Európai Parlament
2019-2024

Plenárisülés-dokumentum

B9-0260/2023

22.5.2023

AZ EURÓPAI PARLAMENT AJÁNLÁSTERVEZETE A TANÁCSNAK ÉS A BIZOTTSÁGNAK

az eljárási szabályzat 208. cikkének (12) bekezdése alapján

a Pegasus és azzal egyenértékű kémszoftverek használata tekintetében az uniós jog állítólagos megsértésének és az annak alkalmazása során állítólagosan elkövetett hivatali visszásságoknak a kivizsgálását követően (2023/2500(RSP))

Sophie in ‘t Veld
a Pegasus és azzal egyenértékű kémszoftverek használatának kivizsgálásával foglalkozó vizsgálóbizottság nevében

B9-0260/2023

Az Európai Parlament ajánlástervezete a Tanácsnak és a Bizottságnak a Pegasus és azzal egyenértékű kémszoftverek használata tekintetében az uniós jog állítólagos megsértésének és az annak alkalmazása során állítólagosan elkövetett hivatali visszásságoknak a kivizsgálását követően (2023/2500(RSP))

Az Európai Parlament,

– tekintettel az Európai Unióról szóló szerződésre (EUSZ) és különösen annak 2., 4., 6. és 21. cikkére,

– tekintettel az Európai Unió működéséről szóló szerződés (EUMSZ) 16., 223., 225. és 226. cikkére,

– tekintettel az Európai Unió Alapjogi Chartájára (a Charta) és különösen annak 7., 8., 11., 17., 21., 41., 42. és 47. cikkére,

– tekintettel az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló, 2002. július 12-i 2002/58/EK európai parlamenti és tanácsi irányelvre (elektronikus hírközlési adatvédelmi irányelv)[1],

– tekintettel a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv visszavonásáról szóló, 2016. április 27-i (EU) 2016/679 rendeletre (általános adatforgalmi rendelet)[2]

– tekintettel a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/680 európai parlamenti és tanácsi irányelvre[3],

– tekintettel az információs rendszerek elleni támadásokról szóló, 2013. augusztus 12-i (EU) 2013/40 európai parlamenti és tanácsi irányelvre[4] (a kiberbűnözésről szóló irányelv),

– tekintettel a kettős felhasználású termékek kivitelére, az azokkal végzett brókertevékenységre, az azokkal kapcsolatos technikai segítségnyújtásra, valamint azok tranzitjára és transzferjére vonatkozó uniós ellenőrzési rendszer kialakításáról szóló, 2021. május 20-i (EU) 2021/821 európai parlamenti és tanácsi rendeletre[5] (a kettős felhasználású termékekről szóló rendelet),

[1] HL L 201., 2002.7.31., 37. o.
[2] HL L 119., 2016.5.4., 1. o.
[3] HL L 119., 2016.5.4., 89. o.
[4] HL L 218., 2013.8.14., 8. o.
[5] HL L 206., 2021.6.11., 1. o.

– tekintettel a 2021. május 17-i (KKBP) 2021/796 tanácsi határozattal[6] módosított, az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről szóló, 2019. május 17-i (KKBP) 2019/797 tanácsi határozatra[7],

– tekintettel az Európai Parlament tagjainak közvetlen és általános választójog alapján történő választásáról szóló okmányra[8],

– tekintettel az Európai Parlament vizsgálati jogának gyakorlására vonatkozó részletes rendelkezésekről szóló, 1995. április 19-i 95/167/EK, Euratom, ESZAK európai parlamenti, tanácsi és bizottsági határozatra[9],

– tekintettel a Pegasus és azzal egyenértékű kémszoftverek használatának kivizsgálásával foglalkozó vizsgálóbizottság felállításáról, valamint a vizsgálat tárgyáról, illetve a bizottság feladatairól, összetételéről és mandátumának időtartamáról szóló, 2022. március 10-i (EU) 2022/480 európai parlamenti határozatra[10],

– tekintettel a pénzügyi rendszerek pénzmosás vagy terrorizmusfinanszírozás céljára való felhasználásának megelőzéséről szóló (EU) 2015/849 irányelv, valamint a 2009/139/EK és a 2013/36/EU irányelv módosításáról szóló, 2018. május 30-i (EU) 2018/843 európai parlamenti és tanácsi irányelvre[11] (pénzmosás elleni irányelv),

– tekintettel a belső piaci médiaszolgáltatások közös keretének létrehozásáról (az európai tömegtájékoztatás szabadságáról szóló jogszabály) és a 2010/13/EU irányelv módosításáról szóló európai parlamenti és tanácsi rendeletre irányuló 2022. szeptember 16-i javaslatra (COM(2022)0457),

– tekintettel az Emberi Jogok Egyetemes Nyilatkozatának 12. cikkére,

– tekintettel az Európai Unió Bíróságának a pénzmosás elleni irányelvről szóló C-37/20. sz. ítéletére[12], amely kimondja, hogy érvénytelen az a rendelkezés, amely szerint a tagállamok területén bejegyzett társaságok tényleges tulajdonlására vonatkozó információk minden esetben hozzáférhetők a nyilvánosság bármely tagja számára,

– tekintettel a Polgári és Politikai Jogok Nemzetközi Egyezségokmányának 17. cikkére,

– tekintettel az Egyesült Nemzetek Alapokmányára és az üzleti vállalkozások emberi jogi felelősségére vonatkozó ENSZ-irányelvekre[13],

– tekintettel az ENSZ emberi jogi főbiztosának, Michelle Bachelet-nek „Az újságírók és az emberijog-védők megfigyelésére használt kémszoftverek használata” című 2022. július 19-i nyilatkozatára,

---

[6] HL L 174. I, 2021.5.18., 13. o.
[7] HL L 129. I, 2019.5.17., 13. o.
[8] HL L 278., 1976.10.8., 5. o.
[9] HL L 113., 1995.5.19., 1. o.
[10] HL L 98., 2022.3.25., 72. o.
[11] HL L 156., 2018.6.19., 43–74. o.
[12] A Bíróság (nagytanács) 2022. november 22-i WM és Sovim SA kontra Luxembourg Business Registers ítélete, C-37/20, EU:C:2022:912.
[13] https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

