Europski parlament
2019-2024

Dokument s plenarne sjednice

B9-0260/2023

22.5.2023

NACRT PREPORUKE EUROPSKOG PARLAMENTA VIJEĆU I KOMISIJI

podnesen u skladu s člankom 208. stavkom 12. Poslovnika

nakon ispitivanja navodnih kršenja i nepravilnosti pri primjeni prava Unije u pogledu uporabe Pegasusa i jednakovrijednog špijunskog softvera za nadzor (2023/2500(RSP))

Sophie in ‘t Veld
u ime Istražnog odbora za ispitivanje uporabe Pegasusa i jednakovrijednog špijunskog softvera za nadzor

B9-0260/2023

Nacrt Preporuke Europskog parlamenta Vijeću i Komisiji nakon ispitivanja navodnih kršenja i nepravilnosti pri primjeni prava Unije u pogledu uporabe Pegasusa i jednakovrijednog špijunskog softvera za nadzor (2023/2500(RSP))

Europski parlament,

– uzimajući u obzir Ugovor o Europskoj uniji (UEU), a posebno njegove članke 2., 4., 6. i 21.,

– uzimajući u obzir članke 16., 223., 225. i 226. Ugovora o funkcioniranju Europske unije (UFEU),

– uzimajući u obzir Povelju Europske unije o temeljnim pravima (Povelja), a posebno njezine članke 7., 8., 11., 17., 21., 41., 42. i 47.,

– uzimajući u obzir Direktivu 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama)[1] („Direktiva o e-privatnosti”),

– uzimajući u obzir Uredbu (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka)[2],

– uzimajući u obzir Direktivu (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP[3],

– uzimajući u obzir Direktivu (EU) 2013/40 Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP[4] („Direktiva o kiberkriminalitetu”),

– uzimajući u obzir Uredbu (EU) 2021/821 Europskog parlamenta i Vijeća od 20. svibnja 2021. o uspostavi režima Unije za kontrolu izvoza, brokeringa, tehničke pomoći, provoza i prijenosa robe s dvojnom namjenom[5] („Uredba o robi s dvojnom namjenom”),

– uzimajući u obzir Odluku Vijeća (ZVSP) 2019/797 od 17. svibnja 2019. o mjerama ograničavanja protiv kibernapada koji predstavljaju prijetnju Uniji ili njezinim

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

državama članicama[6], kako je izmijenjena Odlukom Vijeća (ZVSP) 2021/796 od 17. svibnja 2021.[7],

– uzimajući u obzir Akt o izboru zastupnika u Europski parlament neposrednim općim izborima[8],

– uzimajući u obzir Odluku 95/167/EZ, Euratom, EZUČ Europskog parlamenta, Vijeća i Komisije od 6. ožujka 1995. o detaljnim odredbama o izvršavanju prava Europskog parlamenta na istragu[9],

– uzimajući u obzir Odluku (EU) 2022/480 Europskog parlamenta od 10. ožujka 2022. o osnivanju, nadležnostima, brojčanom sastavu i trajanju mandata Istražnog odbora za istraživanje uporabe Pegasusa i ekvivalentnog špijunskog softvera za nadzor te o određivanju predmeta istrage[10],

– uzimajući u obzir Direktivu (EU) 2018/843 Europskog parlamenta i Vijeća od 30. svibnja 2018. o izmjeni Direktive (EU) 2015/849 o sprečavanju korištenja financijskog sustava u svrhu pranja novca ili financiranja terorizma i o izmjeni direktiva 2009/139/EZ i 2013/36/EU[11] („Direktiva o sprečavanju pranja novca”),

– uzimajući u obzir Prijedlog uredbe Europskog parlamenta i Vijeća od 16. rujna 2022. o uspostavi zajedničkog okvira za medijske usluge na unutarnjem tržištu („Europski akt o slobodi medija”) i izmjeni Direktive 2010/13/EU (COM(2022)0457),

– uzimajući u obzir članak 12. Opće deklaracije o ljudskim pravima,

– uzimajući u obzir presudu Suda Europske unije u predmetu C-37/20[12] o Direktivi o sprečavanju pranja novca kojom se presuđuje da nije valjana odredba kojom se predviđa da su informacije o stvarnim vlasnicima društava osnovanih na području država članica uvijek dostupne cjelokupnoj javnosti,

– uzimajući u obzir članak 17. Međunarodnog pakta o građanskim i političkim pravima,

– uzimajući u obzir Povelju Ujedinjenih Naroda i Vodeća načela Ujedinjenih Naroda o poslovanju i ljudskim pravima[13],

– uzimajući u obzir izjavu visoke povjerenice UN-a za ljudska prava Michelle Bachelet od 19. srpnja 2022. naslovljenu „Use of spyware to surveil journalists and human rights defenders” (Uporaba špijunskog softvera za nadzor novinara i boraca za ljudska prava),

– uzimajući u obzir komentar povjerenice Vijeća Europe za ljudska prava Dunje Mijatović od 27. siječnja 2023. naslovljen „Highly intrusive spyware threatens the

[6] SL L 129 I, 17.5.2019, str. 13.
[7] SL L 174 I, 18.5.2021, str. 1.
[8] SL L 278, 8.10.1976, str. 5.
[9] SL L 113, 19.5.1995, str. 1.
[10] SL L 98, 25.3.2022, str. 72.
[11] SL L 156, 19.6.2018, str. 43–74.
[12] Presuda Suda (Veliko vijeće) od 22. studenoga 2022. u predmetu C-37/20, WM i Sovim SA protiv Luxembourg Business Registers, EU:C:2022:912.
[13] https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

essence of human rights”[14] (Iznimno nametljiv špijunski softver prijetnja je biti ljudskih prava),

– uzimajući u obzir uvodne napomene Europskog nadzornika za zaštitu podataka (EDPS) o modernom špijunskom softveru od 15. veljače 2022.[15],

– uzimajući u obzir Europsku konvenciju za zaštitu ljudskih prava i temeljnih sloboda, a posebno njezine članke 8., 10., 13., 14. i 17., te protokole uz tu konvenciju,

– uzimajući u obzir Europolovu Procjenu prijetnje teškog i organiziranog kriminala naslovljenu „A Corrupting Influence: the Infiltration and Undermining of Europe’s Economy and Society by Organised Crime” (Štetan utjecaj: kako se organizirani kriminal infiltrirao u europsko gospodarstvo i društvo i kako ih ugrožava),

– uzimajući u obzir izvješće Agencije Europske unije za temeljna prava iz 2017. naslovljeno „Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU” (Nadzor koji provode obavještajne službe: mjere zaštite temeljnih prava i pravni lijekovi u EU-u) i ažuriranja predstavljena 28. veljače 2023. Istražnom odboru za ispitivanje uporabe Pegasusa i jednakovrijednog špijunskog softvera za nadzor (PEGA),

– uzimajući u obzir svoju Rezoluciju od 12. ožujka 2014. o programu nadzora Agencije za nacionalnu sigurnost SAD-a (NSA), nadzornim tijelima u različitim državama članicama i njihovu utjecaju na temeljna prava građana EU-a te o transatlantskoj suradnji u pravosuđu i unutarnjim poslovima[16] te posebno preporuke o jačanju informatičke sigurnosti u institucijama, tijelima i agencijama EU-a iznesene u toj rezoluciji,

– uzimajući u obzir mišljenje Europskog nadzornika za zaštitu podataka br. 24/2022 od 11. studenoga 2022. o Europskom aktu o slobodi medija,

– uzimajući u obzir glosar o zlonamjernom i špijunskom softveru koji je sastavila Agencija Europske unije za kibersigurnost (ENISA),

– uzimajući u obzir odluku Europskog ombudsmana o tome kako je Europska komisija procijenila učinak na ljudska prava prije pružanja potpore za razvoj sposobnosti za nadzor afričkim zemljama (predmet 1904/2021/MHZ),

– uzimajući u obzir izjavu koju su 2. veljače 2023. dali gđa Irene Kahn, posebna izvjestiteljica UN-a za slobodu mišljenja i izražavanja, i g. Fernand de Varennes, posebni izvjestitelj UN-a za manjinska pitanja, u kojoj zahtijevaju istragu navodnog nadziranja katalonskih vođa špijunskim programom[17],

– uzimajući u obzir izvješće Europske komisije za demokraciju putem prava

[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] SL C 378, 9.11.2017, str. 104.
[17] https://www.ohchr.org/en/press-releases/2023/02/spain-un-experts-demand-investigation-alleged-spying-programme-targeting

(Venecijanska komisija) o demokratskom nadzoru sigurnosnih službi[18] i njezino mišljenje naslovljeno „Poljska – Mišljenje o Aktu od 15. siječnja 2016. o izmjeni Akta o policiji i određenih drugih akata”[19],

– uzimajući u obzir izvješće Istražnog odbora za ispitivanje uporabe Pegasusa i jednakovrijednog špijunskog softvera za nadzor (A9-0189/2023),

– uzimajući u obzir članak 208. stavak 12. Poslovnika,

A. budući da je zahvaljujući naporima organizacija CitizenLab i Amnesty Tech te brojnih istraživačkih novinara otkriveno da vladina tijela u nekoliko zemalja, i u državama članicama EU-a i u trećim zemljama, upotrebljavaju Pegasus i jednakovrijedni špijunski softver za nadzor novinara, političara, službenika tijela kaznenog progona, diplomata, odvjetnika, poslovnih ljudi, aktera civilnog društva i drugih aktera, u političke, pa čak i u kriminalne svrhe; budući da su takve prakse iznimno zabrinjavajuće te da pokazuju rizik od zlouporabe nadzornih tehnologija za ugrožavanje temeljnih prava, demokracije i izbornih procesa;

B. budući da se pod svakim spomenom pojma „špijunski softver” u izvješću misli na „Pegasus i jednakovrijedni špijunski softver za nadzor” kako je definiran u odluci Parlamenta o osnivanju odbora PEGA;

C. budući da je primijećeno da se državni akteri namjerno koriste špijunskim softverom na zavaravajući način, primjenjujući špijunski softver koji se može lažno predstavljati kao legitiman program, datoteka ili sadržaj („trojanski konj”), poput lažnih poruka javnih institucija; budući da su javna tijela u nekim slučajevima iskoristila telefonske operatere kako bi prenijela zlonamjeran sadržaj na uređaj osobe koja je bila predmet nadzora; budući da se špijunski softver može implementirati tako da se iskoriste ranjivosti nultoga dana bez interakcije između osobe koja je predmet nadzora i zaraženog sadržaja, da može ukloniti sve tragove svoje prisutnosti nakon deinstalacije te da može anonimizirati vezu između daljinskih operatera i poslužitelja;

D. budući da je u začecima mobilne komunikacije prisluškivanje provođeno presretanjem poziva, a poslije i tekstualnih poruka u jednostavnom formatu;

E. budući da je pojava šifriranih mobilnih komunikacijskih aplikacija dovela do pojave industrije špijunskog softvera u okviru koje se iskorištavaju postojeće ranjivosti operativnih sustava pametnih telefona kako bi se instalirao softver kojim se u telefon ubacuje špijunski softver, među ostalim kako bi se uređaj zarazio bez ijednog klika i bez znanja ili bilo kakve radnje korisnika, čime se omogućuje izvlačenje podataka prije šifriranja; budući da sam dizajn takvog špijunskog softvera čija instalacija ne zahtijeva nijedan klik izuzetno otežava djelotvoran i smislen nadzor njegove uporabe;

F. budući da se znanje o ranjivostima u softverskim sustavima razmjenjuje izravno među stranama ili putem posrednika; budući da u toj trgovini sudjeluju nedržavni akteri i zločinačke organizacije;

[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

G. budući da se pribavljanjem i prikupljanjem ranjivosti nultoga dana te trgovanjem njima stubokom ugrožava cjelovitost i sigurnost komunikacija te kibersigurnost građana EU-a;

H. budući da bi nadzor špijunskim softverom trebao ostati iznimka i da bi se za njega uvijek trebalo zahtijevati djelotvorno, obvezujuće i smisleno prethodno sudsko odobrenje nepristranog i neovisnog pravosudnog tijela koje mora osigurati da je ta mjera nužna, razmjerna i strogo ograničena na slučajeve koji utječu na nacionalnu sigurnost ili uključuju terorizam i teška kaznena djela; budući da je u okruženjima u kojima ne postoje djelotvorne provjere i ravnoteže vjerojatno da će doći do zlouporabe tehnika nadzora;

I. budući da svaki nadzor špijunskim softverom mora kontrolirati neovisno ex post nadzorno tijelo koje mora osigurati da se svaki ovlašteni nadzor provodi u skladu s temeljnim pravima i uvjetima koje su utvrdili Sud Europske unije, Europski sud za ljudska prava i Venecijanska komisija; budući da bi to ex post nadzorno tijelo trebalo odmah naložiti prekid nadzora ako se utvrdi da on nije sukladan sa spomenutim pravima i uvjetima;

J. budući da je nadzor špijunskim softverom koji ne ispunjava uvjete utvrđene pravom Unije te sudskom praksom Suda Europske unije i Europskog suda za ljudska prava protivan vrijednostima iz članka 2. UEU-a i temeljnim pravima sadržanim u Povelji, posebno u njezinim člancima 7., 8., 11., 17., 21. i 47., kojima se priznaju posebna prava, slobode i načela kao što su poštovanje privatnog i obiteljskog života, zaštita osobnih podataka, sloboda izražavanja i informiranja, pravo na vlasništvo, pravo na nediskriminaciju, kao i pravo na djelotvoran pravni lijek i pošteno suđenje te pretpostavka nedužnosti;

K. budući da su prava osoba koje su predmet nadzora utvrđena u Povelji i međunarodnim konvencijama, posebno pravo na privatnost i pravo na pošteno suđenje, kao i u pravilima Unije o pravima osumnjičenika i optuženika; budući da su ta prava potvrđena sudskom praksom Suda Europske unije i Europskog suda za ljudska prava;

L. budući da učinak ciljanog nadzora na žene može biti osobito težak, jer tijela vlasti mogu iskoristiti povećan interes javnosti kojem su žene izložene kako bi protiv njih iskoristila privatne i intimne podatke dobivene s pomoću špijunskog softvera za klevetničke kampanje;

