căruia acest lucru „constituie o măsură necesară și proporțională într-o societate democratică”;

51. subliniază că Convenția 108+ permite un număr foarte limitat de excepții în ceea ce privește articolul 15, dar nu permite astfel de excepții, în special în ceea ce privește alineatul (2) [obligații de sensibilizare], alineatul (3) [consultarea privind măsurile legislative și administrative], alineatul (4) [cereri și plângeri din partea persoanelor fizice], alineatul (5) [independență și imparțialitate], alineatul (6) [resurse necesare pentru îndeplinirea eficientă a sarcinilor], alineatul (7) [raportare periodică], alineatul (8) [confidențialitate], punctul 9 [posibilitatea de a introduce o cale de atac] și punctul 10 [necesitatea organismelor atunci când acționează în exercitarea funcției lor judiciare];

O mai bună punere în aplicare și asigurare a aplicării legislației în vigoare

[33] Această evaluare este prevăzută în jurisprudența CEDO, care stabilește că sarcina probei revine statului/legiuitorului. Jurisprudența relevantă a CEDO include: Roman Zakharov împotriva Rusiei (Cererea nr. 47143/06), 4 decembrie 2015; Szabó și Vissy împotriva Ungariei (Cererea nr. 37138/14), 12 ianuarie 2016; Big Brother Watch și alții împotriva Regatului Unit (Cererea nr. 58170/13, 62322/14 și 24969/15), 25 mai 2021 și Centrum För Rättvisa împotriva Suediei (Cererea nr. 35252/08), 25 mai 2021.

52. subliniază deficiențele cadrelor juridice naționale și necesitatea unei mai bune aplicări a legislației existente a Uniunii pentru a contracara aceste deficiențe; consideră că următoarele acte legislative ale Uniunii sunt relevante, dar aplicate și/sau implementate prea des în mod necorespunzător: directiva privind combaterea spălării banilor, directiva privind protecția datelor în materie de asigurare a respectării legii, normele privind achizițiile publice, regulamentul privind produsele cu dublă utilizare, jurisprudența (hotărâri privind supravegherea și securitatea națională) și directiva privind avertizorii de integritate; invită Comisia să investigheze și să raporteze cu privire la deficiențele în punerea în aplicare și asigurarea respectării legislației și să prezinte o foaie de parcurs pentru corectarea acestor deficiențe până la 1 august 2023 cel târziu;

53. consideră esențiale punerea în aplicare corespunzătoare și asigurarea respectării stricte a cadrului juridic al Uniunii privind protecția datelor, în special a Directivei privind protecția datelor, a Regulamentului general privind protecția datelor și a Directivei asupra confidențialității și comunicațiilor electronice; consideră la fel de importantă punerea în aplicare deplină a hotărârilor relevante ale CJUE, care încă nu are loc în unele state membre; reamintește că Comisia are un rol central în asigurarea respectării dreptului UE și în asigurarea aplicării sale uniforme în întreaga Uniune și ar trebui să utilizeze toate instrumentele disponibile, inclusiv procedurile de constatare a neîndeplinirii obligațiilor în caz de nerespectare persistentă;

54. solicită ca Aranjamentul de la Wassenaar să devină un acord obligatoriu pentru toți participanții, cu scopul de a-l transforma într-un tratat internațional;

55. solicită Ciprului și Israelului să devină state participante la Aranjamentul de la Wassenaar; reamintește statelor membre că trebuie depuse toate eforturile pentru a permite Ciprului și Israelului să adere la Aranjamentul de la Wassenaar;

56. subliniază că Aranjamentul de la Wassenaar ar trebui să includă un cadru privind drepturile omului care să prevadă norme privind acordarea de licențe pentru tehnologiile de spionaj, să evalueze și să revizuiască conformitatea întreprinderilor producătoare de tehnologii de spionaj și că participanții ar trebui să interzică achiziționarea de tehnologii de supraveghere de la statele care nu sunt parte la aranjament;

57. subliniază că, având în vedere dezvăluirile privind programele spion, Comisia și statele membre ar trebui să efectueze o investigație aprofundată a licențelor de export acordate pentru utilizarea programelor spion în temeiul Regulamentului privind produsele cu dublă utilizare, iar Comisia ar trebui să transmită Parlamentului rezultatele acestei evaluări;

58. subliniază că este nevoie de trasabilitate și responsabilitate pentru exporturile de programe spion și reamintește că companiile din UE ar trebui să poată exporta numai acele programe spion care demonstrează suficiente proprietăți de trasabilitate, necesare pentru a garanta că responsabilitatea poate fi întotdeauna atribuită;