– tekintettel az Európa Tanács emberi jogi biztosának, Dunja Mijatović-nek „A rendkívül tolakodó kémszoftverek veszélyeztetik az emberi jogok lényegét” című 2023. január 27-i megjegyzésére[14],

– tekintettel az európai adatvédelmi biztosnak a korszerű kémszoftverekkel kapcsolatos 2022. február 15-i előzetes megjegyzéseire[15],

– tekintettel az emberi jogok és alapvető szabadságjogok védelméről szóló európai egyezményre és különösen annak 8., 10., 13. és 17. cikkére, valamint az egyezményhez csatolt jegyzőkönyvekre,

– tekintettel az Europol súlyos és szervezett bűnözés általi fenyegetettségének „The infiltration and undermining of Europe’s economy and society by organised crimes” (Romboló befolyás: A szervezett bűnözés beszivárgása Európa gazdaságába és társadalmába és azok aláásása) című 2021. évi értékelését (SOCTA),

– tekintettel az Európai Unió Alapjogi Ügynökségének „Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU” (A hírszerző szolgálatok általi megfigyelés: az alapvető jogokkal kapcsolatos garanciák és jogorvoslatok az EU-ban) című 2017. évi jelentésére, valamint annak 2023. február 28-án a Pegasus és azzal egyenértékű kémszoftverek használatának kivizsgálásával foglalkozó vizsgálóbizottságnak (PEGA) bemutatott frissítéseire,

– tekintettel az egyesült államokbeli NSA megfigyelési programjáról, a különféle tagállamokban megfigyelést végző szervekről és az uniós polgárok alapvető jogaira gyakorolt hatásukról, valamint a transzatlanti bel- és igazságügyi együttműködésről szóló, 2014. március 12-i állásfoglalására[16], és különösen az uniós intézmények, szervek és ügynökségek informatikai biztonságának megerősítésére vonatkozó ajánlásaira,

– tekintettel az európai adatvédelmi biztosnak az európai tömegtájékoztatás szabadságáról szóló jogszabállyal kapcsolatos 2022. november 11-i 24/2022. sz. véleményére,

– tekintettel az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) kémszoftverekkel és kártékony szoftverekkel kapcsolatos fogalomtárára,

– tekintettel az Európai ombudsman „How the European Commission assessed human rights impacts before providing support to African countries to develop surveillance capabilities” (Hogyan értékelte az Európai Bizottság az emberi jogi hatásokat, mielőtt támogatást nyújtott volna az afrikai országoknak megfigyelési képességeik fejlesztéséhez?) című határozatára (1904/2021/MHZ. sz. ügy),

– tekintettel a véleményalkotás és véleménynyilvánítás szabadságához való jog előmozdításával és védelmével foglalkozó különleges ENSZ-előadó, Irene Kahn, valamint a kisebbségi kérdésekkel foglalkozó különleges ENSZ-előadó, Fernand de Varennes 2023. február 2-i nyilatkozatára, amelyben követelik a katalán vezetők elleni

[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] HL C 378., 2017.11.9., 104. o.

állítólagos kémszoftvertámadás kivizsgálását[17],

– tekintettel a Jog a Demokráciáért Európai Bizottságnak (Velencei Bizottság) a biztonsági szolgálatok demokratikus felügyeletéről szóló jelentésére[18], valamint a „Lengyelország – A rendőrségi törvényt és egyéb törvényeket módosító, 2016. január 15-i törvényről szóló vélemény” című véleményére[19],

– tekintettel a Pegasus és azzal egyenértékű kémszoftverek használatának kivizsgálásával foglalkozó vizsgálóbizottság jelentésére (A9-0189/2023),

– tekintettel eljárási szabályzata 208. cikkének (12) bekezdésére,

A. mivel a CitizenLabnek és az Amnesty Technek, valamint számos oknyomozó újságírónak köszönhetően kiderült, hogy több ország – mind tagállamok, mind nem uniós országok – kormányzati szervei a Pegasus és azzal egyenértékű kémszoftvereket használtak újságírók, politikusok, bűnüldöző szervek tisztviselői, diplomaták, ügyvédek, üzletemberek, civil társadalmi szereplők és más szereplők ellen politikai célokra, sőt bűncselekmények céljára; mivel ezek a gyakorlatok rendkívül aggasztóak, és rámutatnak arra a kockázatra, hogy az alapvető emberi jogok, a demokrácia és a választási folyamatok aláásása érdekében visszaélnek a megfigyelési technológiákkal;

B. mivel a jelentésben a „kémszoftver” kifejezés alatt a PEGA bizottság felállításáról szóló parlamenti határozatban meghatározott „Pegasus és azzal egyenértékű kémszoftver” értendő;

C. mivel megállapítást nyert, hogy állami szereplők szándékosan, félrevezető módon használtak olyan kémszoftvereket, amelyek legális programnak, fájlnak vagy tartalomnak álcázhatják magukat („trójai faló”), például a közintézmények nevében küldött hamis üzenetek formájában; mivel egyes esetekben a hatóságok a telefonszolgáltatók kihasználásával továbbítottak rosszindulatú tartalmat a célszemély eszközére; mivel a kémszoftverek nulladik napi sebezhetőségek kihasználásával telepíthetők a célobjektum és a fertőzött tartalom közötti interakció nélkül, és eltávolításkor képesek eltüntetni a jelenlétük minden nyomát, valamint anonimizálni a távoli operátorok és a szerver közötti kapcsolatot;

D. mivel a mobilkommunikáció kezdeti időszakában a lehallgatás a hívások lehallgatásával, később pedig az egyszerű szöveges üzenetek megszerzésével történt;

E. mivel a titkosított mobilkommunikációs alkalmazások megjelenése a kémszoftveripar kialakulásához vezetett, amely az okostelefonok operatív rendszereinek meglévő sebezhetőségeit kihasználva olyan szoftvereket telepít a telefonra, amelyekkel kémszoftvereket lehet a telefonba importálni, akár „zéró kattintásos” fertőzéssel a felhasználó tudta vagy a felhasználó bármilyen cselekménye nélkül, lehetővé téve az adatok titkosítás előtti kinyerését; mivel a „zéró kattintásos” kémszoftver már kialakításánál fogva is nagyon megnehezíti használatának hatékony és érdemi