M. budući da je iz svjedočanstava osoba koje su predmet nadzora jasno da čak i ako pravni lijek i građanska prava postoje na papiru, oni uglavnom postaju ništavni zbog ometanja koje provode vladina tijela, nepostojanja ili neostvarivanja prava osoba koje su predmet nadzora na informiranje i administrativne prepreke koja nastaje jer pojedinci moraju dokazati da su predmet nadzora; budući da je zbog prirode špijunskog softvera čak i u sustavima u kojima postoje brzi i otvoreni postupci vrlo teško dokazati autorstvo te prirodu i razmjer u kojem je pojedinac predmet nadzora;

N. budući da sudovi nisu prihvatili forenzičke dokaze neovisnih stručnjaka, već samo dokaze utemeljene na istrazi koju provode vladina ili sigurnosna tijela ili tijela kaznenog progona koja navodno stoje iza napada; budući da se time osobe koje su predmet nadzora dovode u paradoksalan položaj jer nemaju izvedivu mogućnost dokazivanja zaraze špijunskim softverom;

O. budući da je poljska vlada oslabila i ukinula institucionalne i pravne zaštitne mjere, uključujući odgovarajuće postupke nadzora i kontrole, čime su osobe koje su predmet nadzora ostale bez ikakvog smislenog pravnog lijeka; budući da se špijunski softver za nadzor Pegasus nezakonito implementira u političke svrhe za špijuniranje novinara, oporbenih političara, odvjetnika, tužitelja i aktera civilnog društva;

P. budući da je mađarska vlada oslabila i ukinula institucionalne i pravne zaštitne mjere, uključujući odgovarajuće postupke nadzora i kontrole, čime su osobe koje su predmet nadzora ostale bez ikakvog smislenog pravnog lijeka; budući da se špijunski softver za nadzor Pegasus nezakonito implementira u političke svrhe za špijuniranje novinara, oporbenih političara, odvjetnika, tužitelja i aktera civilnog društva;

Q. budući da je službeno potvrđeno da je grčka nacionalna obavještajna služba EYP prisluškivala jednog grčkog zastupnika u Europskom parlamentu i jednog grčkog novinara te da ih je podvrgnula nadzoru s pomoću špijunskog softvera Predator; budući da je EYP istovremeno prisluškivao jednog bivšeg američko-grčkog zaposlenika društva Meta i upotrijebio protiv njega špijunski softver Predator, čija je uporaba prema grčkom pravu nezakonita; budući da su mediji izvještavali o tome da je EYP upotrijebio špijunski softver Predator protiv zastupnika vladajuće stranke i oporbenih stranaka u grčkom parlamentu, stranačkih aktivista i novinara ili ih je prisluškivao konvencionalnim metodama ili oboje; budući da grčka vlada poriče da je kupila ili da rabi Predator, ali je vrlo vjerojatno da ga upotrebljavaju osobe koje su vrlo bliske uredu predsjednika vlade ili da se Predator upotrebljava u njihovo ime; budući da je grčka vlada priznala da je društvu Intellexa dala izvozne dozvole za prodaju špijunskog softvera Predator represivnim vladama, među ostalim Madagaskara i Sudana; budući da je vlada na taj skandal odgovorila zakonodavnim izmjenama kojima se dodatno smanjuju prava osoba koje su predmet nadzora na informiranje nakon provedenog nadzora i kojima se dodatno otežava rad neovisnih tijela;

R. budući da su otkrićima utvrđene dvije kategorije osoba koje su predmet nadzora špijunskim softverom u Španjolskoj; budući da prva kategorija obuhvaća predsjednika Vlade, ministra obrane, ministra unutarnjih poslova i druge visoke dužnosnike; budući da se druga kategorija odnosi na skandal koji je organizacija Citizen Lab prozvala „CatalanGate” i kojim je obuhvaćeno 65 osoba koje su bile predmet nadzora, uključujući političare iz regionalne vlade Katalonije, pripadnike pokreta za neovisnost Katalonije, zastupnike u Europskom parlamentu, odvjetnike, pripadnike akademske zajednice i aktere civilnog društva; budući da su španjolske vlasti u svibnju 2022. priznale da je predmet njihova nadzora bilo 18 osoba uz sudsko odobrenje, ali dosad nisu otkrile naloge niti bilo kakve druge informacije, pozivajući se na nacionalnu sigurnost kao obrazloženje za uporabu nadzora špijunskim softverom u Španjolskoj; budući da je predmetom nadzora navodno bilo 47 drugih osoba, ali one nisu dobile nikakve informacije osim onih koje je navela organizacija Citizen Lab;

S. budući da na Cipru nisu potvrđeni navodi o zarazama špijunskim softverom; budući da je Cipar važno europsko izvozno čvorište za industriju nadzora i privlačno mjesto za društva koja prodaju tehnologije nadzora;

T. budući da postoje čvrste naznake da vlade Maroka i Ruande, među ostalima, nadziru istaknute građane Unije špijunskim softverom, uključujući predsjednika Francuske,

predsjednika Vlade, ministra obrane i ministra unutarnjih poslova Španjolske, bivšeg belgijskog predsjednika Vlade, bivšeg predsjednika Komisije, bivšeg talijanskog predsjednika Vlade te Carine Kanimba, kćer Paula Rusesabagine;

U. budući da se sa sigurnošću može pretpostaviti da su sve države članice kupile ili da upotrebljavaju jedan sustav špijunskog softvera ili više njih; budući da će se većina vlada u Europskoj uniji suzdržati od nezakonite uporabe špijunskog softvera, ali je rizik od zlouporabe vrlo vjerojatan u nedostatku čvrstog pravnog okvira, uključujući zaštitne mjere i nadzor, te s obzirom na tehničke izazove u otkrivanju i praćenju zaraza;

V. budući da vlade država članica i parlamenti država članica većinom nisu Europskom parlamentu dostavili smislene informacije o svojim pravnim okvirima kojima se uređuje uporaba špijunskog softvera, osim onih koje su već bile javno poznate, unatoč obvezi da to učine u skladu s člankom 3. stavkom 4. Odluke Europskog parlamenta, Vijeća i Komisije od 6. ožujka 1995. o detaljnim odredbama o izvršavanju prava Europskog parlamenta na istragu; budući da je teško procijeniti provedbu zakonodavstva i zaštitnih mjera Unije, nadzora i pravnih sredstava, što sprečava odgovarajuću zaštitu temeljnih prava građana;

W. budući da u članku 4. stavku 3. UEU-a stoji: „Na temelju načela lojalne suradnje i uz puno uzajamno poštovanje, Unija i države članice međusobno si pomažu pri obavljanju zadaća koje proizlaze iz Ugovorâ.”;

X. budući da je nekoliko ključnih aktera iz industrije špijunskog softvera steklo malteško državljanstvo, čime se olakšava njihovo poslovanje unutar Unije i iz nje;

Y. budući da su brojni razvojni inženjeri i prodavači špijunskog softvera registrirani u jednoj državi članici ili više njih; budući da ti primjeri obuhvaćaju grupaciju NSO s korporativnom prisutnošću u Luksemburgu, na Cipru te u Nizozemskoj i Bugarskoj; matično društvo Intellexe, Thalestris Limited, u Irskoj, Grčkoj, Švicarskoj i na Cipru; DSIRF u Austriji; Amesys i Nexa Technologies u Francuskoj; Tykelab i RCS Lab u Italiji te FinFisher (koji više ne postoji) u Njemačkoj;

Z. budući da Europska unija ne sudjeluje u Wassenaarskom aranžmanu o kontroli izvoza konvencionalnog oružja i robe i tehnologije dvojne namjene; budući da sve države članice osim Cipra sudjeluju u Wassenaarskom aranžmanu, iako je Cipar davno podnio zahtjev da mu se pridruži; budući da Uredba o robi s dvojnom namjenom obvezuje Cipar;

AA. budući da se izraelski režim[20] izvoza u načelu primjenjuje na sve izraelske građane, čak i kad djeluju iz EU-a; budući da Izrael ne sudjeluje u Wassenaarskom aranžmanu, ali ipak tvrdi da primjenjuje njegove standarde;

AB. budući da je izvoz špijunskog softvera iz Unije u treće zemlje uređen Uredbom o robi s dvojnom namjenom, koja je revidirana 2021.; budući da je Komisija u rujnu 2022. objavila prvo izvješće o njezinoj provedbi[21];

[20] Zakon o kontroli izvoza u području obrane 5766-2007, izraelsko Ministarstvo obrane.
[21] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A434%3AFIN&qid=1662029750223.

AC. budući da neki proizvođači špijunskog softvera koji izvoze u treće zemlje registriraju poslovni nastan u Uniji kako bi postigli ugled do istovremeno trguju špijunskim softverom s represivnim režimima; budući da se takav softver izvozi iz Unije represivnim režimima ili nedržavnim akterima, čime se krše izvozna pravila EU-a;

AD. budući da se društva Amesys i Nexa Technologies trenutačno kazneno gone u Francuskoj zbog izvoza tehnologije za nadzor u Libiju, Egipat i Saudijsku Arabiju; budući da su društva iz grupe Intellexa sa sjedištem u Grčkoj svoje proizvode navodno izvozila u Bangladeš, Sudan, Madagaskar i najmanje jednu arapsku državu; budući da softver društva FinFisher rabe deseci zemalja diljem svijeta, uključujući Angolu, Bahrein, Bangladeš, Egipat, Etiopiju, Gabon, Jordan, Kazahstan, Mjanmar, Oman, Katar, Saudijsku Arabiju, Tursku i marokanske obavještajne službe te da su Amnesty International i Forbidden Stories optužili te zemlje za uporabu špijunskog softvera Pegasus protiv novinara, boraca za ljudska prava, civilnog društva i političara; budući da nije poznato jesu li za izvoz špijunskog softvera u sve te zemlje izdane izvozne dozvole;

AE. budući da broj sudionika na sajmovima oružja i konferenciji ISSWorld koji su stavljali na tržište mogućnosti špijunskog softvera pokazuje dominaciju pružatelja špijunskog softvera i srodnih proizvoda i usluga iz trećih zemalja, od kojih znatan broj ima sjedište u Izraelu (npr. grupacija NSO, Wintego, Quadream i Cellebrite), te otkriva istaknute proizvođače u Indiji (ClearTrail), Ujedinjenoj Kraljevini (BAe Systems i Black Cube) i Ujedinjenim Arapskim Emiratima (DarkMatter), dok crna lista Sjedinjenih Američkih Država na kojoj se nalaze proizvođači špijunskog softvera iz Izraela (grupacija NSO i Candiru), Rusije (Positive Technologies) i Singapura (Computer Security Initiative Consultancy PTE LTD.) dodatno ističe raznoliko podrijetlo proizvođača špijunskog softvera; budući da taj sajam posjećuje i velik broj raznih europskih javnih tijela, uključujući lokalne policijske snage;

AF. budući da je člankom 4. stavkom 2. UEU-a predviđeno da nacionalna sigurnost ostaje isključiva odgovornost svake države članice;

AG. budući da je, međutim, Sud Europske unije donio odluku (u predmetu C-623/17) da „iako je na državama članicama da definiraju svoje osnovne interese sigurnosti i donesu prikladne mjere da osiguraju svoju unutarnju i vanjsku sigurnost, sama činjenica da je nacionalna mjera donesena radi zaštite nacionalne sigurnosti ne može dovesti do neprimjenjivosti prava Unije i osloboditi države članice obveze da nužno poštuju to pravo”;

AH. budući da je Sud Europske unije donio odluku (u predmetu C-203/15) da „Članak 15. stavak 1. Direktive 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama), kako je izmijenjena Direktivom 2009/136/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009., u vezi s člancima 7., 8. i 11. i člankom 52. stavkom 1. Povelje Europske unije o temeljnim pravima, treba tumačiti na način da mu se protivi nacionalni propis koji u cilju borbe protiv kriminaliteta određuje opće i neselektivno zadržavanje svih podataka o prometu i lokaciji svih pretplatnika i registriranih korisnika u pogledu svih sredstava elektroničke komunikacije”;

AI. budući da je Sud Europske unije donio odluku (u predmetu C-203/15) da „Članak 15. stavak 1. Direktive 2002/58, kako je izmijenjena Direktivom 2009/136, u vezi s člancima 7., 8. i 11. i člankom 52. stavkom 1. Povelje o temeljnim pravima, treba tumačiti na način da mu se protivi nacionalni propis kojim se uređuje zaštita i sigurnost podataka o prometu i lokaciji i osobito pristup nadležnih nacionalnih tijela zadržanim podacima kad svrha tog pristupa u okviru borbe protiv kriminaliteta nije ograničena na borbu protiv teških kaznenih djela, kad se navedeni pristup ne podvrgava prethodnom nadzoru suda ili neovisnog upravnog tijela i kad nije propisano da se predmetni podaci zadržavaju na području Unije”;

AJ. budući da je iz sudske prakse Europskog suda za ljudska prava jasno da se svaki nadzor mora odvijati u skladu sa zakonom, služiti legitimnom cilju te biti potreban i razmjeran; budući da se, nadalje, pravnim okvirom moraju utvrditi precizne, djelotvorne i opsežne zaštitne mjere za izdavanje naloga za mjere nadzora, koje moraju biti podložne odgovarajućem sudskom preispitivanju i djelotvornom nadzoru, kao i za izvršavanje tih mjera te potencijalne mogućnosti pravne zaštite od njih[22];

AK. budući da se Konvencija Vijeća Europe za zaštitu pojedinaca u vezi s automatskom obradom osobnih podataka (Konvencija br. 108), nedavno modernizirana kao Konvencija br. 108+, primjenjuje na obradu osobnih podataka u svrhu državne (nacionalne) sigurnosti, uključujući obranu; budući da su sve države članice EU-a stranke te Konvencije;

AL. budući da važni aspekti uporabe špijunskog softvera za nadzor u svrhu sprečavanja, istrage, otkrivanja ili progona kaznenih djela i izvršavanja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje, pripadaju području primjene prava EU-a;

AM. budući da se Poveljom utvrđuju uvjeti za ograničenje ostvarivanja temeljnih prava, kojima se zahtijeva da ono mora biti predviđeno zakonom, poštovati bit predmetnih prava i sloboda, biti podložno načelu proporcionalnosti te se postavljati samo ako je potrebno i ako zaista odgovara ciljevima od općeg interesa koje priznaje Unija ili potrebi za zaštitom prava i sloboda drugih osoba; budući da pri uporabi špijunskog softvera razina zadiranja u pravo na privatnost može biti toliko visoka da je pojedincu zapravo uskraćeno pravo na privatnost te se ta uporaba ne može uvijek smatrati proporcionalnom, neovisno o tome može li se mjera smatrati nužnom za postizanje legitimnih ciljeva demokratske države;