59. subliniază că Comisia trebuie să verifice periodic și să pună în aplicare în mod corespunzător Regulamentul reformat privind produsele cu dublă utilizare pentru a evita situațiile în care se caută regimul de export cel mai favorabil în întreaga Uniune, așa cum se întâmplă în prezent în Bulgaria și Cipru, și că Comisia ar trebui să dispună de

resurse adecvate pentru această sarcină;

60. invită Comisia să asigure o capacitate de personal suficientă pentru unitățile responsabile cu supravegherea și aplicarea Regulamentului privind produsele cu dublă utilizare;

61. solicită modificarea Regulamentului privind produsele cu dublă utilizare pentru a clarifica la articolul 15 faptul că autorizațiile de export pentru produsele cu dublă utilizare nu trebuie acordate în cazul în care bunurile sunt sau pot fi destinate pentru acte de represiune internă și/sau comitere a unor încălcări grave ale drepturilor omului și ale dreptului internațional umanitar; solicită aplicarea deplină a verificărilor de diligență necesară și drepturile omului în procesul de acordare a licențelor și îmbunătățiri ulterioare, cum ar fi măsuri reparatorii pentru țintele încălcărilor drepturilor omului și raportarea transparentă a diligenței necesare efectuate;

62. solicită modificarea Regulamentului privind produsele cu dublă utilizare pentru a se garanta că tranzitul este interzis în cazurile în care bunurile sunt sau pot fi destinate represiunii interne și/sau săvârșirii unor încălcări grave ale drepturilor omului și ale dreptului internațional umanitar;

63. subliniază că, la o viitoare modificare a Regulamentului privind produsele cu dublă utilizare, autoritățile naționale desemnate responsabile cu aprobarea și refuzarea licențelor de export pentru produsele cu dublă utilizare ar trebui să furnizeze rapoarte detaliate, inclusiv informații privind produsele cu dublă utilizare în cauză, numărul de licențe solicitate, numele țării de export, o descriere a întreprinderii exportatoare și dacă această întreprindere este o filială, o descriere a utilizatorului final și a destinației; valoarea licenței de export; precum și motivul pentru care licența de export a fost aprobată sau refuzată; subliniază că aceste rapoarte ar trebui făcute publice trimestrial; solicită înființarea unei comisii parlamentare permanente specifice, care să aibă acces la informații clasificate de la Comisie, în scopul realizării controlului parlamentar;

64. subliniază că, la o viitoare modificare a Regulamentului privind produsele cu dublă utilizare, trebuie eliminată excepția de la cerința de a furniza informații Comisiei pe motive de sensibilitate comercială, de apărare și de politică externă sau pe motive de securitate națională; consideră, în schimb, că, pentru a împiedica accesul țărilor din afara UE la informații sensibile, Comisia poate decide să clasifice anumite informații în raportul său anual;

65. subliniază că definiția produselor de supraveghere cibernetică din Regulamentul reformat privind produsele cu dublă utilizare nu poate fi interpretată restrictiv, ci ar trebui să includă toate tehnologiile din acest domeniu, cum ar fi interceptarea telecomunicațiilor mobile sau echipamentele de bruiaj; programele software de intruziune; sistemele sau echipamentele de supraveghere a comunicațiilor în rețea prin IP; software-ul special conceput sau modificat pentru monitorizare sau analiză de către autoritățile de aplicare a legii; echipamentele laser de detecție acustică; instrumentele criminalistice care extrag date brute dintr-un dispozitiv informatic sau de comunicații și care eludează controalele de „autentificare” sau de autorizare a dispozitivului; sistemele sau echipamentele electronice concepute pentru supravegherea și monitorizarea spectrului electromagnetic în scopuri militare sau de securitate; și vehiculele aeriene

fără pilot capabile să desfășoare activități de supraveghere;

66. solicită să se introducă acte legislative europene suplimentare care să impună actorilor corporativi care produc și/sau exportă tehnologii de supraveghere să includă cadre privind drepturile omului și obligația de diligență, în conformitate cu Principiile directoare ale ONU privind afacerile și drepturile omului (UNGP);

Cooperarea internațională pentru protecția cetățenilor

67. solicită o strategie comună UE-SUA în materie de programe spion, inclusiv o listă albă și/sau neagră comună de furnizori de programe spion ale căror instrumente au fost sau riscă să fie utilizate în mod abuziv de către guverne străine cu un bilanț slab în materie de drepturile omului pentru a viza într-un mod rău intenționat funcționari guvernamentali, jurnaliști și societatea civilă și care acționează împotriva securității și a politicii externe a Uniunii, care (nu) sunt autorizați să vândă autorităților publice, criterii comune pentru ca vânzătorii să fie incluși pe oricare dintre liste, acorduri pentru raportarea comună UE-SUA cu privire la industrie, un control comun, obligații comune de diligență pentru vânzători și incriminarea vânzării de programe spion către actori nestatali;