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

vizsgálatát;

F. mivel a szoftverrendszerek sebezhetőségeire vonatkozó ismeretekkel a felek közvetlenül kereskednek, vagy ezt közvetítők segítik elő; mivel e kereskedelemben nem állami szereplők és bűnszervezetek is részt vesznek;

G. mivel a nulladik napi sebezhetőségek beszerzése, kereskedelme és felhalmozása alapvetően aláássa a kommunikáció integritását és biztonságát, valamint az uniós polgárok kiberbiztonságát;

H. mivel a kémszoftverrel folytatott megfigyelésnek továbbra is kivételnek kell maradnia, és azt mindig egy pártatlan és független bírósági hatóság kötelező erejű, hatékony és érdemi előzetes bírósági engedélyéhez kell kötni, amelynek biztosítania kell, hogy az intézkedés szükséges és arányos legyen, és szigorúan a nemzetbiztonságot, a terrorizmust és a súlyos bűncselekményeket érintő esetekre korlátozódjon; mivel a megfigyelési technikákkal jellemzően visszaélnek olyan környezetben, ahol nincsenek hatékony fékek és ellensúlyok;

I. mivel minden kémszoftverrel folytatott megfigyelést egy független utólagos felügyeleti hatóságnak kell ellenőriznie, amelynek biztosítania kell, hogy az engedélyezett megfigyelés az alapvető jogokkal összhangban és az Európai Unió Bírósága (EUB), az Emberi Jogok Európai Bírósága (EJEB) és a Velencei Bizottság által meghatározott feltételeknek megfelelően történik; mivel az utólagos felügyeleti hatóságnak el kell rendelnie a felügyelet azonnali megszüntetését, amennyiben az összeegyeztethetetlennek bizonyul a fent említett jogokkal és feltételekkel;

J. mivel az uniós jogban, valamint az EUB és az EJEB ítélkezési gyakorlatában meghatározott követelményeknek nem megfelelő kémszoftveres megfigyelés ellentétes az EUSZ 2. cikkében foglalt értékkel, valamint a Chartában és különösen annak 7., 8., 11., 17., 21. és 47. cikkében foglalt alapvető jogokkal, amelyek elismerik a bennük foglalt konkrét jogokat, szabadságokat és elveket, mint amilyen a magán- és családi élet tiszteletben tartása, a személyes adatok védelme, a véleménynyilvánítás és a tájékozódás szabadsága, a tulajdonhoz való jog, a megkülönböztetésmentességhez való jog, valamint a hatékony jogorvoslathoz, a tisztességes eljáráshoz és az ártatlanság vélelméhez való jog;

K. mivel a célszemélyek jogait, nevezetesen a magánélethez való jogot és a tisztességes eljáráshoz való jogot a Charta és nemzetközi egyezmények, valamint a gyanúsítottak és vádlottak jogaira vonatkozó uniós szabályok rögzítik; mivel ezeket a jogokat az EUB és az EJEB ítélkezési gyakorlata is megerősítette;

L. mivel a célzott megfigyelés nőkre gyakorolt hatása különösen súlyos lehet, mert a hatóságok a nők fokozott társadalmi ellenőrzését kihasználva fegyverként alkalmazhatják a rágalmazási kampányok során kémszoftverek segítségével megszerzett magánjellegű és intim adatokat;

M. mivel a célszemélyek tanúvallomásaiból egyértelmű, hogy még ha papíron léteznek is jogorvoslati lehetőségek és polgári jogok, azok többnyire érvényüket vesztik a kormányzati szervek általi akadályoztatás, a célszemélyek esetében a tájékoztatáshoz való jog érvényre juttatásának elmaradása és azon adminisztratív akadályok miatt, hogy

a célszemélynek bizonyítania kell célponttá válását; mivel a kémprogramok jellege még a gyors és nyílt eljárású rendszerekben is nagyon megnehezíti a szerzőség, valamint annak bizonyítását, hogy egy adott személy milyen módon és milyen mértékben vált célponttá;

N. mivel a bíróságok nem fogadták el a független szakértőktől származó igazságügyi szakértői bizonyítékokat, hanem csak a hatóságok, a biztonsági vagy bűnüldöző szervek által végzett vizsgálaton alapuló bizonyítékokat, amelyek állítólag a támadás mögött állnak; mivel ez paradox helyzetet teremt a célszemélyek számára, amelyben nincs lehetőségük a kémszoftver-fertőzés bizonyítására;

O. mivel a lengyel kormány meggyengítette és megszüntette az intézményi és jogi biztosítékokat, beleértve a megfelelő felügyeleti és ellenőrzési eljárásokat, így a célba vett személyek gyakorlatilag érdemi jogorvoslat nélkül maradtak; mivel a Pegasus kémszoftvert jogellenesen alkalmazták politikai célokra újságírók, ellenzéki politikusok, ügyvédek, ügyészek és a civil társadalom szereplői elleni kémkedésre;

P. mivel a magyar kormány meggyengítette és megszüntette az intézményi és jogi biztosítékokat, beleértve a megfelelő felügyeleti és ellenőrzési eljárásokat, így a célba vett személyek gyakorlatilag érdemi jogorvoslat nélkül maradtak; mivel a Pegasus kémszoftvert jogellenesen alkalmazták politikai célokra újságírók, ellenzéki politikusok, ügyvédek, ügyészek és a civil társadalom szereplői elleni kémkedésre;