AN. budući da se Direktivom o e-privatnosti predviđa da države članice moraju zajamčiti povjerljivost komunikacija; budući da se implementiranjem nadzornih instrumenata ograničava pravo na zaštitu terminalne opreme predviđeno Direktivom o e-privatnosti; budući da se takvim ograničenjima nacionalni zakoni o špijunskom softveru uvrštavaju u područje primjene Direktive o e-privatnosti na način sličan nacionalnim zakonima o zadržavanju podataka; budući da česta implementacija nametljive špijunske tehnologije ne bi bila u skladu s pravnim poretkom Unije;

AO. budući da u skladu s međunarodnim pravom država ima pravo istraživati potencijalna kaznena djela samo u okviru svoje nadležnosti i mora pribjeći pomoći drugih država

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

ako se istraga mora provesti u drugim državama, osim ako postoji osnova za provođenje istraga u drugim nadležnostima temeljem međunarodnog sporazuma ili, u slučaju država članica, prava Unije;

AP. budući da se zaraza uređaja špijunskim softverom i prikupljanje podataka koje slijedi nakon toga odvijaju putem poslužitelja koji pripadaju pružateljima usluga mobilne telefonije; budući da zbog besplatnog roaminga unutar Unije osobe ponekad imaju ugovore za mobilne telefone iz država članica u kojima ne prebivaju te da pravna osnova za prikupljanje podataka u drugoj državi članici uporabom špijunskog softvera trenutačno ne postoji u pravu Unije;

AQ. budući da su David Kaye, bivši posebni izvjestitelj UN-a o promicanju i zaštiti prava na slobodu mišljenja i izražavanja[23], i Irene Khan, aktualna posebna izvjestiteljica UN-a o promicanju i zaštiti prava na slobodu mišljenja i izražavanja[24], pozvali na trenutni moratorij na uporabu, prijenos i prodaju sredstava nadzora dok se ne uspostave stroge mjere za zaštitu ljudskih prava za regulaciju praksi i dok se ne zajamči da se vlade i nedržavni akteri tim sredstvima koriste na legitimne načine;

AR. budući da su u nekim slučajevima društva koja se bave špijunskim softverom, osobito Intellexa, uz samu tehnologiju za presretanje i izvlačenje podataka prodala i cjelokupnu uslugu, što se naziva i „hakiranje kao usluga” ili „aktivni kiberobavještajni rad”, nudeći paket metoda za nadzor i tehnologija za presretanje te osposobljavanja osoblja i tehničke, operativne i metodološke podrške; budući da bi ta usluga mogla omogućiti predmetnom društvu kontrolu nad cijelom operacijom nadzora i agregiranje podataka prikupljenih nadzorom; budući da je relevantnim tijelima gotovo nemoguće nadzirati i kontrolirati tu praksu; budući da je zbog toga otežano poštovanje načela proporcionalnosti, nužnosti, legitimnosti, zakonitosti i primjerenosti; budući da izraelska agencija za izvoz obrambenih proizvoda (DECA) ne dopušta tu uslugu; budući da je Cipar poslužio za zaobilaženje postojećih ograničenja utvrđenih izraelskim pravom kako bi se pružala usluga hakiranja;

AS. budući da su države članice obvezne poštovati Direktivu 2014/24/EU i Direktivu 2009/81/EZ o javnoj nabavi odnosno nabavi u području obrane; budući da one moraju primjereno opravdati odstupanja u skladu s člankom 346. stavkom 1. točkom (b) UFEU-a jer se Direktivom 2009/81/EZ izričito uzimaju u obzir osjetljiva obilježja nabave u području obrane te poštovati Sporazum WTO-a o javnoj nabavi, kako je izmijenjen 30. ožujka 2012.[25], ako su njegove stranke;

AT. budući da je Europski nadzornik za zaštitu podataka istaknuo da države članice moraju poštovati Europsku konvenciju o ljudskim pravima i sudsku praksu Europskog suda za ljudska prava, kojom se ograničavaju aktivnosti nadzora koje se provode u svrhu nacionalne sigurnosti; budući da, nadalje, nadzor koji se upotrebljava u svrhe kaznenog progona mora biti usklađen s pravom EU-a, osobito Poveljom i direktivama EU-a poput

[23] „Surveillance and human rights” (Nadzor i ljudska prava), izvješće posebnog izvjestitelja UN-a o promicanju i zaštiti prava na slobodu mišljenja i izražavanja, A/HRC/41/35, 2019**.**
[24] Ured visoke povjerenice UN-a za ljudska prava, „Spyware scandal: UN experts call for moratorium on sale of ‘life threatening’ surveillance tech” (Skandal špijunskog softvera: UN-ovi stručnjaci pozivaju na moratorij na prodaju tehnologije za nadzor kojom se „ugrožavaju životi”).
[25] https://www.wto.org/english/tratop_e/gproc_e/gpa_1994_e.htm.

Direktive o e-privatnosti i Direktive o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela;

AU. budući da su prema izvješćima velike financijske institucije pokušale potaknuti proizvođače špijunskog softvera na to da se suzdrže od primjene odgovarajućih standarda ljudskih prava i dužne pažnje te da nastave prodavati špijunski softver represivnim režimima;

AV. budući da je Izrael na trećem mjestu među pridruženim zemljama programa Obzor 2020. u pogledu ukupnog sudjelovanja u programu; budući da ukupni proračun sporazuma o programu Obzor Europa s Izraelom za razdoblje 2021. – 2027. iznosi 95,5 milijardi EUR[26]; budući da su u okviru tih europskih programa određena sredstva stavljena na raspolaganje izraelskim vojnim i sigurnosnim društvima[27];

AW. budući da je Uredba (EU) 2021/947[28] (Uredba o uspostavi Instrumenta za susjedstvo, razvoj i međunarodnu suradnju – Globalna Europa) glavni zakonodavni instrument za razvojne politike Unije i da se financijska sredstva Unije mogu pružati u okviru vrsta financiranja predviđenih Financijskom uredbom; budući da se pomoć može obustaviti u slučaju narušavanja demokracije, ljudskih prava ili vladavine prava u trećim zemljama;

1. ističe neosporivu važnost zaštite privatnosti, prava na dostojanstvo, privatni i obiteljski život, slobode izražavanja i informiranja, slobode okupljanja i udruživanja te prava na pravično suđenje, posebno u svijetu koji se sve više digitalizira i u kojem se sve više naših aktivnosti odvija na internetu;

2. zauzima čvrsto stajalište da su kršenja tih temeljnih prava i sloboda ključna u pogledu poštovanja zajedničkih pravnih načela utvrđenih u Ugovorima i ostalim izvorima te napominje da je sama demokracija u opasnosti jer nadziranje političara, civilnog društva i novinara špijunskim softverom ima odvraćajući učinak i ozbiljno utječe na pravo mirnog okupljanja te slobodu izražavanja i sudjelovanje javnosti;

3. oštro osuđuje uporabu špijunskog softvera od strane vlada država članica i članova vladinih tijela ili državnih institucija u svrhu praćenja, ucjenjivanja, zastrašivanja, manipuliranja i diskreditiranja članova oporbe, kritičara i civilnog društva, ukidanja demokratskog nadzora i slobodnog tiska, manipuliranja izborima i potkopavanja vladavine prava podvrgavanjem nadzoru sudaca, tužitelja i odvjetnika u političke svrhe;

4. ističe da ta nezakonita uporaba špijunskog softvera od strane nacionalnih vlada i vlada trećih zemalja izravno i neizravno utječe na institucije Unije i postupak donošenja odluka, čime se ugrožava integritet demokracije Europske unije;

5. s dubokom zabrinutošću konstatira temeljnu neadekvatnost trenutačne upravljačke

[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 Uredba (EU) 2021/947 Europskog parlamenta i Vijeća od 9. lipnja 2021. o uspostavi Instrumenta za susjedstvo, razvoj i međunarodnu suradnju – Globalna Europa, izmjeni i stavljanju izvan snage Odluke br. 466/2014/EU Europskog parlamenta i Vijeća te stavljanju izvan snage Uredbe (EU) 2017/1601 Europskog parlamenta i Vijeća i Uredbe Vijeća (EZ, Euratom) br. 480/2009, SL L 209, 14.6.2021.

strukture Unije da odgovori na napade na demokraciju, temeljna prava i vladavinu prava koji dolaze iz Unije te nedjelovanje brojnih država članica; napominje da se ugrožavanjem demokracije, temeljnih prava i vladavine prava u jednoj državi članici dovodi u opasnost cijela Unija;

6. naglašava da se digitalnim standardima kojima se uređuju tehnološke novine u Uniji moraju poštovati temeljna prava;

7. zauzima čvrsto stajalište da se izvozom špijunskog softvera iz Unije diktaturama i represivnim režimima s lošim stanjem ljudskih prava, u kojima se takvi alati koriste protiv aktivista za ljudska prava, novinara i kritičara vlade, ozbiljno krše temeljna prava utvrđena Poveljom i teško krše izvozna pravila Unije;

8. izražava zabrinutost, nadalje, zbog toga što se države članice nezakonito koriste špijunskim softverom i nezakonito trguju njime, jer se tom kombinacijom Unija pretvara u odredište industrije špijunskog softvera;

9. izražava zabrinutost zbog toga što treće zemlje provode nadzor istaknutih osoba, boraca za ljudska prava i novinara u Uniji s pomoću špijunskog softvera;

10. jednako je zabrinut zbog očitog oklijevanja da se istraži zlouporaba špijunskog softvera i u slučajevima kad je osumnjičenik vladino tijelo neke od država članica Unije i kad je osumnjičenik vladino tijelo treće zemlje; primjećuje vrlo spor napredak i nedostatak transparentnosti u sudskim istragama zlouporabe špijunskog softvera protiv čelnika vlada i ministara država članica EU-a i Komisije, kao i protiv pripadnika civilnog društva, novinara ili političkih protivnika;

11. napominje da se pravnim okvirom nekih država članica ne predviđaju precizne, djelotvorne i opsežne zaštitne mjere za izdavanje naloga za mjere nadzora, kao i za izvršavanje tih mjera te potencijalne mehanizme pravne zaštite od njih; napominje da takve mjere moraju služiti legitimnom cilju te biti nužne i proporcionalne;

12. žali zbog toga što vlade država članica, Vijeće i Komisija nisu u potpunosti surađivali u istrazi i podijelili sve relevantne i smislene informacije kako bi pomogli istražnom odboru u izvršavanju njegovih zadaća utvrđenih njegovim mandatom; uvažava da neke od tih informacija mogu biti podložne strogim zakonskim zahtjevima tajnosti i povjerljivosti; smatra da je zajednički odgovor Vijeća potpuno neprimjeren i u suprotnosti s načelom lojalne suradnje utvrđenom u članku 4. stavku 3. UEU-a;

13. zaključuje da se i države članice i Vijeće i Komisija doimaju potpuno nezainteresiranima da maksimalno povećaju svoje napore kako bi se u potpunosti istražila zlouporaba špijunskog softvera, čime svjesno štite vlade država članica Unije koje krše ljudska prava unutar i izvan Unije;

14. zaključuje da je u Poljskoj došlo do ozbiljnih kršenja i nepravilnosti pri provedbi prava Unije;

15. poziva Poljsku da:

(a) apelira na glavnog državnog odvjetnika da pokrene istrage o zlouporabi špijunskog

softvera;

(b) hitno ponovno uspostavi dostatne institucionalne i pravne zaštitne mjere, uključujući djelotvorne, obvezujuće ex ante i ex post kontrole, kao i neovisne mehanizme nadzora, uključujući sudsko preispitivanje aktivnosti nadzora; naglašava da bi u kontekstu djelotvornih ex ante kontrola zahtjev upućen sudu za operativni nadzor i sudski nalog za takav nadzor trebali sadržavati jasno obrazloženje i naznaku tehničkih sredstava koja će se primjenjivati za nadzor te da bi u kontekstu djelotvornog ex post nadzora trebalo uspostaviti obvezu informiranja osobe koja se podvrgava nadzoru o toj činjenici te o trajanju i opsegu nadzora i načinu obrade podataka dobivenih tijekom operativnog nadzora;

(c) uvede dosljedno zakonodavstvo kojim će se štititi građani bez obzira na to provode li operativni nadzor državno odvjetništvo, tajne službe ili bilo koje drugo državno tijelo;

(d) poštuje odluku Ustavnog suda o Zakonu o policiji iz 1990.;

(e) postupi u skladu s mišljenjem Venecijanske komisije o Zakonu o policiji iz 2016.;

(f) poštuje različite presude Europskog suda za ljudska prava kao što je presuda u predmetu *Roman Zakharov* protiv *Rusije* iz 2015. u kojoj se naglašava nužnost strogih kriterija nadzora, pravilnog sudskog odobrenja i nadzora, trenutnog uništavanja nerelevantnih podataka, sudskog nadzora hitnih postupaka i zahtjeva o obavješćivanju osoba koje su predmet nadzora te presuda u slučaju *Klass i drugi* protiv *Njemačke* iz 1987. u kojoj se iznosi da nadzor mora biti dovoljno važan da bi bilo potrebno takvo zadiranje u privatnost;

(g) poštuje sve odluke Suda Europske unije i Europskog suda za ljudska prava povezane s neovisnošću sudstva i nadređenosti prava Unije;

(h) povuče članak 168.a izmijenjenog Zakona o izmjenama i dopunama Zakona o kaznenom postupku iz 2016.;

(i) ponovno uspostavi potpunu neovisnost pravosuđa i poštuje zakonske ovlasti svih relevantnih nadzornih tijela, kao što su pučki pravobranitelj, predsjednik Ureda za zaštitu osobnih podataka i Vrhovni ured za reviziju kako bi se osiguralo da sva nadzorna tijela dobiju potpunu suradnju i pristup informacijama te kako bi se svim osobama koje su predmet nadzora pružile potpune informacije;

(j) hitno uvede nasumičnu dodjelu predmeta sucima sudova za svaki podneseni zahtjev, čak i vikendom i izvan uobičajenog radnog vremena, kako bi se izbjeglo to da tajne službe biraju „prijateljske sudce”, te da zajamči transparentnost takvog sustava, među ostalim javnom objavom algoritma na temelju kojeg se sudac nasumično dodjeljuje predmetu;

(k) ponovno uspostavi tradicionalni sustav parlamentarnog nadzora u kojem oporbena stranka preuzima predsjedanje parlamentarnim nadzornim odborom za posebne službe;