68. solicită Consiliului UE-SUA pentru comerț și tehnologie să organizeze consultări ample și deschise cu societatea civilă pentru dezvoltarea strategiei și standardelor comune UE-SUA, inclusiv a listei albe și/sau negre comune;

69. solicită lansarea unor discuții cu alte țări, în special cu Israelul, pentru a stabili un cadru privind comercializarea programelor spion și licențele de export, inclusiv norme privind transparența, o listă a țărilor eligibile din punctul de vedere al standardelor de drepturile omului și mecanisme de diligență necesară;

70. ia act de faptul că, în comparație cu SUA, unde NSO a fost inclusă rapid pe lista neagră, iar președintele SUA a semnat un ordin executiv, în care se afirmă că nu trebuie să utilizeze în mod operațional programe spion comerciale care prezintă riscuri semnificative de contrainformații sau de securitate pentru guvernul Statelor Unite sau riscuri semnificative de utilizare necorespunzătoare de către un guvern străin sau de către o persoană străină, nu au fost luate măsuri suficiente la nivelul UE în ceea ce privește importurile de programe spion și aplicarea normelor de export;

71. conchide că normele Uniunii privind exporturile și punerea lor în aplicare trebuie înăsprite pentru protecția drepturilor omului în țările din afara UE și trebuie să dispună de instrumentele necesare pentru a le pune în aplicare în mod eficace prevederile; reamintește că UE ar trebui să încerce să își unească forțele cu SUA și cu alți aliați în reglementarea comerțului cu programe spion și în utilizarea puterii lor de piață combinate pentru a forța schimbarea și să stabilească standarde solide de transparență, trasabilitate și responsabilitate pentru utilizarea tehnologiei de supraveghere, care ar trebui să culmineze cu o inițiativă la nivelul Organizației Națiunilor Unite;

Vulnerabilitățile de ziua zero

72. solicită să se reglementeze descoperirea, partajarea, corectarea și exploatarea vulnerabilităților, precum și procedurile de divulgare, definitivând astfel baza stabilită

de Directiva (UE) 2022/2555[34] (Directiva NIS 2) și propunerea de act legislativ privind reziliența cibernetică[35];

73. consideră că cercetătorii trebuie să fie în măsură să analizeze vulnerabilitățile și să își partajeze rezultatele fără răspundere civilă și penală, în temeiul Directivei privind criminalitatea informatică și al Directivei privind drepturile de autor, printre altele;

74. invită principalii actori din industrie să creeze stimulente pentru ca cercetătorii să participe la analizarea vulnerabilităților, investind în planuri de tratament al vulnerabilităților, în practici de dezvăluire a informațiilor în cadrul industriei și cu societatea civilă și să desfășoare programe de stimulare a identificării bugurilor;

75. invită Comisia să își sporească sprijinul și finanțarea pentru programele de stimulare a identificării erorilor și pentru alte proiecte care vizează identificarea și corectarea de vulnerabilități de securitate și să instituie o abordare coordonată între statele membre în ceea ce privește divulgarea obligatorie a vulnerabilităților;

76. solicită interzicerea vânzării vulnerabilităților într-un sistem în orice alt scop decât consolidarea securității sistemului respectiv, precum și obligația de a dezvălui rezultatele tuturor cercetărilor privind vulnerabilitatea într-un mod coordonat și responsabil, care să promoveze siguranța publică și să reducă la minimum riscul de exploatare a vulnerabilității;

77. invită entitățile publice și private să creeze un punct de contact accesibil public, unde vulnerabilitățile să poată fi raportate într-un mod coordonat și responsabil, iar organizațiile care primesc informații cu privire la vulnerabilitățile din sistemul lor să acționeze imediat pentru a le remedia; atunci când sunt disponibile corecții, organizațiile ar trebui să fie obligate să dispună de măsuri adecvate pentru a asigura o implementare rapidă și garantată, în cadrul unui proces coordonat și responsabil de divulgare;

78. consideră că statele membre ar trebui să aloce suficiente resurse financiare, tehnice și umane pentru cercetarea în domeniul securității și corectarea vulnerabilităților;

79. invită statele membre să dezvolte procese de echitate a vulnerabilităților, prevăzute de lege, care să stabilească faptul că, în mod implicit, vulnerabilitățile trebuie dezvăluite și neexploatate și că orice decizie de a se abate de la aceasta trebuie să constituie o excepție și să fie evaluată în conformitate cu cerințele privind necesitatea și proporționalitatea, inclusiv să analizeze dacă infrastructura afectată de vulnerabilitate este utilizată de o mare parte a populației și să facă obiectul unei supravegheri stricte de către un organism independent de supraveghere, precum și al unor proceduri și decizii transparente;

---

[34] Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148, JO L 333, 27.12.2022, p. 80.