Q. mivel hivatalosan is megerősítették, hogy egy görög európai parlamenti képviselőt és egy görög újságírót a görög Nemzeti Hírszerző Szolgálat (EYP) lehallgatott és Predator kémprogrammal célba vett; mivel a Meta egy korábbi amerikai–görög alkalmazottját az EYP egyidejűleg lehallgatta és Predator kémprogrammal célba vette, amelynek használata a görög törvények alapján jogellenes; mivel médiabeszámolók szerint a görögországi ellenzéki és kormánypárti parlamenti képviselők, pártaktivisták és újságírók állítólag szintén célpontjai voltak a Predator kémprogramnak vagy az EYP hagyományos lehallgatásának, illetve mindkettőnek; mivel a görög kormány tagadja, hogy megvásárolta vagy használta volna a Predatort, de nagyon valószínű, hogy a Predatort a miniszterelnöki hivatalhoz nagyon közel álló személyek használták, illetve az ő nevükben vetették be; mivel a görög kormány elismerte, hogy exportengedélyeket adott az Intellexa vállalatnak, hogy elnyomó kormányoknak, mint Madagaszkárnak és Szudánnak adja el a Predator kémszoftvert; mivel a kormány olyan jogalkotási módosításokkal reagált a botrányra, amelyek tovább szűkítik a célszemélyek jogát arra, hogy a megfigyelést követően tájékoztatást kapjanak, és még inkább hátráltatják a független hatóságok munkáját;

R. mivel a leleplezések nyomán a kémszoftverek célpontjainak két kategóriáját azonosították Spanyolországban; mivel az elsőbe tartozik a miniszterelnök és a védelmi miniszter, a belügyminiszter és más magas rangú tisztviselők; mivel a második kategóriába tartozik a CitizenLab szervezet által „CatalanGate” néven emlegetett ügy mintegy 65 célszemélye, köztük Katalónia regionális önkormányzatának politikai személyiségei, a katalán függetlenségi mozgalom tagjai, európai parlamenti képviselők, ügyvédek, tudományos szakemberek és a civil társadalom szereplői; mivel a spanyol hatóságok 2022 májusában elismerték, hogy 18 személyt bírósági engedéllyel célba vettek, bár semmilyen végzést vagy egyéb információt nem mutattak be, és amikor

megkérték őket, hogy magyarázzák meg a kémszoftveres megfigyelés spanyolországi alkalmazását, a nemzetbiztonságra hivatkoztak; mivel állítólag 47 másik személyt is célba vettek, de a Citizen Lab-on kívül senki mástól nem kaptak információt;

S. mivel Cipruson nem erősítettek meg állítólagos kémszoftverfertőzéseket; mivel Ciprus a megfigyelési szektor fontos európai exportközpontja, és vonzó helyszín a megfigyelési technológiákat értékesítő vállalatok számára;

T. mivel komoly jelek utalnak arra, hogy többek között Marokkó és Ruanda kormányai kémszoftverrel támadtak meg magas rangú uniós személyiségeket, köztük Franciaország elnökét, Spanyolország miniszterelnökét, hadügyminiszterét és védelmi miniszterét, Belgium akkori miniszterelnökét, a Bizottság korábbi elnökét és Olaszország korábbi miniszterelnökét, valamint Carine Kanimbát, Paul Rusesabagina lányát;

U. mivel biztonsággal feltételezhető, hogy minden tagállam vásárolt vagy használt egy vagy több kémprogramrendszert; mivel az Európai Unió legtöbb kormánya tartózkodni fog a kémszoftverek jogellenes használatától, de a visszaélések kockázata nagyon valószínű a biztosítékokkal és felügyelettel megerősített szilárd jogi keret hiányában, valamint a fertőzések felderítésével és nyomon követésével kapcsolatos technikai kihívások fényében;

V. mivel a legtöbb tagállam kormánya és parlamentje a már nyilvánosan ismerteken túl nem nyújtott érdemi tájékoztatást az Európai Parlamentnek a kémszoftverek használatát szabályozó jogi keretéről, annak ellenére, hogy az Európai Parlament vizsgálati jogának gyakorlását szabályozó részletes rendelkezésekről szóló, 1995. március 6-i európai parlamenti, tanácsi és bizottsági határozat 3. cikkének (4) bekezdése értelmében kötelezettek erre; mivel nehéz értékelni az uniós jogszabályok végrehajtását, valamint a biztosítékok, a felügyelet és a jogorvoslati lehetőségek érvényre juttatását, ami megakadályozza a polgárok alapvető jogainak megfelelő védelmét;

W. mivel az EUSZ 4. cikkének (3) bekezdése kimondja: „Az Unió és a tagállamok a lojális együttműködés elvének megfelelően kölcsönösen tiszteletben tartják és segítik egymást a Szerződésekből eredő feladatok végrehajtásában”;

X. mivel a kémszoftveripar legfontosabb szereplői máltai állampolgárságot szereztek, ami megkönnyíti az Unióban és az Unióból folytatott tevékenységüket;

Y. mivel sok kémszoftverszállító -és fejlesztő egy vagy több tagállamban van vagy volt bejegyezve; mivel példaként említhető a luxemburgi, ciprusi, hollandiai és bulgáriai vállalati jelenléttel rendelkező NSO Group, az Intellexa anyavállalata, a Thalestris Limited Írországban, Görögországban, Svájcban és Cipruson, az ausztriai DSIRF, a franciaországi Amesys és Nexa Technologies, az olaszországi Tykelab és RCS Lab, valamint a németországi FinFisher (ma már nem létezik);

Z. mivel az Európai Unió nem vesz részt a hagyományos fegyverek és kettős felhasználású termékek és technológiák exportjának ellenőrzéséről szóló Wassenaari Megállapodásban; mivel Ciprus kivételével valamennyi tagállam részt vesz a Wassenaari Megállapodásban, bár Ciprus már régen benyújtotta a Wassenaari Megállapodáshoz való csatlakozás iránti kérelmét; mivel Ciprust köti a kettős

felhasználású termékekről szóló rendelet;

AA. mivel Izrael exportrendszere[20] elvben minden izraeli állampolgárra érvényes, még akkor is, ha az EU-ból tevékenykedik; mivel Izrael nem vesz részt a Wassenaari Megállapodásban, de azt állítja, hogy ennek ellenére alkalmazza annak előírásait;

AB. mivel a kémszoftverek Unióból nem uniós országokba történő kivitelét a kettős felhasználású termékekről szóló, 2021-ben felülvizsgált rendelet szabályozza; mivel a Bizottság 2022 szeptemberében adta ki első végrehajtási jelentését[21];