(l) hitno razjasni situaciju u vezi sa zlouporabom špijunskog softvera u Poljskoj kako ne bi bilo nikakvih sumnji u integritet nadolazećih izbora;

(m) pravilno primijeni i provede Direktivu (EU) 2016/680 (Direktiva o zaštiti podataka pri izvršavanju zakonodavstva) te zajamči da tijelo za zaštitu podataka ima ovlast nadzora nad obradom osobnih podataka koju među ostalim provode tijela kao što je Središnji ured za borbu protiv korupcije i Agencija za unutarnju sigurnost;

(n) provede Direktivu o zviždačima;

(o) suzdrži se od donošenja odredaba protivnih Europskoj konvenciji o ljudskim pravima u novim zakonima o elektroničkim komunikacijama ;

(p) zajamči dostupnost djelotvornih pravnih lijekova građanima Poljske na koje utječe provedba zakona protivnih poljskom Ustavu i Europskoj konvenciji o ljudskim pravima;

(q) pozove Europol da istraži sve slučajeve navodne zlouporabe špijunskog softvera;

(r) zajamči neovisnu ocjenu ustavnosti zakona u Poljskoj;

(s) ponovno uspostavi neovisnost uloge glavnog državnog odvjetnika od ministra pravosuđa kako bi se zajamčilo da se u istragama navodnih kršenja temeljnih prava ne uzimaju u obzir politička razmatranja;

16. poziva Komisiju da ocijeni usklađenost poljskog Zakona o zaštiti osobnih podataka koji se obrađuju u vezi sa sprečavanjem i suzbijanjem zločina iz 2018. s Direktivom EU-a o zaštiti podataka pri izvršavanju zakonodavstva te da prema potrebi pokrene postupak zbog povrede zakonodavstva;

17. zaključuje da je u Mađarskoj došlo do ozbiljnih kršenja i nepravilnosti pri provedbi prava Unije;

18. poziva Mađarsku da:

(a) hitno ponovno uspostavi dostatne institucionalne i pravne zaštitne mjere, uključujući učinkovite i obvezujuće ex ante i ex post kontrole, kao i neovisne mehanizme nadzora; uključujući sudsko preispitivanje aktivnosti nadzora; naglašava da bi u kontekstu djelotvornih ex ante kontrola zahtjev upućen sudu za operativni nadzor i sudski nalog za takav nadzor trebali sadržavati jasno obrazloženje i naznaku tehničkih sredstava koja će se primjenjivati za nadzor te da bi u kontekstu djelotvornog ex post nadzora trebalo uspostaviti obvezu informiranja osobe koja se podvrgava nadzoru o toj činjenici te o trajanju i opsegu nadzora i načinu obrade podataka dobivenih tijekom operativnog nadzora;

(b) poštuje različite presude Europskog suda za ljudska prava kao što je presuda u predmetu *Roman Zakharov* protiv *Rusije* iz 2015. u kojoj se naglašava nužnost strogih kriterija nadzora, pravilnog sudskog odobrenja i nadzora, trenutnog uništavanja nerelevantnih podataka, sudskog nadzora hitnih postupaka i zahtjeva o obavješćivanju osoba koje su predmet nadzora te presuda u slučaju *Klass i drugi* protiv *Njemačke* iz 1987. u kojoj se iznosi da nadzor mora biti dovoljno važan da bi bilo potrebno takvo zadiranje u privatnost, kao i zahtjev obavješćivanja predmeta nadzora;

(c) poštuje sve odluke Suda Europske unije i Europskog suda za ljudska prava povezane s neovisnošću sudstva i nadređenosti prava Unije;

(d) ponovno uspostavi neovisna nadzorna tijela u skladu s presudom Europskog suda za ljudska prava u predmetu Hüttl protiv Mađarske, u kojoj sud navodi da nacionalno tijelo za zaštitu podataka i slobodu informacija (NAIH) ne može provoditi neovisan nadzor nad uporabom špijunskog softvera s obzirom na to da tajne službe imaju pravo uskratiti pristup određenim dokumentima na temelju tajnosti;

(e) ponovno uspostavi potpunu neovisnost pravosuđa i svih relevantnih nadzornih tijela, kao što su pučki pravobranitelj i tijela za zaštitu podataka, kako bi se osiguralo da sva nadzorna tijela dobiju punu suradnju i pristup informacijama te kako bi se svim osobama koje su predmet nadzora pružile potpune informacije;

(f) vrati neovisne zaposlenike na vodeće položaje u nadzornim tijelima kao što su Ustavni sud, Vrhovni sud, Revizorski sud, državno odvjetništvo, Mađarska narodna banka i Nacionalno izborno povjerenstvo;

(g) provede Direktivu o zviždačima;

(h) pozove Europol da istraži sve slučajeve navodne zlouporabe špijunskog softvera;

(i) suzdrži se od donošenja odredaba protivnih Europskoj konvenciji o ljudskim pravima u novim zakonima o elektroničkim komunikacijama;

(j) zajamči dostupnost djelotvornih pravnih lijekova građanima Mađarske na koje utječe provedba zakona protivnih mađarskom Ustavu i Europskoj konvenciji o ljudskim pravima;

19. zaključuje da je u Grčkoj došlo do kršenja i nepravilnosti pri provedbi prava Unije;

20. poziva Grčku da:

(a) hitno ponovno uspostavi i ojača institucionalne i pravne zaštitne mjere, uključujući djelotvorne ex ante i ex post kontrole, kao i neovisne mehanizme nadzora;

(b) hitno stavi izvan snage sve izvozne dozvole koje nisu u potpunosti u skladu s Uredbom o robi s dvojnom namjenom i istraži navode o nezakonitom izvozu, među ostalim u Sudan;

(c) zajamči da nadležna tijela mogu slobodno i neometano istraživati sve navode o uporabi špijunskog softvera;

(d) hitno povuče izmjenu 826/145 Zakona 2472/1997 kojom je ukinuta mogućnost da grčko tijelo za sigurnost i privatnost komunikacija (ADAE) obavješćuje građane o ukidanju povjerljivosti komunikacija; izmijeni Zakon 5002/2022 kako bi se ponovno uspostavilo pravo osoba koje su predmet nadzora na trenutne informacije na zahtjev odmah po dovršetku nadzora te ispravi druge odredbe kojima se slabe zaštitne mjere, nadzor i odgovornost;

(e) ponovno uspostavi potpunu neovisnost pravosuđa i svih relevantnih nadzornih tijela,

kao što su pučki pravobranitelj i tijela za zaštitu podataka, uz puno poštovanje neovisnosti tijela ADAE, kako bi se osiguralo da sva nadzorna tijela dobiju punu suradnju i pristup informacijama te svim osobama koje su predmet nadzora pruži potpune informacije;

(f) omogući tijelu ADAE uspostavu elektronskog arhiva kako bi ono moglo obavljati svoju zadaću;

(g) hitno razjasni situaciju u vezi sa zlouporabom špijunskog softvera u Grčkoj kako ne bi bilo nikakvih sumnji u integritet nadolazećih izbora;

(h) poništi zakonodavnu izmjenu iz 2019. kojom je nacionalna obavještajna služba (EYP) stavljena pod izravnu kontrolu predsjednika Vlade; uvede ustavna jamstva kojima će se omogućiti parlamentarni nadzor njezinih aktivnosti bez izgovora povjerljivosti informacija;

(i) osigura neovisnost vodstva nacionalnog tijela za transparentnost (EAD);

(j) zajamči da sudstvo ima sva potrebna sredstva i potporu za istragu nakon navodne zlouporabe špijunskog softvera i zaplijeni fizičke dokaze o pomagačima, posredničkim društvima i prodavačima špijunskog softvera koji su povezani sa zarazama špijunskim softverom;

(k) pozove Europol da se odmah pridruži istragama;

(l) suzdrži se od političkog upletanja u rad glavnog državnog odvjetnika;

21. zaključuje da je regulatorni okvir u Španjolskoj općenito usklađen sa zahtjevima utvrđenim Ugovorima; ističe, međutim, da su potrebne određene reforme te da primjena u praksi mora biti u potpunosti usklađena s temeljnim pravima i da se mora zajamčiti zaštita sudjelovanja javnosti;

22. stoga poziva Španjolsku da:

(a) provede potpunu, pravednu i djelotvornu istragu kojom će se u potpunosti razjasniti svi navodni slučajevi uporabe špijunskog softvera, uključujući 47 slučajeva u kojima je i dalje nejasno jesu li dotične osobe bile predmetom nadzora španjolske nacionalne obavještajne agencije (CNI) uz sudski nalog ili je neko drugo tijelo primilo sudske naloge da ih zakonito podvrgne nadzoru, kao i uporabu špijunskog softvera protiv predsjednika i članova Vlade, te da zaključke predstavi na najširi mogući način u skladu s primjenjivim zakonima;

(b) pruži osobama koje su bile predmet nadzora odgovarajući pristup sudskom odobrenju koje je Vrhovni sud izdao agenciji CNI za nadzor 18 osoba;

(c) surađuje sa sudovima kako bi se zajamčilo da osobe koje su bile predmet nadzora špijunskim softverom imaju pristup realnom i smislenom pravnom lijeku te da se sudske istrage zaključe bez odgode na nepristran i temeljit način, za što je potrebno dodijeliti odgovarajuće resurse;

(d) započne reformu pravnog okvira kojim se uređuje agencija CNI kao što je najavljeno u svibnju 2022.;

(e) pozove Europol, koji može pomoći tehničkim stručnim znanjima, da se pridruži istragama;

23. zaključuje da postoje dokazi o nepravilnostima u provedbi Uredbe EU-a o robi s dvojnom namjenom na Cipru koji zahtijevaju detaljan nadzor;

24. poziva Cipar da:

(a) temeljito procijeni sve izvozne dozvole izdane za špijunski softver i po potrebi ih stavi izvan snage;

(b) temeljito procijeni otpremu materijala povezanog sa špijunskim softverom na unutarnjem tržištu EU-a između država članica te izradi pregled različitih izraelskih društava ili društava u vlasništvu ili pod upravom izraelskih građana koja su registrirana na Cipru i koja sudjeluju u takvim aktivnostima;

(c) objavi izvješće posebnog istražitelja o predmetu „Spyware Van” kao što je to odbor zatražio tijekom svoje službene misije na Cipru;

(d) uz pomoć Europola u potpunosti istraži sve navode o nezakonitoj uporabi i izvozu špijunskog softvera, posebno za nadzor novinara, odvjetnika, aktera civilnog društva i ciparskih građana;

25. smatra da je stanje u nekim drugim državama članicama također razlog za zabrinutost, posebno s obzirom na prisutnost unosne i rastuće industrije špijunskog softvera koja ima koristi od dobrog ugleda, jedinstvenog tržišta i slobodnog kretanja u Uniji, čime se nekim državama članicama kao što su Cipar i Bugarska omogućuje da postanu izvozno središte špijunskog softvera za represivne režime diljem svijeta;

26. smatra da propust ili odbijanje nekih nacionalnih tijela da osiguraju odgovarajuću zaštitu građana Unije, uključujući regulatorne nedostatke i odgovarajuće pravne instrumente, sa svom potrebnom jasnoćom pokazuje da je djelovanje na razini Unije nužno kako bi se osiguralo pridržavanje slova Ugovora i zakonodavstva Unije da bi se poštovalo pravo građana na život u sigurnom okruženju u kojem se poštuju ljudsko dostojanstvo, privatni život, osobni podaci i imovina, što se zahtijeva Direktivom 2012/29/EU, prema kojoj svaka žrtva zločina ima pravo dobiti potporu i zaštitu u skladu sa svojim individualnim potrebama;

27. zaključuje da je došlo do ozbiljnih nedostataka u primjeni prava EU-a kada su Komisija i Europska služba za vanjsko djelovanje (ESVD) pružale potporu trećim zemljama, uključujući ali ne ograničavajući se na 10 takvih zemalja regije Sahel, kako bi im omogućile da razviju sposobnosti za nadzor[29];

28. zauzima stajalište da se trgovina špijunskim softverom i njegova uporaba moraju strogo regulirati; uvažava, međutim, da zakonodavni postupak može potrajati, dok se

[29] Odluka u predmetu 1904/2021/MHZ, dostupna na https://www.ombudsman.europa.eu/hr/decision/hr/163491.

zlouporaba mora odmah zaustaviti; poziva na donošenje uvjeta za zakonitu uporabu, prodaju, kupnju i prijenos špijunskog softvera; ustraje u tome da države članice moraju ispuniti sve uvjete nabrojane u nastavku do 31. prosinca 2023. kako bi se nastavile koristiti špijunskim softverom:

(a) odgovarajuća tijela kaznenog progona, tužiteljstva i pravosudna tijela moraju u potpunosti istražiti i bez odgode rješavati sve slučajeve navodne zlouporabe špijunskog softvera;

(b) moraju dokazati da je okvir kojim se uređuje uporaba špijunskog softvera u skladu sa standardima koje je utvrdila Venecijanska komisija i relevantnom sudskom praksom Suda Europske unije i Europskog suda za ljudska prava;

(c) moraju se izričito obvezati da će uključiti Europol u istrage o navodnim nezakonitim uporabama špijunskog softvera u skladu sa člancima 4., 5. i 6. Uredbe o Europolu; te

(d) moraju staviti izvan snage sve izvozne dozvole koje nisu u potpunosti usklađene s Uredbom o robi s dvojnom namjenom;

29. smatra da Komisija mora ocijeniti ispunjavanje tih uvjeta do 30. studenoga 2023.; smatra, nadalje, da se zaključci te ocjene moraju objaviti u javnom izvješću;

30. uvažava da je mogućnost suzbijanja teških kaznenih djela i terorizma od kritične važnosti za države članice, ali naglašava da je nužna zaštita ljudskih prava i demokracije; naglašava, nadalje, da se države članice moraju koristiti špijunskim softverom na način koji je proporcionalan i nije proizvoljan te da se nadzor mora odobravati isključivo u ograničenim unaprijed utvrđenim okolnostima; smatra da su djelotvorni ex ante mehanizmi kojima se jamči sudski nadzor ključni za zaštitu osobnih sloboda; ponovno potvrđuje da se individualna prava ne smiju ugroziti dopuštanjem neograničenog pristupa nadzoru; naglašava da je sposobnost sudstva da vrši smislen i djelotvoran ex post nadzor u području zahtjeva za nadzor u svrhe nacionalne sigurnosti također važna jer se tako jamči mogućnost osporavanja nerazmjerne uporabe špijunskog softvera od strane vlada;