[35] Propunerea din 15 septembrie 2022 de regulament al Parlamentului European și al Consiliului privind cerințele orizontale de securitate cibernetică pentru produsele cu elemente digitale și de modificare a Regulamentului (UE) 2019/1020, (COM(2022)0454).

Rețelele de telecomunicații

80. subliniază că ar trebui revocată licența oricărui furnizor de servicii despre care s-a constatat că facilitează accesul ilegal la infrastructura națională și/sau internațională de semnalizare mobilă pentru toate generațiile (în prezent, 2G-5G);

81. subliniază că procesele prin care noi numere de telefon din întreaga lume pot fi create de către actori răuvoitori ar trebui să fie mai bine reglementate, astfel încât activitățile ilicite să fie mai dificil de ascuns;

82. subliniază că furnizorii de servicii de telecomunicații trebuie să se asigure că au capacitatea de a detecta posibila utilizare abuzivă a accesului, a controlului sau a utilizării finale efective a infrastructurii de semnalizare obținute de terți prin acorduri comerciale sau de altă natură în statul membru în care își desfășoară activitatea;

83. invită statele membre să se asigure că autoritățile naționale competente, în conformitate cu dispozițiile Directivei NIS 2, evaluează nivelul de reziliență a furnizorilor de telecomunicații la intruziunile neautorizate;

84. invită furnizorii de telecomunicații să ia măsuri ferme și demonstrabile de a reduce diferitele forme de emulare neautorizată a inițierii de trafic de telecomunicații de către un element al rețelei pentru a accesa datele sau serviciile destinate utilizatorilor legitimi și alte activități care implică manipularea funcționării normale a elementelor și a infrastructurii rețelelor mobile în scopuri de supraveghere de către actori rău-intenționați, inclusiv actori statali, precum și grupuri infracționale;

85. invită statele membre să ia măsuri pentru a se asigura că actorii statali din afara UE care nu respectă drepturile fundamentale nu au control sau utilizare finală efectivă a infrastructurii strategice și nici nu influențează deciziile legate de infrastructura strategică din Uniune, inclusiv asupra infrastructurii de telecomunicații;

86. invită toate statele membre să acorde prioritate unor investiții mai mari în protecția infrastructurilor critice, cum ar fi sistemele naționale de telecomunicații, pentru a acoperi lacunele de protecție împotriva încălcărilor vieții private, scurgerile de date și intruziunile neautorizate, pentru a apăra drepturile fundamentale ale cetățenilor;

87. invită autoritățile naționale competente să promoveze în mod activ consolidarea capacităților furnizorilor, precum și a capacităților de răspuns, pentru a sprijini mai bine identificarea persoanelor vizate în mod ilegal, notificarea și raportarea incidentelor, cu scopul de a oferi asigurări continue și măsurabile și de a atenua exploatarea lacunelor în materie de securitate de către actorii răuvoitori din afara UE și interni;

Viața privată și comunicațiile electronice

88. solicită adoptarea rapidă a Regulamentului privind viața privată și comunicațiile electronice într-un mod care să reflecte pe deplin jurisprudența privind restricțiile pentru securitatea națională și necesitatea de a preveni utilizarea abuzivă a tehnologiilor de supraveghere, care să consolideze dreptul fundamental la viață privată și să ofere garanții solide și o aplicare efectivă; subliniază că domeniul de aplicare al interceptării legale nu ar trebui să depășească domeniul de aplicare al Directivei asupra

confidențialității și comunicațiilor electronice (2002/58/CE);

89 solicită protecția tuturor comunicațiilor electronice, a conținutului și a metadatelor împotriva utilizării abuzive a datelor cu caracter personal și a comunicațiilor private de către companiile private și autoritățile guvernamentale; subliniază că instrumentele de siguranță digitală asigurată prin proiectare, cum ar fi criptarea de la un capăt la altul, nu ar trebui să fie slăbite;

90. invită Comisia să evalueze punerea în aplicare de către statele membre a Directivei asupra confidențialității și comunicațiilor electronice în întreaga UE și să inițieze proceduri de constatare a neîndeplinirii obligațiilor în cazul în care apar încălcări ale acesteia;

Rolul Europol

91. ia act de faptul că o scrisoare a Europol adresată președintelui Comisiei PEGA din aprilie 2023 informează comisia că Europol a contactat Grecia, Ungaria, Bulgaria, Spania și Polonia pentru a verifica dacă există anchete penale în curs sau preconizate sau alte anchete în temeiul dispozițiilor aplicabile din legislația națională, care ar putea fi sprijinite de Europol; subliniază că oferirea de asistență statelor membre nu constituie inițierea, desfășurarea sau coordonarea unei anchete penale, astfel cum se prevede la articolul 6;