AC. mivel a harmadik országokba exportáló kémszoftvergyártók közül néhány az Unióban telepedik le, hogy jó hírnévre és tiszteletre tegyen szert, miközben kémszoftvereket forgalmaz az elnyomó rezsimek számára; mivel az Unióból elnyomó rezsimek vagy nem állami szereplők számára történő export sérti az uniós exportszabályokat;

AD. mivel az Amesys és a Nexa Technologies ellen jelenleg Franciaországban folyik eljárás megfigyelési technológia Líbiába, Egyiptomba és Szaúd-Arábiába történő exportálása miatt; mivel az Intellexa görögországi székhelyű vállalatai állítólag Bangladesbe, Szudánba, Madagaszkárra és legalább egy arab országba exportálták termékeiket; mivel a FinFisher szoftverét a világ több tucat országában használják, többek között Angolában, Bahreinben, Bangladesben, Egyiptomban, Etiópiában, Gabonban, Jordániában, Kazahsztánban, Mianmarban, Ománban, Katarban, Szaúd-Arábiában, Törökországban, valamint Marokkó hírszerző szolgálataiban, amelyeket az Amnesty International és a Forbidden Stories azzal váddal illetett, hogy a Pegasus kémszoftvert használják újságírók, emberijog-védők, a civil társadalom és politikusok ellen; mivel nem ismert, hogy a kémszoftverek ezen országokba történő exportjára adtak-e ki kiviteli engedélyeket;

AE. mivel a kémszoftverképességeket forgalmazó fegyvervásárok és az ISSWorld résztvevőinek száma azt mutatja, hogy túlsúlyban vannak a kémszoftverek és a kapcsolódó termékek és szolgáltatások harmadik országbeli szolgáltatói, amelyek között jelentős számban vannak izraeli székhelyű vállalatok (pl. NSO Group, Wintego, Quadream és Cellebrite), és hogy kiemelkedő gyártók vannak Indiában (ClearTrail), az Egyesült Királyságban (BAe Systems és Black Cube) és az Egyesült Arab Emírségekben (DarkMatter), eközben pedig az Egyesült Államok izraeli (NSO Group és Candiru), oroszországi (Positive Technologies) és szingapúri (Computer Security Initiative Consultancy PTE LTD.) kémszoftvergyártókat helyezett tiltólistára, ami rávilágít a kémszoftvergyártók származásának sokféleségére; mivel a vásáron az európai hatóságok széles köre, köztük a helyi rendőrségi erők is részt vesznek;

AF. mivel az EUSZ 4. cikkének (2) bekezdése szerint a nemzetbiztonság továbbra is az egyes tagállamok kizárólagos hatáskörébe tartozik;

AG. mivel azonban az EUB úgy határozott (C-623/17. sz. ügy), hogy „noha alapvető biztonsági érdekeik meghatározása, valamint a külső és belső biztonságukat szolgáló, megfelelő intézkedések meghozatala a tagállamok feladatkörébe tartozik, önmagában az

[20] A védelmi termékek és technológiák exportellenőrzéséről szóló 5766-2007. sz. törvény, Izraeli Védelmi Minisztérium.
[21] https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=COM%3A2022%3A434%3AFIN&qid=1662029750223

a tény, hogy egy nemzeti intézkedést a nemzetbiztonság védelme érdekében fogadtak el, még nem eredményezi az uniós jog alkalmazhatatlanságát és nem mentesíti a tagállamokat az uniós jog kellő tiszteletben tartása alól”;

AH. mivel az EUB úgy határozott (C-203/15. sz. ügy), hogy: „A 2009. november 25-i 2009/136/EK európai parlamenti és tanácsi irányelvvel módosított, az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról [helyesen: a személyes adatok kezeléséről] és a magánélet védelméről szóló, 2002. július 12-i 2002/58/EK európai parlamenti és tanácsi irányelv (elektronikus hírközlési adatvédelmi irányelv) 15. cikkének (1) bekezdését – az Európai Unió Alapjogi Chartája 7., 8. és 11. cikkével, valamint 52. cikkének (1) bekezdésével összefüggésben – úgy kell értelmezni, hogy azzal ellentétes az olyan nemzeti szabályozás, amely a bűnözés elleni küzdelem céljából minden elektronikus hírközlési eszköz tekintetében valamennyi előfizető és nyilvántartott felhasználó összes forgalmi és helymeghatározó adatának általános és különbségtétel nélküli megőrzését írja elő”;

AI. mivel az EUB úgy határozott (C-203/15. sz. ügy), hogy: „A 2009/136 irányelvvel módosított 2002/58 irányelv 15. cikkének (1) bekezdését – az Alapjogi Charta 7., 8. és 11. cikkével, valamint 52. cikkének (1) bekezdésével összefüggésben – úgy kell értelmezni, hogy azzal ellentétes az olyan nemzeti szabályozás, amely anélkül szabályozza a forgalmi és helymeghatározó adatok védelmét és biztonságát, különösen az illetékes nemzeti hatóságoknak a megőrzött adatokhoz való hozzáférését, hogy a bűnözés elleni küzdelem keretében történő e hozzáférést kizárólag a súlyos bűncselekmények elleni küzdelem céljára korlátozná, és bíróság vagy független közigazgatási szerv előzetes felülvizsgálatához kötné, továbbá megkövetelné, hogy a szóban forgó adatokat az Unió területén őrizzék”;

AJ. mivel az EJEB ítélkezési gyakorlata egyértelművé teszi, hogy minden megfigyelésnek a joggal összhangban kell történnie, törvényes célt kell szolgálnia, valamint szükségesnek és arányosnak kell lennie; mivel ezen túlmenően a jogi keretnek pontos, hatékony és átfogó biztosítékokat kell nyújtania a megfigyelési intézkedések elrendelésére, végrehajtására és lehetséges jogorvoslati lehetőségeire vonatkozóan, amelyeket megfelelő bírósági felülvizsgálatnak és hatékony felügyeletnek kell alávetni[22];

AK. mivel az Európa Tanácsnak a személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezménye (108. sz. egyezmény), amelyet nemrégiben korszerűsítettek, és a 108+ Egyezmény nevet kapta, a személyes adatok állami (nemzetbiztonsági) célú feldolgozására alkalmazandó, beleértve a honvédelmet is; mivel ennek az egyezménynek valamennyi tagállam részes fele;