31. naglašava da bi uporabu špijunskog softvera u svrhe kaznenog progona trebalo izravno regulirati mjerama temeljenim na poglavlju 4. glave V. UFEU-a o pravosudnoj suradnji u kaznenim stvarima; ističe da bi konfiguraciju špijunskog softvera koji se uvozi u EU i na drugi način stavlja na tržište trebalo regulirati mjerom utemeljenom na članku 114. UFEU-a; napominje da se uporaba špijunskog softvera u svrhe nacionalne sigurnosti može regulirati samo neizravno, na primjer, temeljnim pravima i pravilima o zaštiti podataka;

32. smatra da je zbog transnacionalne dimenzije uporabe špijunskog softvera i njezine dimenzije koja se odnosi na EU potreban koordiniran i transparentan nadzor na razini EU-a kako bi se zajamčila zaštita građana EU-a, ali i valjanost dokaza prikupljenih s pomoću špijunskog softvera u prekograničnim predmetima, te da postoji jasna potreba za zajedničkim standardima EU-a utemeljenim na poglavlju 4. glave V. UFEU-a kojima će se regulirati uporaba špijunskog softvera od strane tijela država članica na temelju standarda koje su utvrdili Sud Europske unije, Europski sud za ljudska prava,

Venecijanska komisija i Agencija za temeljna prava[30]; smatra da bi takvi standardi EU-a trebali obuhvaćati barem sljedeće elemente:

(a) predviđena uporaba špijunskog softvera trebala bi biti odobrena samo u iznimnim i posebnim slučajevima kako bi se zaštitila nacionalna sigurnost i podlijegati djelotvornom, obvezujućem i smislenom ex ante sudskom odobrenju nepristranog i neovisnog pravosudnog tijela ili nekog drugog neovisnog tijela za demokratski nadzor koje ima pristup svim relevantnim informacijama, čime se dokazuje nužnost i proporcionalnost predviđene mjere;

(b) nadzor špijunskim softverom trebao bi trajati samo onoliko dugo koliko je nužno potrebno, u sudskom odobrenju trebalo bi unaprijed definirati točan opseg i trajanje za svaki uređaj kojem se pristupa, a hakiranje se može produljiti samo ako se izda dodatno sudsko odobrenje na drugi određeni rok, s obzirom na prirodu špijunskog softvera i mogućnost retroaktivnog nadzora; tijela država članica trebala bi nadalje podvrgavati nadzoru samo pojedinačne uređaje ili račune krajnjih korisnika i suzdržati se od hakiranja pružatelja internetskih i tehnoloških usluga kako se ne bi utjecalo na korisnike koji nisu predmet nadzora;

(c) odobrenje za uporabu špijunskog softvera može se dodijeliti samo u iznimnim slučajevima za istrage ograničenog i zatvorenog popisa jasno i precizno definiranih teških kaznenih djela koja su istinska prijetnja nacionalnoj sigurnosti, a špijunski softver može se upotrebljavati samo na osobama za koje postoji dovoljno naznaka da su počinile ili planiraju počiniti takva teška kaznena djela;

(d) podaci zaštićeni povjerljivošću ili imunitetima koji se odnose na kategorije osoba (kao što su političari, liječnici itd.) ili posebno zaštićenim odnosima (kao što je povjerljivi odnos između odvjetnika ili klijenta) ili pravilima o utvrđivanju i ograničavanju kaznene odgovornosti u vezi sa slobodom tiska i slobodom izražavanja u drugim medijima ne smiju se pribavljati primjenom špijunskog softvera osim ako postoje dovoljne osnove, utvrđene pod sudskim nadzorom, kojima se potvrđuje uključenost u kriminalne aktivnosti ili pitanja nacionalne sigurnosti, što bi trebalo podlijegati zajedničkom okviru;

(e) moraju se izraditi posebna pravila za nadzor tehnologijom špijunskog softvera s obzirom na to da se njome omogućuje neograničen retroaktivan pristup porukama, datotekama i metapodacima;

(f) države članice trebale bi objaviti barem broj odobrenih i odbijenih zahtjeva za nadzor te vrstu i svrhu istrage i anonimno registrirati svaku istragu u nacionalnom registru s jedinstvenom identifikacijskom oznakom kako bi se ona mogla istražiti u slučaju sumnje na zlouporabu;

(g) nacionalna nadzorna tijela trebala bi izvješćivati države članice, a države članice trebale bi zatim redovito izvješćivati Komisiju o tim informacijama; Komisija bi trebala te

[30] Agencija za temeljna prava, „Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Volume II Summary” (Nadzor koji provode obavještajne agencije: mjere zaštite ljudskih prava i pravni lijekovi u EU-u – sažetak II. sveska), 2017.,https://fra.europa.eu/en/publication/2017/surveillance-intelligence-services-fundamental-rights-safeguards-and-remedies-eu.

informacije iskoristiti u svojem godišnjem izvješću o vladavini prava kako bi omogućila usporedbu uporabe špijunskog softvera u državama članicama;

(h) pravo na obavješćivanje za osobu koja je predmet nadzora: nakon završetka nadzora tijela vlasti trebala bi obavijestiti osobu o činjenici da su je tijela vlasti podvrgnula nadzoru s pomoću špijunskog softvera, uključujući informacije o datumu i trajanju nadzora, nalogu izdanom za operaciju nadzora, prikupljenim podacima, informacijama o tome kako su se ti podaci upotrebljavali i koji su to akteri činili, datumu brisanja podataka te pravu da zatraži administrativne i sudske lijekove pred nadležnim tijelima i praktičnim mehanizmima kako to učiniti; napominje da bi tu obavijest trebalo poslati bez nepotrebne odgode, osim ako neovisno pravosudno tijelo odobri odgodu obavješćivanja, u slučaju da bi se trenutačnim obavješćivanjem ozbiljno ugrozila svrha nadzora;

(i) pravo na obavješćivanje za osobe koje nisu predmet nadzora i čijim se podacima pristupalo: po isteku razdoblja za koje je odobren nadzor, tijela vlasti trebala bi obavijestiti osobe u čije se pravo na privatnost ozbiljno zadiralo uporabom špijunskog softvera, ali koje nisu bile predmet operacije; tijela vlasti trebala bi tu osobu obavijestiti o činjenici da su tijela vlasti pristupila njezinim podacima i pritom navesti informacije o datumu i trajanju nadzora, nalogu izdanom za operaciju nadzora, prikupljenim podacima, informacijama o tome kako su se ti podaci upotrebljavali i koji su to akteri činili te o datumu brisanja podataka; napominje da bi tu obavijest trebalo poslati bez nepotrebne odgode, osim ako neovisno pravosudno tijelo odobri odgodu obavješćivanja, u slučaju da bi se trenutačnim obavješćivanjem ozbiljno ugrozila svrha nadzora;

(j) djelotvoran, obvezujući i neovisan ex post nadzor nad primjenom špijunskog softvera, za koji tijela koja su za njega odgovorna moraju raspolagati svim potrebnim sredstvima i ovlastima kako bi mogla vršiti smislen nadzor, mora se kombinirati s parlamentarnim nadzorom utemeljenim na višestranačkom članstvu s odgovarajućom provjerom i s punim pristupom dostatnim informacijama kako bi se utvrdilo da je nadzor provođen zakonito i proporcionalno i parlamentarni nadzor osjetljivih povjerljivih podataka trebalo bi olakšati potrebnom infrastrukturom, postupcima i sigurnosnim provjerama; bez obzira na definiciju ili razgraničene pojma nacionalne sigurnosti, nacionalna nadzorna tijela moraju biti nadležna za puni opseg nacionalne sigurnosti;

(k) temeljna načela zakonitog postupanja i sudskog nadzora moraju biti u središtu sustava koji okružuje špijunski softver za nadzor;

(l) smislen pravni lijek za osobe koje su izravno ili neizravno predmet nadzora te obvezan pristup pravnoj zaštiti u okviru neovisnog tijela za pojedince koji tvrde da na njih nadzor negativno utječe; stoga poziva na uvođenje obveze obavješćivanja za državna tijela, uključujući odgovarajuće rokove za obavješćivanje, pri čemu se dostava odvija po isteku sigurnosne prijetnje;

(m) pravni lijekovi moraju biti djelotvorni u pravu i činjeničnom stanju te moraju biti poznati i dostupni; naglašava da takvi pravni lijekovi zahtijevaju brzu, temeljitu i nepristranu istragu neovisnog nadzornog tijela te da bi to tijelo trebalo imati pristup, kao i stručno znanje i tehničke sposobnosti, za obradu svih relevantnih podataka kako bi moglo utvrditi je li sigurnosna procjena pojedinca koju su provela tijela vlasti pouzdana

i proporcionalna; u slučajevima u kojima su zlouporabe potvrđene trebale bi se primjenjivati odgovarajuće sankcije kaznene ili upravne prirode u skladu s relevantnim nacionalnim pravom u državama članicama;

(n) poboljšanje besplatnog pristupa tehnološkom stručnom znanju u ovoj fazi za osobe koje su predmet nadzora, budući da bi se povećanom dostupnošću i cjenovnom pristupačnošću tehnoloških postupaka kao što je forenzička analiza omogućilo osobama koje su predmet nadzora da bolje iznesu svoj predmet pred sudom te bi se poboljšalo zastupanje osoba koje su predmet nadzora na sudu izgradnjom tehnoloških kapaciteta pravnih zastupnika i sudstva kako bi mogli pružati bolje savjete osobama koje su predmet nadzora, utvrđivati kršenja te poboljšati nadzor nad zlouporabama špijunskog softvera i odgovornost za njih;

(o) jačanje prava na obranu i prava na pravično suđenje tako što će se zajamčiti da je optuženicima za kaznena djela dopušteno i moguće provjeriti točnost, vjerodostojnost, pouzdanost i čak zakonitost dokaza koji se upotrebljavaju protiv njih te na taj način odbaciti svaku opću primjenu pravila o tajnosti povezanih s nacionalnom obranom;

(p) tijekom nadzora tijela vlasti trebala bi izbrisati sve podatke koji su nebitni za odobrenu istragu, a nakon završetka nadzora i istrage za koju je izdano odobrenje trebala bi izbrisati podatke i sve povezane dokumente, kao što su bilješke koje su nastale tijekom tog razdoblja, a takvo brisanje mora se evidentirati i biti podložno reviziji;

(q) mogućnost pristupa relevantnim informacijama dobivenim s pomoću špijunskog softvera trebala bi imati samo ovlaštena tijela i to isključivo u svrhu operacije; taj bi pristup trebao biti ograničen na određeno razdoblje kako je navedeno u sudskom postupku;

(r) potrebno je uspostaviti minimalne standarde za prava pojedinaca u kaznenim postupcima o prihvatljivosti dokaza prikupljenih s pomoću špijunskog softvera; u pravo o kaznenom postupku potrebno je uključiti mogućnost lažnih ili manipuliranih informacija dobivenih implementacijom špijunskog softvera (lažno predstavljanje);

(s) države članice moraju se međusobno obavješćivati u slučaju nadzora građana ili rezidenata druge države članice ili mobilnog broja pružatelja usluga u drugoj državi članici;

(t) u špijunski softver za nadzor potrebno je uključiti oznaku kako bi nadzorna tijela mogla nedvojbeno identificirati subjekt koji implementira špijunski softver u slučaju da postoji sumnja na zlouporabu; obvezni potpis za svaku implementaciju špijunskog softvera trebao bi se sastojati od individualne oznake tijela koje postupa, vrste špijunskog softvera koji se upotrebljava i anonimiziranog broja predmeta;

33. poziva države članice da održe javna savjetovanja s dionicima, zajamče transparentnost zakonodavnog postupka i uključe standarde i zaštitne mjere EU-a pri izradi novog zakonodavstva o primjeni i prodaji špijunskog softvera;

34. ističe da se samo špijunski softver koji je dizajniran tako da omogućuje i olakšava funkcionalnost špijunskog softvera u skladu sa zakonodavnim okvirom kako je utvrđeno u stavku 29. može staviti na unutarnje tržište, razviti ili upotrebljavati u Uniji;

potvrđuje da bi se takvom uredbom o stavljanju špijunskog softvera na tržište kojom se predviđa dizajn usklađen s vladavinom prava na temelju članka 114. UFEU-a trebala pružiti visoka razina zaštite građanima Unije; smatra da nema opravdanja za to da se Uredbom o robi s dvojnom namjenom od 2021. štiti građane trećih zemalja od izvoza špijunskog softvera iz EU-a, ali se ne pruža jednakovrijedna zaštita građanima EU-a;

35. smatra da društva u EU-u mogu prodavati i da države članice mogu kupovati samo tehnologiju za presretanje i izvlačenje podataka, a ne „hakiranje kao uslugu”, koje uključuje pružanje tehničke, operativne i metodološke podrške tehnologije za nadzor i omogućuje pružatelju usluge pristup nerazmjernoj količini podataka koja nije u skladu s načelima proporcionalnosti, nužnosti, legitimnosti, zakonitosti i primjerenosti; poziva Komisiju da iznese zakonodavni prijedlog u tom pogledu;

36. naglašava da se špijunski softver može staviti na tržište samo za prodaju javnim tijelima i uporabu od strane javnih tijela, na temelju zatvorenog popisa, čiji nalozi uključuju istrage kaznenih djela ili zaštitu nacionalne sigurnosti za koje se može odobriti uporaba špijunskog softvera; smatra da bi se sigurnosne agencije trebale koristiti špijunskim softverom samo kad su provedene sve preporuke koje je iznijela Agencija za temeljna prava[31];

37. ističe obvezu uporabe verzije špijunskog softvera koja je dizajnirana tako da se pristup svim podacima pohranjenim na uređaju svede na najmanju moguću mjeru, ali bi trebala biti dizajnirana tako da pristup podacima ograniči na minimum koji je izričito nužan za svrhu odobrene istrage;

38. zaključuje da kupnja špijunskog softvera od strane države članice mora nakon toga biti podložna reviziji neovisnog, nepristranog revizorskog tijela koje je prošlo odgovarajuću provjeru;

39. naglašava da bi svi subjekti koji stavljaju špijunski softver na unutarnje tržište trebali poštovati stroge zahtjeve dužne pažnje, a društva koja se javljaju da budu dobavljači u postupku javne nabave trebala bi proći postupak kontrole koji uključuje odgovor društva na kršenja ljudskih prava počinjena njegovim špijunskim softverom te odgovor na pitanje oslanja li se njegova tehnologija na podatke prikupljene u okviru nedemokratskih praksi nadzora pri kojima je počinjena zlouporaba; naglašava da bi nadležna nacionalna nadzorna tijela trebala jednom godišnje podnositi izvješće o sukladnosti Komisiji;