92. invită Europol să facă uz pe deplin de competențele pe care le-a dobândit recent în temeiul articolului 6 alineatul (1a) din Regulamentul (UE) 2022/991, care îi permite să propună autorităților competente ale statelor membre în cauză să inițieze, să desfășoare sau să coordoneze o anchetă, după caz; reamintește că, în conformitate cu articolul 6, este de competența statelor membre să respingă o astfel de propunere;

93. invită toate statele membre să se angajeze în fața Parlamentului European și a Consiliului că implică Europol în anchetele privind acuzațiile de utilizare ilegală a programelor spion la nivel național, în special atunci când a fost făcută o propunere în temeiul articolului 6 alineatul (1a) din Regulamentul (UE) 2022/991;

94. invită statele membre să creeze, în cadrul Europol, un registru al operațiunilor naționale de aplicare a legii care implică utilizarea programelor spion, în care fiecare operațiune să fie identificată printr-un cod, iar utilizarea programelor spion de către guverne să fie inclusă în raportul anual al Europol de evaluare a amenințării pe care o reprezintă criminalitatea organizată pe internet;

95. consideră că trebuie lansat un proces de reflecție cu privire la rolul Europol în cazul în care autoritățile naționale nu reușesc sau refuză să investigheze și există amenințări clare la adresa intereselor și securității UE;

Politicile pentru dezvoltare ale Uniunii

96. invită Comisia și SEAE să implementeze mecanisme de control mai riguroase pentru a se asigura că ajutorul pentru dezvoltare al Uniunii, inclusiv donarea de tehnologie de supraveghere și formare privind implementarea programelor informatice de supraveghere, nu finanțează sau facilitează instrumente sau activități care ar putea afecta

principiile democrației, bunei guvernanțe, statului de drept și respectării drepturilor omului sau care periclitează securitatea internațională sau securitatea esențială a Uniunii și a statelor sale membre; ia act de faptul că evaluările privind respectarea dreptului Uniunii efectuate de Comisie, în special a Regulamentului financiar, ar trebui să conțină criterii specifice de control și mecanisme de punere în aplicare pentru a preveni astfel de abuzuri, inclusiv posibila suspendare temporară a unor proiecte specifice, în cazul în care se detectează o încălcare a acestor principii;

97. invită Comisia și SEAE să includă în toate procedurile de evaluare a impactului asupra drepturilor omului și a drepturilor fundamentale o procedură de monitorizare a potențialei utilizări abuzive a supravegherii, care să țină seama pe deplin de articolul 51 din Carta drepturilor fundamentale, în termen de un an [de la publicarea recomandărilor PEGA]; subliniază că această procedură trebuie prezentată Parlamentului și Consiliului și că această evaluare a impactului trebuie efectuată înainte de acordarea oricărui sprijin țărilor din afara UE;

98. invită SEAE să raporteze cu privire la abuzul de programe spion împotriva apărătorilor drepturilor omului în Raportul anual al UE privind drepturile omului și democrația;

Normele financiare ale Uniunii

99. subliniază că respectarea drepturilor omului de către sectorul financiar trebuie consolidată; subliniază că recomandările UNGP 10 + trebuie transpuse în dreptul Uniunii și că Directiva privind diligența necesară ar trebui să se aplice pe deplin sectorului financiar, pentru a asigura respectarea democrației, a drepturilor omului și a statului de drept în sectorul financiar;

100. este preocupat de implicațiile deciziei CJUE privind Directiva (UE) 2018/843 privind prevenirea utilizării sistemului financiar în scopul spălării banilor sau finanțării terorismului[36], prin care informațiile privind beneficiarii efectivi ai entităților corporative și ai altor entități juridice stabilite într-un registru național public al beneficiarilor efectivi (UBO) sunt declarate nule și neavenite[37]; subliniază că, ținând seama de hotărârea CJUE, viitoarea directivă ar trebui să permită cât mai multă accesibilitate publică, astfel încât să devină mai dificil să se ascundă cumpărările sau vânzările de programe spion prin interpuși și societăți de intermediere;

Acțiuni întreprinse în urma rezoluțiilor Parlamentului

101. cere să se dea curs urgent rezoluției Parlamentului din 12 martie 2014 referitoare la programul de supraveghere al Agenției Naționale de Securitate (NSA) a SUA, la organismele de supraveghere din diferite state membre și la impactul acestora asupra drepturilor fundamentale ale cetățenilor UE și asupra cooperării transatlantice în materie de justiție și de afaceri interne; subliniază că recomandări acesteia trebuie să fie puse în aplicare de urgență;