AL. mivel a megfigyelési kémszoftverek bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása és büntetőjogi szankciók végrehajtása céljából, többek között a köz- vagy a nemzetbiztonságot fenyegető veszélyekkel szembeni védelem és e veszélyek megelőzése érdekében történő használatának fontos aspektusai az uniós jog hatálya alá tartoznak;

AM. mivel a Charta meghatározza az alapvető jogok gyakorlásának korlátozására vonatkozó feltételeket, előírva, hogy arról törvényben kell rendelkezni, tiszteletben kell tartani az

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

érintett jogok és szabadságok lényegét, szem előtt kell tartani az arányosság elvét és csak akkor lehet alkalmazni, ha az szükséges és ténylegesen az Unió által elismert általános érdekű célkitűzéseket vagy mások jogainak és szabadságainak védelmét szolgálja; mivel a kémszoftverek használata esetén a magánélethez való jogba való beavatkozás mértéke olyan súlyos lehet, hogy az egyént ténylegesen megfosztják tőle, és a felhasználás nem tekinthető mindig arányosnak, függetlenül attól, hogy az intézkedés szükségesnek tekinthető-e egy demokratikus állam legitim céljainak eléréséhez;

AN. mivel az elektronikus hírközlési adatvédelmi irányelv előírja, hogy a tagállamoknak biztosítaniuk kell a közlések titkosságát; mivel a megfigyelési eszközök alkalmazása korlátozza a végberendezések védelméhez való jogot, amelyet az elektronikus hírközlési adatvédelmi irányelv garantál; mivel az ilyen korlátozások a kémszoftverekre vonatkozó nemzeti jogszabályokat – az adatmegőrzésre vonatkozó nemzeti jogszabályokhoz hasonlóan – az elektronikus hírközlési adatvédelmi irányelv hatálya alá helyeznék; mivel a behatoló kémszoftver-technológia gyakori alkalmazása nem egyeztethető össze az uniós jogrenddel;

AO. mivel a nemzetközi jog értelmében egy államnak csak a saját joghatóságán belül van joga a lehetséges bűncselekmények kivizsgálására, és más államok segítségét kell igénybe vennie, ha a nyomozást más államokban kell lefolytatni, kivéve, ha nemzetközi megállapodás vagy – a tagállamok esetében – az uniós jog alapján van jogalap a nyomozás más joghatóságok területén történő lefolytatására;

AP. mivel egy készülék kémszoftverrel való megfertőzése és az ezt követő adatgyűjtés a mobilszolgáltatók szerverein keresztül történik; mivel az Unión belüli ingyenes barangolás azt eredményezte, hogy a személyek néha más tagállamokban kötött mobilszerződéssel rendelkeznek, mint a lakóhelyük szerinti tagállam, az uniós jogban jelenleg nincs jogalap a másik tagállamban kémszoftverek alkalmazásával történő adatgyűjtésre;

AQ. mivel David Kaye, a véleményalkotás és véleménynyilvánítás szabadságához való jog előmozdításával és védelmével foglalkozó korábbi különleges ENSZ-előadó[23], valamint Irene Khan, a véleményalkotás és véleménynyilvánítás szabadságához való jog előmozdításával és védelmével foglalkozó jelenlegi különleges ENSZ-előadó[24], azonnali moratóriumot kér a megfigyelési eszközök használatára, átadására és értékesítésére vonatkozóan mindaddig, amíg szigorú emberi jogi biztosítékokat nem vezetnek be a gyakorlatok szabályozására és annak biztosítására, hogy a kormányok és a nem állami szereplők jogszerű módon használják az eszközöket;

AR. mivel vannak olyan esetek, amikor kémszoftverrel foglalkozó vállalatok, különösen az Intellexa, nemcsak magát a lehallgatási és adatkinyerési technológiát értékesítették, hanem „hekkerszolgáltatásnak” vagy „aktív kiberhírszerzésnek” is nevezett egész

[23] „Surveillance and human rights” (Megfigyelés és emberi jogok), a véleményalkotás és véleménynyilvánítás szabadságához való jog előmozdításával és védelmével foglalkozó különleges előadó jelentése, A/HRC/41/35, 2019.

[24] „Spyware scandal: UN experts call for moratorium on sale of ‘life threatening’ surveillance tech” (Kémszoftverbotrány: Az ENSZ szakértői moratóriumot sürgetnek az „életveszélyes” megfigyelési technológiák értékesítésére vonatkozóan), az ENSZ Emberi Jogi Főbiztosának Hivatala.

szolgáltatást is, megfigyelési és lehallgatási technológiai módszereket, valamint képzést és technikai, operatív és módszertani támogatást kínálva a személyzet számára; mivel ez a szolgáltatás lehetővé teheti a vállalat számára, hogy a teljes megfigyelési művelet felett ellenőrzést gyakoroljon, és összesítse a megfigyelési adatokat; mivel az illetékes hatóságok számára ezt a gyakorlatot szinte lehetetlen felügyelni és ellenőrizni; mivel ez megnehezíti az arányosság, a szükségesség, a legitimitás, a jogszerűség és a megfelelőség elveinek betartását; mivel ezt a szolgáltatást Izrael védelmi exportügynöksége (DECA) nem engedélyezi; mivel Ciprust arra használták fel, hogy megkerüljék az izraeli törvények által előírt korlátozásokat hekkerszolgáltatás nyújtása érdekében;

AS. mivel a tagállamoknak meg kell felelniük a közbeszerzésről szóló 2014/24/EU irányelvnek, illetve a védelmi beszerzésekről szóló 2009/81/EK irányelvnek; mivel a tagállamoknak megfelelően indokolniuk kell az EUMSZ 346. cikke (1) bekezdésének b) pontja szerinti eltéréseket, mivel a 2009/81/EK irányelv kifejezetten figyelembe veszi a védelmi beszerzések érzékeny jellemzőit, valamint be kell tartaniuk a közbeszerzésekről szóló, 2012. március 30-án módosított WTO-megállapodást[25] (GPA), amennyiben részes felei annak;