40. naglašava da bi društva koja nude tehnologije ili usluge nadzora državnim akterima trebala nadležnim nacionalnim nadzornim tijelima otkriti prirodu izvoznih dozvola;

41. naglašava da bi države članice trebale utvrditi razdoblje mirovanja tijekom kojeg se bivši zaposlenici vladinih tijela ili agencija neće moći zaposliti u društvima koja se bave špijunskim softverom;

Potreba za granicama nacionalne sigurnosti

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

42. zabrinut je zbog slučajeva neopravdanog pozivanja na „nacionalnu sigurnost” kako bi se opravdala implementacija i uporaba špijunskog softvera te kako bi se zajamčila potpuna tajnost i nedostatak odgovornosti; pozdravlja izjavu Komisije, u skladu sa sudskom praksom Suda Europske unije[32], da se samo upućivanje na nacionalnu sigurnost ne može tumačiti kao neograničeno izuzeće od primjene prava EU-a i da bi se za njega trebalo zahtijevati jasno obrazloženje te poziva Komisiju da poduzme daljnje mjere na temelju te izjave u slučajevima kad postoje naznake zlouporabe; smatra da će u demokratskom transparentnom društvu u kojem se poštuje vladavina prava takva ograničenja u ime nacionalne sigurnosti biti iznimka, a ne pravilo;

43. smatra da se pojmu nacionalne sigurnosti mora suprotstaviti ograničeniji opseg u odnosu na unutarnju sigurnost, pri čemu potonja ima širi opseg, uključujući sprečavanje rizika za građane i posebno provedbu kaznenog prava;

44. žali zbog poteškoća koje proizlaze iz nedostatka zajedničke pravne definicije nacionalne sigurnosti kojom bi se utvrdili kriteriji za određivanje pravnog režima koji se može primjenjivati u pitanjima nacionalne sigurnosti, kao i jasno razgraničenje područja u kojem se takav poseban režim može primjenjivati;

45. smatra da uporaba špijunskog softvera predstavlja ograničenje temeljnih prava; smatra, nadalje, da pojam koji se upotrebljava u pravnom kontekstu te uključuje prijenos prava i propisivanje obveza (a posebno ograničavanje temeljnih prava pojedinaca) mora biti jasan i predvidljiv svim osobama na koje taj pojam utječe; podsjeća da se Poveljom o temeljnim pravima predviđa da svako ograničenje temeljnih prava u skladu s člankom 52. stavkom 1. mora biti utvrđeno zakonom; stoga smatra da je potrebno jasno definirati „nacionalnu sigurnost”; naglašava da područje nacionalne sigurnosti, bez obzira na jasno razgraničenje, mora biti u cijelosti podložno neovisnom, obvezujućem i djelotvornom nadzoru;

46. naglašava da bi tijela vlasti, u slučaju da se pozivaju na razloge nacionalne sigurnosti kao obrazloženje za uporabu špijunskog softvera, uz okvir utvrđen u stavku 29. trebala dokazati sukladnost s pravom EU-a, uključujući poštovanje načela proporcionalnosti, nužnosti, legitimnosti, zakonitosti i primjerenosti; naglašava da bi to obrazloženje trebalo biti lako pristupačno i da bi se trebalo staviti na raspolaganje nacionalnom nadzornom tijelu radi ocjenjivanja;

47. ponavlja u tom kontekstu da su sve države članice potpisale Konvenciju br. 108+ kojom se utvrđuju standardi i obveze za zaštitu pojedinaca u vezi s obradom osobnim podataka, među ostalim u svrhe nacionalne sigurnosti; ističe da je Konvencija br. 108+ obvezujući europski okvir kojim se uređuje obrada podataka koju provode obavještajne i sigurnosne službe; potiče sve države članice da bez odgode ratificiraju tu konvenciju, da već provedu njezine standarde u nacionalno pravo i da postupaju u skladu s njima u području nacionalne sigurnosti;

[32] Presuda od 6. listopada 2020., predmet C-623/17, Privacy International protiv Secretary of State for Foreign and Commonwealth Affairs i drugih, EU:C:2020:790, stavak 44., i presude od 6. listopada 2020., spojeni predmeti C-511/18, C-512/18 i C-520/18, La Quadrature du Net i ostali protiv Premier ministre i ostalih, EU:C:2020:791, stavak 99.: „sama činjenica da je nacionalna mjera donesena radi zaštite nacionalne sigurnosti ne može dovesti do neprimjenjivosti prava Unije i osloboditi države članice obveze da nužno poštuju to pravo”..

48. naglašava da su izuzeća i ograničenja ograničenog broja odredaba te konvencije dopuštena samo ako su u skladu sa zahtjevima iz članka 11. te konvencije, što znači da pri primjeni Konvencije br. 108+ svako pojedino izuzeće i ograničenje mora biti predviđeno zakonom, da se njime mora poštovati bit temeljnih prava i sloboda te da se mora obrazložiti da ono „predstavlja nužnu i proporcionalnu mjeru u demokratskom društvu” za jedan od legitimnih razloga iz članka 11.[33] i da takva izuzeća i ograničenja ne smiju utjecati na „neovisno i djelotvorno preispitivanje i nadzor na temelju nacionalnog zakonodavstva dotične stranke”;

49. nadalje napominje da se u Konvenciji br. 108+ naglašava da nadzor „mora imati ovlasti za istragu i intervenciju”; smatra da djelotvorno preispitivanje i nadzor podrazumijevaju obvezujuće ovlasti u slučajevima najvećeg utjecaja na temeljna prava, posebno u fazama obrade osobnih podataka koje se odnose na pristup podacima te analizu i pohranjivanje podataka;

50. smatra da nedostatak obvezujućih ovlasti nadzornih tijela u području nacionalne sigurnosti nije u skladu s kriterijem utvrđenim u Konvenciji br. 108+ da to „predstavlja nužnu i proporcionalnu mjeru u demokratskom društvu”;

51. ističe da je Konvencijom br. 108+ dopušten vrlo ograničen broj iznimaka u vezi s njezinim člankom 15., ali da se takve iznimke ne dopuštaju, posebno u vezi sa stavkom 2. [obveze upozoravanja], stavkom 3. [savjetovanje o zakonodavnim i upravnim mjerama], stavkom 4. [zahtjevi i pritužbe koje podnose pojedinci], stavkom 5. [neovisnost i nepristranost], stavkom 6. [potrebni resursi za djelotvorno obavljanje zadaća], stavkom 7. [periodičko izvješćivanje], stavkom 8. [povjerljivost], stavkom 9. [mogućnost žalbe] i stavkom 10. [nema ovlasti u vezi s tijelima kad ona obavljaju svoju sudbenu funkciju];

Bolja primjena i provedba postojećeg zakonodavstva

52. ističe nedostatke u nacionalnim pravnim okvirima i potrebu za boljom primjenom postojećeg zakonodavstva Unije kako bi se ti nedostaci uklonili; ustvrđuje da su sljedeći zakoni Unije relevantni, ali se prečesto nepravilno primjenjuju i/ili provode: Direktiva o sprečavanju pranja novca, Direktiva o zaštiti podataka pri izvršavanju zakonodavstva, pravila o nabavi, Uredba o robi s dvojnom namjenom, sudska praksa (odluke o nadzoru i nacionalnoj sigurnosti) i Direktiva o zviždačima; poziva Komisiju da istraži i izvijesti o nedostacima u primjeni i provedbi te da predstavi plan djelovanja za njihovo ispravljanje najkasnije do 1. kolovoza 2023.;

53. smatra ključnom pravilnu primjenu i strogu provedbu pravnog okvira Unije o zaštiti podataka, posebno Direktive o zaštiti podataka pri izvršavanju zakonodavstva, Opće uredbe o zaštiti podataka i Direktive o privatnosti i elektroničkim komunikacijama; smatra jednako važnom punu provedbu relevantnih presuda Suda Europske unije koja u

[33] Ta ocjena utvrđena je u sudskoj praksi Europskog suda za ljudska prava kojom se teret dokazivanja stavlja na državu/zakonodavca. Relevantna sudska praksa Europskog suda za ljudska prava uključuje: Roman Zakharov protiv Rusije (predstavka br. 47143/06), 4. prosinca 2015.; Szabó and Vissy protiv Mađarske (predstavka br. 37138/14), 12. siječnja 2016.; Big Brother Watch i drugi protiv Ujedinjene Kraljevine (br. zahtjeva 58170/13, 62322/14 i 24969/15), 25. svibnja 2021. te Centrum för rättvisa protiv Švedske (predstavka br. 35252/08), 25. svibnja 2021.

nekim državama članicama i dalje izostaje; podsjeća na to da Komisija ima središnju ulogu u provedbi prava EU-a i osiguravanju njegove ujednačene primjene na cijelom području Unije te bi trebala iskoristiti sve raspoložive instrumente, uključujući postupke zbog povrede prava u slučajevima dugotrajne nesukladnosti;

54. poziva na to da Wassenaarski aranžman postane obvezujući sporazum za sve njegove sudionike kako bi postao međunarodni sporazum;

55. poziva Cipar i Izrael da postanu zemlje sudionice Wassenaarskog aranžmana; podsjeća države članice da je potrebno uložiti sve napore kako bi se Cipru i Izraelu omogućilo da se pridruže Wassenaarskom aranžmanu;

56. naglašava da bi Wassenaarski aranžman trebao uključivati okvir ljudskih prava kojim se ugrađuje licenciranje tehnologija špijunskog softvera te ocjenjuje i preispituje usklađenost društava koja proizvode tehnologije špijunskog softvera i da bi sudionici trebali zabraniti kupnju nadzornih tehnologija iz država koje nisu sudionice tog aranžmana;

57. naglašava da bi u svjetlu saznanja o špijunskom softveru Komisija i države članice trebali provesti temeljitu istragu izvoznih dozvola odobrenih za uporabu špijunskog softvera u skladu s Uredbom o robi s dvojnom namjenom i da bi Komisija trebala obavijestiti Parlament o rezultatima te ocjene;

58. naglašava potrebu za sljedivošću i odgovornošću u vezi s izvozom špijunskog softvera te podsjeća da bi društva iz EU-a trebala moći izvoziti samo špijunski softver za koji su dokazana dostatna svojstva sljedivosti kako bi se uvijek mogla utvrditi odgovornost;

59. ističe da Komisija treba redovito provjeravati i pravilno provoditi preinačenu Uredbu o robi s dvojnom namjenom kako bi se izbjeglo „biranje izvoznog režima” diljem Unije, kao što je trenutačno slučaj u Bugarskoj i Cipru, te da bi Komisija trebala imati odgovarajuća sredstva za tu zadaću;

60. poziva Komisiju da osigura dostatne kadrovske kapacitete odjelima odgovornima za nadzor i provedbu Uredbe o robi s dvojnom namjenom;

61. poziva na izmjene Uredbe o robi s dvojnom namjenom kako bi se u članku 15. pojasnilo da se izvozne dozvole za robu s dvojnom namjenom ne smiju davati ako roba jest ili bi mogla biti namijenjena uporabi u vezi s unutarnjom represijom i/ili teškim kršenjima ljudskih prava i međunarodnog humanitarnog prava; poziva na punu primjenu ljudskih prava i provjera dužne pažnje u postupku izdavanja dozvola te na daljnja poboljšanja kao što je pravni lijek za osobe koje su predmet kršenja ljudskih prava, kao i na transparentno izvješćivanje o provedenoj dužnoj pažnji;

62. poziva na izmjene Uredbe o robi s dvojnom namjenom kako bi se zajamčila zabrana provoza u slučajevima kada je roba namijenjena ili bi mogla biti namijenjena unutarnjoj represiji i/ili teškom kršenju ljudskih prava i međunarodnog humanitarnog prava;

63. naglašava da bi pri budućoj izmjeni Uredbe o robi s dvojnom namjenom imenovana nacionalna tijela odgovorna za odobravanje i odbijanje izvoznih dozvola za robu s dvojnom namjenom trebala dostaviti detaljna izvješća, uključujući informacije o

predmetnoj robi s dvojnom namjenom; broj zatraženih dozvola; naziv zemlje izvoznice; opis izvoznog društva i informaciju o tome je li to ono društvo kći; opis krajnjeg korisnika i odredišta; vrijednost izvozne dozvole; razlog odobrenja ili odbijanja izvozne dozvole; ističe da bi se ta izvješća trebala objavljivati jednom u tromjesečju; poziva na osnivanje posebnog stalnog parlamentarnog odbora s pristupom povjerljivim informacijama Komisije u svrhu parlamentarnog nadzora;

64. naglašava da se pri budućoj izmjeni Uredbe o robi s dvojnom namjenom mora ukinuti izuzeće iz obveze pružanja informacija Komisiji zbog komercijalne osjetljivosti, obrane, vanjske politike ili nacionalne sigurnosti; smatra da, umjesto toga, kako bi se spriječilo da osjetljive informacije postanu dostupne trećim zemljama, Komisija može odlučiti klasificirati određene informacije u svojem godišnjem izvješću;

65. naglašava da se definicija robe za kibernadzor iz preinačene Uredbe o robi s dvojnom namjenom ne može tumačiti restriktivno, već bi trebala uključivati sve tehnologije u tom području, kao što su oprema za presretanje ili ometanje mobilnih telekomunikacija; softver za neovlašten ulazak; sustavi ili oprema za nadzor mreža internetskog protokola; softver posebno izrađen ili izmijenjen za praćenje ili analizu od strane tijela kaznenog progona; laserska oprema za otkrivanje zvuka; forenzički alati koji izdvajaju neobrađene podatke iz računalnog ili komunikacijskog uređaja i zaobilaze „autentifikaciju” ili kontrole autorizacije uređaja; elektronički sustavi ili oprema namijenjeni za nadzor i praćenje elektromagnetskog spektra za vojno-obavještajne ili sigurnosne svrhe; i bespilotne letjelice koje mogu provoditi nadzor;

66. poziva na dodatno europsko zakonodavstvo kojim se od korporativnih aktera koji proizvode i/ili izvoze tehnologije za nadzor zahtijeva da uključe okvire za ljudska prava i dužnu pažnju u skladu s Vodećim načelima UN-a o poslovanju i ljudskim pravima;