102. subliniază că, în ciuda faptului că supravegherea activităților serviciilor de informații ar trebui să se bazeze deopotrivă pe legitimitate democratică (cadru juridic solid,

[36] Hotărârea din 22 noiembrie 2022, cauzele conexate C-37/20 și C 601/20, EU:C:2022:912.
[37] CJUE. Comunicat de presă nr. 188/22, Hotărârea Curții în cauzele conexate C-37/20 și C-601/20.

autorizare ex ante și verificare ex post) și pe capacitate și expertiză tehnică adecvate, acestea lipsesc în mod dramatic majorității actualelor organisme de supraveghere din UE și SUA, în special în ceea ce privește capacitățile tehnice;

103. invită, așa cum a făcut-o și în cazul Echelon, toate parlamentele naționale care nu au făcut-o încă să instituie un control semnificativ al activităților de informații de către parlamentari sau de către organisme de experți cu atribuții juridice de investigare; invită parlamentele naționale să garanteze că astfel de comisii/organisme de supraveghere dispun de suficiente resurse, expertiză tehnică și mijloace juridice, inclusiv de dreptul de a efectua inspecții la fața locului, pentru a putea să controleze în mod efectiv serviciile de informații;

104. solicită înființarea unui grup la nivel înalt pentru a propune, într-un mod transparent și în colaborare cu parlamentele, recomandări și măsuri suplimentare care trebuie adoptate pentru a consolida supravegherea democratică, inclusiv sistemul de control parlamentar și serviciile de informații și pentru a intensifica colaborarea în domeniul supravegherii în UE, îndeosebi în ceea ce privește dimensiunea sa transfrontalieră;

105. consideră că grupul la nivel înalt ar trebui:

(a) să definească standardele sau orientările minime la nivel european cu privire la supravegherea ex ante sau ex post a serviciilor de informații pe baza bunelor practici existente și a recomandărilor organismelor internaționale, cum ar fi ONU și Consiliul Europei, inclusiv a faptului că organismele de supraveghere sunt considerate terți în temeiul „regulii terțului” sau al principiului controlului emitentului privind controlul și răspunderea pentru informațiile din străinătate;

(b) să elaboreze criterii pentru o mai mare transparență, pornind de la principiul general al accesului la informații și pe baza așa-numitelor „principii Tshwane”[38];

106. intenționează să organizeze o conferință cu organismele naționale de supraveghere, parlamentare sau independente;

107. invită statele membre să utilizeze bunele practici cu scopul de a ameliora accesul organismelor lor de supraveghere la informații referitoare la activitățile de spionaj, inclusiv la informații clasificate și informații din alte servicii și de a conferi competența de efectuare a inspecțiilor pe teren, competențe solide de investigare, resurse adecvate și expertiză specializată, independență absolută față de guvernele respective și obligația de raportare către parlamentele respective;

108. invită statele membre la dezvoltarea cooperării între organismele de supraveghere;

109. solicită Comisiei să prezinte o propunere de procedură europeană privind autorizația de securitate a titularilor de funcții publice din Uniune, întrucât actualul sistem, care se bazează pe autorizația de securitate acordată de statul membru al resortisantului, prevede diferite cerințe și durate ale procedurilor în cadrul sistemelor naționale, ceea ce face să existe un tratament diferit pentru deputații în Parlamentul European și echipa

[38] The Global Principles on National Security and the Right to Information (Principiile globale privind securitatea națională și dreptul la informație), iunie 2013.

acestora în funcție de naționalitate;

110. reamintește că dispozițiile acordului interinstituțional dintre Parlamentul European și Consiliu privind transmiterea și prelucrarea de către Parlamentul European a informațiilor clasificate deținute de Consiliu în alte chestiuni decât cele vizate de domeniul politicii externe și de securitate comune ar trebui utilizate în vederea ameliorării supravegherii la nivelul UE;

Programele de cercetare ale Uniunii

111. solicită punerea în aplicare a unor mecanisme de control mai riguroase și mai eficiente pentru a se garanta că fondurile de cercetare ale Uniunii nu finanțează sau facilitează instrumente, inclusiv instrumente de spionaj sau de supraveghere, care încalcă valorile UE; ia act de faptul că evaluările conformității cu dreptul Uniunii ar trebui să conțină criterii specifice de control pentru a preveni astfel de abuzuri; solicită încetarea acordării de fonduri de cercetare din partea Uniunii entităților care sunt sau au fost implicate în facilitarea directă sau indirectă a încălcărilor drepturilor omului prin intermediul instrumentelor de supraveghere;

112. subliniază că finanțarea UE pentru cercetare, cum ar fi acordurile Orizont Europa cu țări din afara UE nu trebuie să fie folosită pentru a contribui la dezvoltarea de programe spion și tehnologii echivalente;