AT. mivel az európai adatvédelmi biztos hangsúlyozta, hogy a tagállamoknak tiszteletben kell tartaniuk az emberi jogokról szóló európai egyezményt és az EJEB joggyakorlatát, amely korlátozza a nemzetbiztonsággal kapcsolatos megfigyelési tevékenységeket; mivel ezen túlmenően a bűnüldözési célú felhasználásnak meg kell felelnie az uniós jognak, különösen az Alapjogi Chartának, valamint az olyan uniós irányelveknek, mint az elektronikus hírközlési adatvédelmi irányelv és a bűnüldözési irányelv;

AU. mivel a beszámolók szerint nagy pénzügyi intézmények megpróbálták arra buzdítani a kémszoftvergyártókat, hogy ne alkalmazzák a megfelelő emberi jogi normákat és a kellő gondosságot, hanem továbbra is adjanak el kémszoftvereket elnyomó rezsimeknek;

AV. mivel a Horizont 2020 programban Izrael a programban való általános részvétel tekintetében a harmadik helyen áll a társult országok között; mivel az Izraellel kötött Horizont Európa-megállapodás teljes költségvetése 95,5 milliárd euró a 2021–27 közötti időszakra[26]; mivel ezeken az európai programokon[27] keresztül pénzeszközöket bocsátottak az izraeli katonai és biztonsági vállalatok rendelkezésére;

AW. mivel az uniós fejlesztési politikák fő jogalkotási eszköze az (EU) 2021/947 rendelet[28], a „Globális Európa rendelet”, és az uniós finanszírozás a költségvetési rendeletben előirányzott finanszírozási típusokon keresztül nyújtható; mivel a támogatást fel lehet

[25] https://www.wto.org/english/tratop_e/gproc_e/gpa_1994_e.htm
[26] https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/israel-joins-horizon-europe-research-and-innovation-programme-2021-12-06_en
[27] https://webgate.ec.europa.eu/dashboard/extensions/CountryProfile/CountryProfile.html?Country=Israel; https://elbitsystems.com/products/comercial-aviation/innovation-rd/
[28] Az Európai Parlament és a Tanács (EU) 2021/947 rendelete (2021. június 9.) a Szomszédsági, Fejlesztési és Nemzetközi Együttműködési Eszköz (Globális Európa) létrehozásáról, a 466/2014/EU európai parlamenti és tanácsi határozat módosításáról és hatályon kívül helyezéséről, valamint az (EU) 2017/1601 európai parlamenti és tanácsi rendelet és a 480/2009/EK, Euratom tanácsi rendelet hatályon kívül helyezéséről, HL L 209., 2021.6.14., 1. o.

függeszteni, ha a demokrácia, az emberi jogok vagy a jogállamiság helyzete romlik a harmadik országokban;

1. kiemeli a magánélet védelmének, a méltósághoz, a magán- és családi élethez, a véleménynyilvánítás és a tájékozódás szabadságához, a gyülekezési és egyesülési szabadsághoz, valamint a tisztességes eljáráshoz való jognak a tagadhatatlan fontosságát, különösen egy egyre inkább digitális világban, ahol tevékenységeink egyre nagyobb része zajlik online;

2. határozottan úgy véli, hogy ezen alapvető jogok és szabadságok megsértése kulcsfontosságú a Szerződésekben és más forrásokban meghatározott közös jogelvek tiszteletben tartása szempontjából, és megjegyzi, hogy maga a demokrácia forog kockán, mivel a kémszoftverek politikusokkal, civil társadalommal és újságírókkal szembeni használata elrettentő hatással bír, és súlyosan érinti a békés gyülekezéshez, a véleménynyilvánítás szabadságához és a közéleti részvételhez való jogot;

3. határozottan elítéli, hogy a tagállamok kormányai és hatóságaik tisztviselői vagy állami intézmények kémszoftvereket használnak politikai célokra az ellenzék tagjai, bírálóik és a civil társadalom megfigyelése, zsarolása, megfélemlítése, manipulálása és hiteltelenítése, a demokratikus ellenőrzés és a szabad sajtó felszámolása, a választások manipulálása, valamint a bírák, ügyészek és ügyvédek célba vétele révén a jogállamiság aláásása céljából;

4. rámutat arra, hogy a kémszoftverek nemzeti és nem uniós országbeli kormányok általi jogellenes használata közvetlenül és közvetve hatással van az uniós intézményekre és a döntéshozatali folyamatra, és ezáltal aláássa az európai uniós demokrácia integritását;

5. súlyos aggodalommal veszi tudomásul, hogy az Unió jelenlegi irányítási struktúrája alapvetően alkalmatlan arra, hogy reagáljon az Unión belülről a demokrácia, az alapvető jogok és a jogállamiság ellen intézett támadásokra, és hogy sok tagállam szinte semmilyen intézkedést sem tesz; megállapítja, hogy amikor egy tagállamban ezek veszélybe kerülnek, az az egész EU-ban veszélybe sodorja;

6. hangsúlyozza, hogy az Unióban a technológiai fejlesztéseket szabályozó digitális szabványoknak tiszteletben kell tartaniuk az alapvető jogokat;

7. határozottan úgy véli, hogy a kémszoftvereknek az Unióból diktatúrákba és gyenge emberi jogi helyzetű, elnyomó rezsimekbe történő exportja, ahol ezeket az eszközöket emberi jogi aktivisták, újságírók és kormányt bíráló emberek ellen használják fel, a Chartában rögzített alapvető jogok súlyos megsértését és az uniós exportszabályok durva megsértését jelenti;

8. aggodalmát fejezi ki amiatt is, hogy a tagállamok jogszerűtlenül használják a kémszoftvereket, és jogellenesen kereskednek velük, és ez együttesen a kémprogram-ipar célpontjává teszik az Uniót;

9. aggodalmát fejezi amiatt, hogy nem uniós országok kémszoftverekkel támadtak meg magas rangú személyiségeket, emberijog-védőket és újságírókat az Unióban;