Međunarodna suradnja za zaštitu građana

67. poziva na zajedničku strategiju EU-a i SAD-a za špijunski softver, uključujući zajedničku bijelu listu i/ili crnu listu dobavljača špijunskog softvera čiji su alati zlorabljeni ili postoji rizik da bi mogli biti zlorabljeni za zlonamjerni nadzor vladinih dužnosnika, novinara i civilnog društva, te čije je poslovanje u suprotnosti sa sigurnosnom i vanjskom politikom Unije, od strane vlada trećih zemalja poznatih po kršenju ljudskih prava, koji (ni)su ovlašteni prodavati javnim tijelima, zajedničke kriterije za dobavljače koji bi trebali biti uvršteni na bilo koju od tih lista, dogovor o zajedničkom izvješćivanju EU-a i SAD-a o toj industriji, zajednički nadzor, zajedničke obveze dužne pažnje za dobavljače i kriminalizaciju prodaje špijunskog softvera nedržavnim akterima;

68. traži da Vijeće za trgovinu i tehnologiju EU-a i SAD-a održi opsežno i otvoreno savjetovanje s civilnim društvom radi razvoja zajedničke strategije i zajedničkih standarda EU-a i SAD-a, uključujući zajedničku bijelu listu i/ili crnu listu;

69. traži pokretanje pregovora s drugim zemljama, posebno s Izraelom, kako bi se uspostavio okvir za stavljanje špijunskog softvera na tržište i izvozne dozvole, uključujući pravila o transparentnosti, popis zemalja koje ispunjavaju uvjete u vezi sa standardima ljudskih prava i postupke dužne pažnje;

70. napominje da, za razliku od SAD-a, gdje je NSO brzo uvršten na crnu listu i predsjednik SAD-a je potpisao izvršni nalog u kojem se navodi da se NSO ne smije operativno koristiti komercijalnim špijunskim softverom koji predstavlja znatne protuobavještajne ili sigurnosne rizike za Vladu Sjedinjenih Država ili znatne rizike od nepravilne uporabe od strane neke inozemne vlade ili inozemnog državljanina, na razini EU-a nisu poduzete dovoljne mjere u vezi s uvozom špijunskog softvera i provedbom izvoznih pravila;

71. zaključuje da se izvozna pravila Unije i njihova provedba moraju ojačati radi zaštite ljudskih prava u trećim zemljama te da se moraju osigurati potrebni alati za djelotvornu provedbu predmetnih odredaba; podsjeća na to da bi EU trebao nastojati udružiti snage s SAD-om i drugim saveznicima na regulaciji trgovine špijunskim softverom te iskoristiti njihovu združenu tržišnu snagu kako bi se nametnule promjene i postavili snažni standardi u pogledu transparentnosti, sljedivosti i odgovornosti za uporabu tehnologije za nadzor, što bi trebalo kulminirati inicijativom na razini Ujedinjenih naroda;

Ranjivosti nultoga dana

72. traži da se reguliraju otkrivanje, razmjena, ispravljanje i iskorištavanje ranjivosti, kao i postupci objavljivanja, te da se na taj način dovrši osnova utvrđena Direktivom (EU) 2022/2555[34] (Direktiva NIS2) i prijedlogom Akta o kiberotpornosti[35];

73. smatra da istraživači moraju imati mogućnost istraživanja ranjivosti i razmjene svojih rezultata bez građanskopravne i kaznene odgovornosti u skladu s, među ostalim, Direktivom o kiberkriminalu i Direktivom o autorskim pravima;

74. poziva glavne aktere u tom sektoru industrije da stvore poticaje za istraživače da sudjeluju u istraživanju ranjivosti ulaganjem u planove za ispravljanje ranjivosti, prakse otkrivanja unutar industrije i s civilnim društvom te da provode programe nagrađivanja pronalaska ranjivosti;

75. poziva Komisiju da poveća svoju potporu programima nagrađivanja pronalaska ranjivosti i financiranje tih programa, kao i potporu i financiranje za druge projekte usmjerene na traženje i ispravljanje sigurnosnih ranjivosti, te da uspostavi koordinirani pristup obveznom otkrivanju ranjivosti među državama članicama;

76. poziva na zabranu prodaje ranjivosti u nekom sustavu u bilo koju drugu svrhu osim u svrhu jačanja sigurnosti tog sustava, kao i na obvezu otkrivanja rezultata svih istraživanja ranjivosti na koordiniran i odgovoran način kojim se promiče javna sigurnost i kojim se smanjuje rizik iskorištavanja ranjivosti;

77. poziva javne i privatne subjekte da uspostave javno dostupnu kontaktnu točku za prijavu ranjivosti na koordiniran i odgovoran način i poziva organizacije koje prime informacije o ranjivostima u svojem sustavu da odmah djeluju kako bi se one ispravile; smatra da bi u slučajevima kad je dostupna „zakrpa” za ispravljanje ranjivosti

[34] Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148, SL L 333, 27.12.2022., str. 80.
[35] Prijedlog uredbe Europskog parlamenta i Vijeća od 15. rujna 2022. o horizontalnim zahtjevima za kibersigurnost za proizvode s digitalnim elementima i o izmjeni Uredbe (EU) 2019/1020 (COM(2022)0454).

organizacije trebale biti obvezne uvesti odgovarajuće mjere kojima će se osigurati njezina brza i zajamčena implementacija u okviru koordiniranog i odgovornost postupka otkrivanja;

78. smatra da bi države članice trebale raspodijeliti dostatne financijske, tehničke i ljudske resurse za istraživanje sigurnosti i ispravljanje ranjivosti;

79. poziva države članice da razviju postupke odlučivanja o otkrivanju svake ranjivosti, propisane zakonom, kojima se utvrđuje da se ranjivosti automatski moraju otkriti, a ne iskorištavati, te da svaka odluka o odstupanju od toga mora biti iznimka i mora se ocijeniti u skladu sa zahtjevima nužnosti i proporcionalnosti, uzimajući u obzir, među ostalim, koristi li se infrastrukturom koja je zahvaćena ranjivošću velik dio stanovništva, i mora biti podložna strogom nadzoru neovisnog nadzornog tijela i transparentnim postupcima i odlukama;

Telekomunikacijske mreže

80. naglašava da bi trebalo oduzeti dozvolu svakom pružatelju usluga za kojeg se utvrdi da olakšava nezakonit pristup nacionalnoj i/ili međunarodnoj infrastrukturi mobilnog signala svih generacija (trenutačno su to generacije od 2G do 5G);

81. naglašava da bi trebalo bolje regulirati postupke s pomoću kojih zlonamjerni akteri mogu stvoriti nove telefonske brojeve iz cijelog svijeta kako bi bilo teže sakriti nezakonite aktivnosti;

82. naglašava da si pružatelji telekomunikacijskih usluga moraju osigurati kapacitet za otkrivanje potencijalne zlouporabe pristupa infrastrukturi za signal, kontrole nad njome ili djelotvorne krajnje uporabe te infrastrukture, koje su stekle treće strane u okviru komercijalnih ili drugih sporazuma u državama članicama u kojima posluju;

83. poziva države članice da zajamče da nadležna nacionalna tijela u skladu s odredbama Direktive NIS 2 ocjenjuju razinu otpornosti pružatelja telekomunikacijskih usluga na neovlaštene ulaske;

84. poziva pružatelje telekomunikacijskih usluga da poduzmu odlučne i dokazive mjere ublažavanja protiv različitih oblika neovlaštene emulacije porijekla prometa telekomunikacijskih operatera od strane mrežnog elementa kako bi se pristupilo podacima ili usluzi namijenjenima zakonitom korisniku te drugih aktivnosti koje uključuju manipulaciju uobičajenim operacijama elemenata i infrastrukture mobilne mreže u svrhe nadzora od strane zlonamjernih aktera, uključujući aktere na razini države, kao i kriminalnih skupina;

85. poziva države članice da poduzmu mjere kako bi se zajamčilo da državni akteri iz trećih zemalja koji ne poštuju temeljna prava nemaju kontrolu nad strateškom infrastrukturom ili djelotvornu krajnju uporabu te infrastrukture ili utjecaj nad odlukama povezanim sa strateškom infrastrukturom unutar Unije, uključujući telekomunikacijsku infrastrukturu;

86. poziva sve države članice da daju prednost većim ulaganjima u zaštitu kritične infrastrukture poput nacionalnih telekomunikacijskih sustava kako bi se otklonili nedostaci u zaštiti od povreda privatnosti, curenja podataka i neovlaštenih ulazaka radi

obrane temeljnih prava građana;

87. poziva nadležna nacionalna tijela da aktivno promiču jačanje sposobnosti pružatelja usluga i sposobnosti za odgovor radi bolje potpore identifikaciji osoba koje su nezakonito podvrgnute nadzoru, obavješćivanju i izvješćivanju o incidentima kako bi se pružilo trajno, mjerljivo jamstvo i ublažavanje iskorištavanja sigurnosnih propusta od strane domaćih zlonamjernih aktera i onih iz trećih zemalja;

E-privatnost

88. poziva na brzo donošenje Uredbe o e-privatnosti na način koji u potpunosti odražava sudsku praksu o ograničenjima nacionalne sigurnosti i potrebu za sprečavanjem zlouporabe tehnologija nadzora, kojom se jača temeljno pravo na privatnost i predviđaju se snažne zaštitne mjere i djelotvorna provedba; ističe da opseg zakonitog presretanja ne bi trebao nadilaziti područje primjene Direktive o e-privatnosti (2002/58/EZ);

89. poziva na zaštitu svih elektroničkih komunikacija i metapodataka te svog sadržaja od zlouporabe osobnih podataka i privatnih komunikacija od strane privatnih društava i vladinih tijela; ističe da ne bi trebalo slabiti digitalne alate sigurnog dizajna poput prolaznog šifriranja;

90. poziva Komisiju da ocijeni kako države članice provode Direktivu o e-privatnosti diljem EU-a te da pokrene postupke zbog povrede prava u slučajevima kršenja;

Uloga Europola

91. napominje da je Europol u pismu upućenom predsjedniku odbora PEGA u travnju 2023. obavijestio taj odbor da je Europol stupio u kontakt s Grčkom, Mađarskom, Bugarskom, Španjolskom i Poljskom kako bi utvrdio jesu li u tijeku kaznene istrage ili druge istrage u skladu s primjenjivim odredbama nacionalnog prava kojima bi Europol mogao pružiti potporu ili su takve istrage predviđene; naglašava da nuđenje pomoći državama članicama ne predstavlja pokretanje, provođenje ili koordinaciju kaznene istrage kako je utvrđeno u članku 6.;

92. poziva Europol da u cijelosti iskoristi novostečene ovlasti temeljene na članku 6. stavku 1.a Uredbe (EU) 2022/991 koje mu omogućuju da prema potrebi nadležnim tijelima predmetnih država članica predloži pokretanje, provođenje ili koordiniranje istrage; ističe da je prema članku 6. na državama članicama da odbiju takav prijedlog;

93. poziva sve države članice da se obvežu Europskom parlamentu i Vijeću da će uključiti Europol u istrage nezakonite uporabe špijunskog softvera na nacionalnoj razini, posebno ako je podnesen prijedlog u skladu s člankom 6. stavkom 1.a Uredbe (EU) 2022/991;

94. poziva države članice da u okviru Europola uspostave registar nacionalnih operacija kaznenog progona koje uključuju uporabu špijunskog softvera u kojem bi svaka operacija trebala biti označena kodom i da se uporaba špijunskog softvera od strane vlada uvrsti u godišnje izvješće Europola o procjeni prijetnje organiziranog kriminala na internetu;

95. smatra da se mora pokrenuti razmatranje uloge Europola u slučaju da nacionalna tijela ne provedu istragu ili je odbiju provesti i da postoje jasne prijetnje interesima i sigurnosti EU-a;

Razvojne politike Unije

96. poziva Komisiju i ESVD da uvedu strože mehanizme kontrole kako bi se zajamčilo da se razvojnom pomoći Unije, uključujući doniranje tehnologije za nadzor i osposobljavanje za implementaciju softvera za nadzor, ne financiraju ili olakšavaju alati i aktivnosti kojima bi se mogla ugroziti načela demokracije, dobrog upravljanja, vladavine prava i poštovanja ljudskih prava ili koji su prijetnja međunarodnoj sigurnosti ili osnovnoj sigurnosti Unije i njezinih članica; napominje da bi procjene usklađenosti s pravom Unije, posebno Financijskom uredbom, koje provodi Komisija trebale sadržavati posebne kriterije kontrole i provedbene mehanizme za sprečavanje takvih zlouporaba, uključujući moguću privremenu obustavu pojedinih projekata ako se otkrije povreda tih načela;

97. poziva Komisiju i ESVD da u svaku procjenu učinka na ljudska i temeljna prava uključe postupak praćenja potencijalne zlouporabe nadzora kojim se u cijelosti uzima u obzir članak 51. Povelje o temeljnim pravima u roku od jedne godine [od objave preporuka odbora PEGA]; naglašava da se taj postupak mora predstaviti Parlamentu i Vijeću i da se ta procjena učinka mora provesti prije pružanja bilo kakve potpore trećim zemljama;

98. poziva ESVD da u Godišnjem izvješću EU-a o ljudskim pravima i demokraciji izvijesti o zlouporabi špijunskog softvera protiv boraca za ljudska prava;

Financijski propisi Unije

99. ističe da se mora poboljšati poštovanje ljudskih prava u financijskom sektoru; naglašava da se preporuke Vodećih načela UN-a 10+ moraju prenijeti u pravo Unije i da bi se Direktiva o dužnoj pažnji trebala u potpunosti primjenjivati na financijski sektor kako bi se zajamčilo poštovanje demokracije, ljudskih prava i vladavine prava u financijskom sektoru;

100. zabrinut je zbog implikacija odluke Suda Europske unije o Direktivi (EU) 2018/843 o sprečavanju korištenja financijskog sustava u svrhu pranja novca ili financiranja terorizma[36] kojima su informacije o stvarnom vlasništvu korporativnih i pravnih subjekata utvrđene u nacionalnom i javnom dostupnom registru stvarnog vlasništva (UBO) proglašene nevažećima[37]; naglašava da bi, uzimajući u obzir odluku Suda Europske unije, buduća direktiva trebala omogućiti što veći pristup javnosti kako bi postalo teže skriti kupnje ili prodaje špijunskog softvera posredstvom pomagača i posredničkih društava;

Daljnje djelovanje u vezi s rezolucijama Parlamenta

[36] Presuda od 22. studenoga 2022., spojeni predmeti C-37/20 i C-601/20, EU:C:2022:912.
[37] Sud Europske unije. Priopćenje za medije br. 188/22, Presuda Suda u spojenim predmetima C-37/20 i C-601/20.