Laboratorul tehnologic al UE

113. invită Comisia să inițieze fără întârziere crearea unui institut european interdisciplinar de cercetare cu conducere independentă, axat pe cercetare și dezvoltare în relație cu tehnologia informației și comunicațiilor, drepturile fundamentale și securitatea; subliniază că acest institut ar trebui să colaboreze cu experți, cu reprezentanți ai mediului academic și ai societății civile, și să fie deschis participării experților și instituțiilor din statele membre;

114. accentuează că acest institut ar contribui la o mai bună conștientizare, atribuire și responsabilizare în Europa și în afara acesteia, precum și la extinderea bazei de talente europene și a înțelegerii noastre cu privire la modul în care vânzătorii de programe spion dezvoltă, întreține, vând și furnizează serviciile lor către terți;

115. consideră că institutul ar trebui să aibă sarcina de a descoperi și a expune utilizarea ilegală a programelor informatice în scopuri de supraveghere ilicită, de a oferi sprijin juridic și tehnologic accesibil și gratuit, inclusiv screeninguri pentru telefoanele inteligente pentru persoanele care suspectează că au fost vizate de programe spion și instrumentele necesare pentru detectarea programelor spion, efectuarea de cercetări criminalistice analitice pentru anchetele judiciare și raportarea periodică cu privire la utilizarea și la utilizarea abuzivă a programelor spyware în UE, ținând seama de actualizările tehnologice; consideră că acest raport ar trebui să fie pus la dispoziție anual și transmis Comisiei, Parlamentului și Consiliului;

116. recomandă Comisiei să înființeze laboratorul tehnologic al Uniunii în strânsă colaborare cu Centrul de răspuns la incidente de securitate cibernetică pentru instituțiile, organele și agențiile UE (CERT-UE) și ENISA și să se consulte cu experți relevanți atunci când

înființează laboratorul tehnologic al UE, pentru a învăța din bunele practici din domeniul academic;

117. subliniază importanța asigurării unei finanțări adecvate pentru laboratorul tehnologic al UE;

118. recomandă Comisiei să propună un sistem de certificare pentru analiza și autentificarea materialelor criminalistice;

119. invită Comisia să sprijine capacitatea societății civile la nivel mondial pentru a consolida reziliența la atacurile spyware și furnizarea de asistență și servicii pentru cetățeni;

Statul de drept

120. subliniază că impactul utilizării nelegitime a programelor spion este mult mai pronunțat în statele membre în care autoritățile care în mod normal ar avea sarcina de a investiga, de a acorda despăgubiri persoanelor vizate și de a asigura responsabilitatea, sunt controlate de stat și că, în cazul în care există o criză a statului de drept și independența sistemului judiciar este pusă în pericol, autoritățile naționale nu pot fi invocate;

121. invită, prin urmare, Comisia să asigure o implementare eficace a setului său de instrumente privind statul de drept, în special prin:

(a) instituirea unei monitorizări mai cuprinzătoare a statului de drept, inclusiv recomandări specifice fiecărei țări referitoare la utilizarea ilegală de către statele membre a programelor spion în raportul anual al Comisiei privind statul de drept, care să evalueze capacitatea de reacție a instituțiilor statului în a acorda despăgubiri persoanelor vizate și să extindă domeniul de aplicare al raportului său anual privind statul de drept și să includă toate provocările la adresa democrației, a statului de drept și a drepturilor fundamentale, astfel cum sunt incluse la articolul 2 din TUE, astfel cum a solicitat în mod repetat Parlamentul;

(b) lansarea proactivă și gruparea procedurilor de constatare a neîndeplinirii obligațiilor împotriva statelor membre pentru deficiențe legate de statul de drept, cum ar fi amenințările la adresa independenței sistemului judiciar și a funcționării eficace a poliției și a procuraturii, în contextul cooperării polițienești și judiciare în materie penală;

Fondul Uniunii pentru litigii

122. solicită crearea, fără întârzieri nejustificate, a unui fond al Uniunii pentru litigii, care să acopere costurile reale ale litigiilor și să le permită persoanelor vizate de programele spion să solicite despăgubiri adecvate, inclusiv daune-interese pentru utilizarea ilegală a programelor spion împotriva lor, în conformitate cu acțiunea pregătitoare adoptată de Parlament în 2017 de creare a unui „fond al UE de sprijin financiar pentru soluționarea litigiilor legate de încălcarea democrației, a statului de drept și a drepturilor fundamentale”;

Instituții UE

123. își exprimă îngrijorarea cu privire la lipsa de acțiune a Comisiei de până în prezent și o îndeamnă să facă uz pe deplin de toate competențele sale în calitate de gardian al tratatelor și să efectueze o anchetă cuprinzătoare și aprofundată cu privire la abuzul și comerțul cu programe spion în Uniune;

124. îndeamnă Comisia să desfășoare o anchetă completă cu privire la toate acuzațiile și suspiciunile de utilizare a programelor spion împotriva funcționarilor săi și să raporteze Parlamentului și autorităților de aplicare a legii responsabile, dacă este necesar;

125. invită Comisia să înființeze un grup de lucru special, în care să implice comisiile electorale naționale, dedicat protecției alegerilor europene din 2024 în întreaga Uniune; reamintește că nu numai interferențele străine, ci și cele interne reprezintă o amenințare la adresa proceselor electorale europene; subliniază că, în cazul utilizării abuzive a instrumentelor de supraveghere generalizată, cum ar fi Pegasus, alegerile pot fi afectate;

126. constată că Comisia PEGA a primit un răspuns colectiv din partea Consiliului la întrebările Parlamentului European adresate tuturor statelor membre numai în ajunul publicării proiectului de raport, la aproximativ patru luni de la scrisorile Parlamentului; își exprimă consternarea cu privire la lipsa de acțiune a Consiliului European și a Consiliului de Miniștri și solicită organizarea unui summit al Consiliului European pe această temă, având în vedere amploarea amenințării la adresa democrației în Europa;

127. invită Consiliul UE să abordeze evoluțiile legate de utilizarea programelor spion și impactul acestora asupra valorilor consacrate la articolul 2 din TUE în cadrul audierilor organizate în temeiul articolului 7 alineatul (1) din TUE;

128. consideră că Parlamentul ar trebui să aibă competențe depline de anchetă, inclusiv un acces mai bun la informații clasificate și neclasificate, competența de a cita martori, de a solicita în mod oficial martorilor să depună mărturie sub jurământ și de a furniza informațiile solicitate în termene specifice; reiterează poziția Parlamentului din propunerea sa de la 23 mai 2012 de regulament al Parlamentului European privind modalitățile detaliate de exercitare a dreptului de anchetă al Parlamentului European și de abrogare a Deciziei 95/167/CE, Euratom, ECSC a Parlamentului European, Consiliului și Comisiei[39]; invită Consiliul să acționeze fără întârziere cu privire la această propunere de regulament pentru a permite un drept de anchetă adecvat pentru Parlamentul European;

129. recunoaște eforturile Parlamentului de detectare a infecțiilor cu programe spion; consideră, cu toate acestea, că protecția personalului ar trebui consolidată, luând în considerare privilegiile și imunitățile celor care au fost spionați; reamintește că orice atac la adresa drepturilor politice ale deputaților reprezintă un atac la adresa independenței și suveranității instituției, precum și un atac la adresa drepturilor alegătorilor;

130. invită Biroul Parlamentului să adopte un protocol pentru cazurile în care deputații sau personalul Parlamentului au devenit ținta directă sau indirectă a programelor spion și subliniază că toate cazurile trebuie raportate de către Parlament autorităților responsabile de aplicarea legii; evidențiază că Parlamentul ar trebui să ofere asistență

[39] JO C 264 E, 13.9.2013, p. 41.

juridică și tehnică în astfel de cazuri;

131. decide să ia inițiativa de a lansa o conferință interinstituțională în cadrul căreia Parlamentul, Consiliul și Comisia să vizeze reforme în materie de guvernanță care să consolideze capacitatea instituțională a Uniunii de a răspunde în mod adecvat atacurilor asupra democrației și statului de drept din interior și să se asigure că Uniunea dispune de metode supranaționale eficace de asigurare a respectării tratatelor și a legislației secundare în caz de nerespectare de către statele membre;

132. solicită adoptarea rapidă a propunerii Comisiei de regulament al Parlamentului European și al Consiliului de stabilire a unor măsuri pentru un nivel comun ridicat de securitate cibernetică la nivelul instituțiilor, organelor, birourilor și agențiilor Uniunii (COM(2022)/0122), precum și implementarea promptă și respectarea strictă a acesteia ulterior, pentru a reduce riscul de infectare cu programe spion a dispozitivelor și sistemelor utilizate de personalul instituțiilor UE și de politicieni;

133. invită UE să semneze Convenția 108+;

134. invită Ombudsmanul European să inițieze discuții în cadrul Rețelei europene a ombudsmanilor cu privire la impactul utilizării abuzive a supravegherii generalizate asupra proceselor democratice și a drepturilor cetățenilor; solicită rețelei să elaboreze recomandări privind căi de atac eficace și semnificative în întreaga UE;

Activitatea legislativă

135. invită Comisia să prezinte cu promptitudine propuneri legislative pe baza acestei recomandări;

°

° °

136. încredințează Președintei sarcina de a transmite prezenta rezoluție statelor membre, Consiliului, Comisiei și Europol.