101. traži hitno daljnje djelovanje u vezi s Rezolucijom Parlamenta od 12. ožujka 2014. o programu nadzora Agencije za nacionalnu sigurnost SAD-a (NSA), nadzornim tijelima u različitim državama članicama i njihovu utjecaju na temeljna prava građana EU-a te o transatlantskoj suradnji u pravosuđu i unutarnjim poslovima; naglašava da je hitno potrebno provesti preporuke iz te rezolucije;

102. ističe da, unatoč činjenici da bi se nadzor aktivnosti obavještajnih službi trebao temeljiti na demokratskoj legitimnosti (snažan pravni okvir, ex ante odobrenje i ex post provjera) i na odgovarajućoj tehničkoj sposobnosti i stručnosti, većini postojećih nadzornih tijela u EU-u i SAD-u drastično nedostaje i jedno i drugo, a posebno tehničke sposobnosti;

103. poziva, kao što je učinio i u slučaju Echelona, sve nacionalne parlamente koji to još nisu učinili da uvedu smislen nadzor obavještajnih aktivnosti koji će vršiti zastupnici u parlamentu ili stručna tijela s pravnim ovlastima za provedbu istrage; poziva nacionalne parlamente da zajamče da takvi nadzorni odbori / takva nadzorna tijela imaju dovoljno resursa, tehničke stručnosti i pravnih sredstava, uključujući pravo provođenja terenskih posjeta, kako bi mogli učinkovito kontrolirati obavještajne službe;

104. poziva na osnivanje skupine na visokoj razini koja će na transparentan način i u suradnji s parlamentima predložiti preporuke i daljnje korake koje treba poduzeti radi boljeg demokratskog nadzora obavještajnih službi, uključujući parlamentarni nadzor, te veće suradnje u području nadzora u EU-u, posebno u pogledu njegove prekogranične dimenzije;

105. smatra da bi ta skupina na visokoj razini trebala:

(a) utvrditi minimalne europske standarde ili smjernice o ex ante i ex post nadzoru obavještajnih službi koji se temelje na postojećim najboljim praksama i preporukama međunarodnih tijela kao što su UN i Vijeće Europe, uključujući pitanje nadzornih tijela koja se smatraju trećim stranama u skladu s „pravilom o trećoj strani" ili načelom „kontrole pošiljatelja", te o nadzoru i odgovornosti obavještajnih službi iz stranih zemalja;

(b) razviti kriterije o povećanoj transparentnosti koji bi se nadovezivali na opće načelo pristupa informacijama i takozvana „načela iz Tshwanea"[38];

106. planira organizirati parlamentarnu ili neovisnu konferenciju s nacionalnim nadzornim tijelima;

107. poziva države članice da primijene najbolju praksu kako bi poboljšale pristup svojih nadzornih tijela informacijama o obavještajnim aktivnostima, uključujući povjerljive informacije i informacije drugih službi, i uspostavile ovlasti za provedbu terenskih posjeta, opsežan skup ovlasti ispitivanja, odgovarajuće resurse i tehničku stručnost, strogu neovisnost o svojim vladama i obvezu izvješćivanja nacionalnih parlamenata;

108. poziva države članice da razviju suradnju među nadzornim tijelima;

109. poziva Komisiju da predstavi prijedlog postupka sigurnosne provjere svih dužnosnika u

[38] Globalna načela o nacionalnoj sigurnosti i pravu na informacije, lipanj 2013.

Uniji jer postojeći sustav koji se oslanja na sigurnosnu provjeru koju provodi država članica državljanstva uključuje različite zahtjeve i različita trajanja postupaka u nacionalnim sustavima, što dovodi do različitog postupanja prema zastupnicima u parlamentu i njihovu osoblju, ovisno o njihovom državljanstvu;

110. podsjeća na odredbe međuinstitucionalnog sporazuma između Europskog parlamenta i Vijeća o slanju povjerljivih podataka Vijeća Parlamentu i o rukovanju Parlamenta tim podacima, a koji se odnose na predmete koji ne pripadaju području zajedničke vanjske i sigurnosne politike, koji bi se trebali iskoristiti za poboljšanje nadzora na razini EU-a;

Istraživački programi Unije

111. traži provedbu strožih i djelotvornih mehanizama kontrole kako bi se zajamčilo da se sredstvima Unije za istraživanje ne financiraju ili ne olakšavaju alati, uključujući špijunski softver i sredstva nadzora, kojima se krše vrijednosti EU-a; napominje da bi procjene usklađenosti s pravom Unije trebale sadržavati posebne kriterije kontrole za sprečavanje takvih zlouporaba; poziva na obustavu sredstava Unije za istraživanje subjektima uključenim u izravno ili neizravno olakšavanje kršenja ljudskih prava s pomoću sredstava nadzora;

112. naglašava da se financijska sredstva EU-a za istraživanje poput sporazuma s trećim zemljama u okviru programa Obzor Europa ne smiju upotrebljavati za doprinos razvoju špijunskog softvera i jednakovrijednih tehnologija;

Tehnološki laboratorij EU-a

113. poziva Komisiju da bez odgode pokrene osnivanje neovisno vođenog europskog interdisciplinarnog instituta za istraživanje, s naglaskom na istraživanju i razvoju na temelju povezanosti informacijske i komunikacijske tehnologije, temeljnih prava i sigurnosti; naglašava da bi taj institut trebao surađivati sa stručnjacima, pripadnicima akademske zajednice i predstavnicima civilnog društva te biti otvoren za sudjelovanje stručnjaka i institucija država članica;

114. naglašava da bi taj institut doprinio boljoj osviještenosti te boljem utvrđivanju i snošenju odgovornosti u Europi i izvan nje, kao i širenju europske baze talenata i našeg razumijevanja načina na koji dobavljači špijunskog softvera razvijaju, održavaju, prodaju i pružaju svoje usluge trećim stranama;

115. smatra da bi taj institut trebao imati zadaću otkrivanja i razotkrivanja nezakonite uporabe softvera u svrhe nezakonitog nadzora, pružajući pristupačnu i besplatnu pravnu i tehnološku potporu, uključujući preglede pametnih telefona za pojedince koji sumnjaju da su predmet nadzora špijunskim softverom i alate potrebne za otkrivanje špijunskog softvera, provodeći forenzičko analitičko istraživanje za sudske istrage i redovito izvješćujući o uporabi i zlouporabi špijunskog softvera u EU-u, uzimajući u obzir tehnološka ažuriranja; smatra da bi to izvješće trebalo jednom godišnje stavljati na raspolaganje i dostavljati Komisiji, Parlamentu i Vijeću;

116. preporučuje da Komisija osnuje tehnološki laboratorij EU-a u bliskoj suradnji s Timom za hitne računalne intervencije za institucije, tijela i agencije EU-a (CERT-EU) i agencijom ENISA te da se pri osnivanju tehnološkog laboratorija EU-a savjetuje s

relevantnim stručnjacima u svrhu učenja iz najboljih praksi u akademskom području;

117. naglašava da je važno osigurati odgovarajuća financijska sredstva za tehnološki laboratorij EU-a;

118. preporučuje da Komisija predloži program certifikacije za analizu i utvrđivanje vjerodostojnosti forenzičkog materijala;

119. poziva Komisiju da pruži potporu kapacitetu civilnog društva na svjetskoj razini radi jačanja otpornosti na napade špijunskim softverom i pružanja pomoći i usluga građanima;

Vladavina prava

120. naglašava da je učinak nezakonite uporabe špijunskog softvera mnogo izraženiji u državama članicama u kojima je država preuzela kontrolu nad tijelima koja bi obično bila zadužena za istragu i pružanje pravne zaštite žrtvama te osiguravanje odgovornosti i da se u slučaju krize vladavine prava i ugroženosti neovisnosti pravosuđa ne može osloniti na nacionalna tijela;

121. stoga poziva Komisiju da zajamči djelotvornu provedbu svojih instrumenata za vladavinu prava, posebno:

(a) uspostavom sveobuhvatnijeg praćenja vladavine prava, uključujući preporuke za pojedinu zemlju povezane s nezakonitom uporabom špijunskog softvera od strane država članica u Komisijinu godišnjem izvješću o vladavini prava, uz procjenu reaktivnosti državnih institucija u pružanju pravne zaštite osobama koje su predmet nadzora, te proširenje područja primjene godišnjeg izvješća o vladavini prava i uključivanje svih izazova za demokraciju, vladavinu prava i temeljna prava, kako je navedeno u članku 2. UEU-a, kao što je Parlament opetovano tražio;

(b) proaktivnim pokretanjem i objedinjavanjem postupaka zbog povrede prava protiv država članica zbog nedostataka u pogledu vladavine prava kao što su prijetnje neovisnosti pravosuđa i djelotvornom funkcioniranju policije i tužiteljstva u kontekstu policijske i pravosudne suradnje u kaznenim stvarima;

Fond Unije za sudske sporove

122. poziva na to da se bez nepotrebne odgode uspostavi Fond Unije za sudske sporove kako bi se pokrili stvarni troškovi sudskih postupaka i kako bi se osobama koje su predmet nadzora špijunskim softverom omogućilo da zatraže odgovarajuću pravnu zaštitu, uključujući odštetu za nezakonitu uporabu špijunskog softvera protiv njih, u skladu s pripremnim djelovanjem koje je Parlament usvojio 2017., kako bi se uspostavio „fond EU-a za financijsku potporu za sudske postupke povezane s kršenjem demokracije, vladavine prava i temeljnih prava”;

Institucije EU-a

123. izražava zabrinutost zbog dosadašnjeg nedostatka djelovanja Komisije i potiče je da u potpunosti iskoristi sve svoje ovlasti čuvarice Ugovora te da provede sveobuhvatnu i

temeljitu istragu o zlouporabi špijunskog softvera i trgovini njime u Uniji;

124. potiče Komisiju da provede cjelovitu istragu o svim navodima i sumnjama na uporabu špijunskog softvera protiv njezinih dužnosnika te da po potrebi izvijesti Parlament i nadležna tijela kaznenog progona;

125. poziva Komisiju da osnuje posebnu radnu skupinu za zaštitu europskih izbora koji će se održati 2024. u cijeloj Uniji, u kojoj će sudjelovati nacionalna izborna povjerenstva; podsjeća da europskim izbornim procesima ne prijeti samo strano, već i unutarnje upletanje; naglašava da moguća zlouporaba sveprisutnih alata za nadzor poput Pegasusa može utjecati na izbore;

126. napominje da je odbor PEGA primio kolektivni odgovor Vijeća na upite Europskog parlamenta svim pojedinim državama članicama tek uoči objave nacrta izvješća, otprilike četiri mjeseca nakon pisama Parlamenta; izražava razočaranje zbog nedostatka djelovanja Europskog vijeća i Vijeća ministara te poziva na održavanje posebnog sastanka na vrhu Europskog vijeća s obzirom na razmjer prijetnje demokraciji u Europi;

127. poziva Vijeće EU-a da razmotri kretanja povezana s primjenom špijunskog softvera i njegovim utjecajem na vrijednosti utvrđene u članku 2. UEU-a tijekom saslušanja organiziranih u skladu s člankom 7. stavkom 1. UEU-a;

128. zauzima stajalište da bi Parlament trebao imati pune istražne ovlasti, uključujući bolji pristup klasificiranim i neklasificiranim podacima i ovlast da pozove svjedoke te da službeno zahtijeva od svjedoka da svjedoče pod prisegom i da dostave tražene informacije u određenim rokovima; ponavlja stajalište koje je Parlament iznio u svojem Prijedlogu uredbe Europskog parlamenta od 23. svibnja 2012. o detaljnim odredbama o izvršavanju prava Europskog parlamenta na istragu i o stavljanju izvan snage Odluke 95/167/EZ, Euratom, EZUČ Europskog parlamenta, Vijeća i Komisije[39] ; poziva Vijeće da odmah poduzme mjere na temelju tog Prijedloga uredbe kako bi se Europskom parlamentu omogućilo valjano pravo na istragu;

129. prima na znanje nastojanja Parlamenta usmjerena na otkrivanje zaraza špijunskim softverom; smatra, međutim, da bi trebalo ojačati zaštitu osoblja, uzimajući u obzir povlastice i imunitete osoba koje su podvrgnute špijuniranju; podsjeća da je svaki napad na politička prava nekog zastupnika u Europskom parlamentu napad na neovisnost i suverenost te institucije i napad na prava birača;

130. poziva Predsjedništvo Parlamenta da usvoji protokol za slučajeve u kojima su zastupnici ili osoblje Parlamenta postali izravan ili neizravan predmet nadzora špijunskim softverom i ističe da Parlament mora prijaviti sve slučajeve nadležnim tijelima kaznenog progona; naglašava da bi Parlament u takvim slučajevima trebao pružiti pravnu i tehničku pomoć;

131. odlučan je da povede inicijativu za pokretanje međuinstitucijske konferencije na kojoj Parlament, Vijeće i Komisija moraju težiti reformama upravljanja kojima bi se ojačao institucionalni kapacitet Unije za primjeren odgovor na napade na demokraciju i vladavinu prava iznutra te kako bi se osiguralo da Unija ima učinkovite nadnacionalne

[39] SL C 264 E, 13.9.2013, str. 41.

metode za provedbu Ugovorâ i sekundarnog prava u slučaju neusklađenosti država članica;

132. poziva na brzo donošenje Komisijina Prijedloga uredbe Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu kibersigurnosti u institucijama, tijelima, uredima i agencijama Unije (COM(2022)0122) te na njezinu brzu primjenu i strogu provedbu nakon toga kako bi se smanjio rizik da se uređaji i sustavi kojima se koristi osoblje i političari institucija EU-a zaraze špijunskim softverom;

133. poziva EU da potpiše Konvenciju br. 108+;

134. poziva Europskog ombudsmana da pokrene rasprave o utjecaju zlouporabe sveprisutnog nadzora na demokratske procese i prava građana u okviru Europske mreže pučkih pravobranitelja; poziva tu mrežu da izradi preporuke za djelotvornu i smislenu pravnu zaštitu u cijelom EU-u;

Zakonodavne mjere

135. poziva Komisiju da bez odgode iznese zakonodavne prijedloge na temelju ove preporuke;

°

° °

136. nalaže svojoj predsjednici da ovu Rezoluciju proslijedi državama članicama, Vijeću, Komisiji i Europolu.