10. ugyanilyen aggodalommal tölti el, hogy láthatóan visszafogottan vizsgálják ki a

kémszoftverrel való visszaéléseket, mind azokban az esetekben, amikor a gyanúsított egy tagállam kormányzati szerve, mind amikor egy nem uniós országé; megjegyzi, hogy az uniós tagállamok kormányfői és miniszterei, a Bizottság tagjai, valamint a civil társadalom tagjai, az újságírók és a politikai ellenfelek ellen kémszoftverekkel való visszaéléssel kapcsolatos bírósági vizsgálatok nagyon lassan haladnak, és nem eléggé átláthatóak;

11. megjegyzi, hogy egyes tagállamok jogi kerete nem nyújt megfelelő pontosságú, hatékony és átfogó biztosítékokat a megfigyelési intézkedések elrendelésére, végrehajtására és lehetséges jogorvoslati mechanizmusaira vonatkozóan; megállapítja, hogy az ilyen intézkedéseknek jogos célt kell szolgálniuk, valamint szükségesnek és arányosnak kell lenniük;

12. sajnálatát fejezi ki amiatt, hogy a tagállamok kormányai, a Tanács és a Bizottság nem tudtak teljes mértékben együttműködni a vizsgálattal, és nem tudtak megosztani minden releváns és érdemi információt annak érdekében, hogy segítsék a vizsgálóbizottságot mandátumában foglalt feladatai ellátásában; elismeri, hogy ezen információk egy részére szigorú titoktartási és bizalmassági követelmények vonatkozhatnak; úgy véli, hogy a Tanács kollektív válasza teljesen elégtelen, és ellentétes az EUSZ 4. cikkének (3) bekezdésében foglalt lojális együttműködés elvével;

13. arra a következtetésre jut, hogy sem a tagállamok, sem a Tanács, sem a Bizottság nem érdekelt a kémszoftverekkel való visszaélés teljes körű kivizsgálására irányuló erőfeszítéseik maximalizálásában, és ezzel tudatosan védi azokat az uniós kormányokat, amelyek az Unióban és azon kívül is megsértik az emberi jogokat;

14. megállapítja, hogy Lengyelországban súlyosan megsértették az uniós jogot, és hivatali visszásságokat követtek el az uniós jog végrehajtása során;

15. felszólítja Lengyelországot, hogy:

a) sürgesse a legfőbb ügyészséget, hogy indítson vizsgálatot a kémszoftverekkel való visszaélések ügyében;

b) sürgősen állítsa helyre az elégséges intézményi és jogi biztosítékokat, beleértve a hatékony és kötelező előzetes és utólagos ellenőrzést, valamint a független felügyeleti mechanizmusokat, többek között a megfigyelési tevékenységek bírósági felülvizsgálatát; hangsúlyozza, hogy a hatékony előzetes ellenőrzés keretében az operatív megfigyelés iránti kérelemnek, valamint az ilyen megfigyelésre vonatkozó bírósági határozatnak egyértelműen meg kell indokolnia és jeleznie kell a megfigyeléshez használandó technikai eszközöket, és hogy a hatékony utólagos ellenőrzés keretében ellenőrizni kell azon kötelezettség teljesítését, hogy a megfigyelés alá vont személyt tájékoztatni kell az operatív megfigyelés során szerzett adatok feldolgozásának tényéről, időtartamáról, hatóköréről és módjáról;

c) vezessen be konzisztens jogszabályokat, amelyek védik a polgárokat, függetlenül attól, hogy az operatív megfigyelést az államügyész hivatala, valamely titkosszolgálat vagy más állami szerv végzi;

d) tartsa be az Alkotmánybíróság 1990. évi rendőrségi törvényről szóló határozatát;

e) tartsa be a Velencei Bizottság 2016. évi rendőrségi törvényről szóló véleményét;

f) tartsa be az EJEB különböző ítéleteit, például a Roman Zakharov kontra Oroszország ügyben 2015-ben hozott ítéletet, amely hangsúlyozza a szigorú megfigyelési kritériumok, a megfelelő bírói engedélyezés és felügyelet, a nem releváns adatok azonnali megsemmisítésének, a sürgősségi eljárások bírói ellenőrzésének és a célszemélyek értesítésének szükségességét, továbbá a Klass és mások kontra Németország ügyben 1978-ban hozott ítéletet, amely szerint a megfigyelésnek kellően fontosnak kell lennie ahhoz, hogy szükségessé tegye a magánéletbe való ilyen jellegű beavatkozást;

g) tartsa be az EUB és az EJEB valamennyi, az igazságszolgáltatás függetlenségével és az uniós jog elsőbbségével kapcsolatos ítéletét;

h) vonja vissza a 2016. évi büntetőeljárási törvénykönyv módosításáról szóló átdolgozott törvény 168a. cikkét;

i) állítsa helyre az igazságszolgáltatás teljes függetlenségét, és tartsa tiszteletben valamennyi érintett felügyeleti szerv – például az ombudsman, a személyes adatok védelmével foglalkozó hivatal elnöke és a legfőbb ellenőrző hivatal – jogkörét annak biztosítása érdekében, hogy valamennyi felügyeleti szerv teljes együttműködésben részesüljön, és hozzáférjen az információkhoz, valamint hogy valamennyi célszemély teljes körű tájékoztatást kapjon;

j) minden benyújtott kereset esetében sürgősen vezesse be az ügyek véletlenszerű kiosztását a bíróságok bírái között, még hétvégén és a rendes munkaidőn kívül is, hogy elkerüljék, hogy a titkosszolgálatok „szimpatizáló bírákat” válasszanak ki, és gondoskodjon róla, hogy ez a rendszer átláthatóan működjön, többek között hozzák nyilvánosságra azt az algoritmust, amely alapján véletlenszerű módon az ügyhöz rendelik a bírát;

k) állítsa vissza a parlamenti felügyelet hagyományos rendszerét, amelyben az ellenzéki párt veszi át a Különleges Szolgálatok Parlamenti Felügyelőbizottságának (KSS) elnöki tisztét;

(l) sürgősen tisztázza a kémszoftverekkel kapcsolatos lengyelországi visszaélések körülményeit, hogy ne lehessen kétségbe vonni a közelgő választások tisztaságát;

m) megfelelően hajtsa végre és érvényesítse az (EU) 2016/680 irányelvet (a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv), és biztosítsa, hogy az adatvédelmi hatóság hatáskörrel rendelkezzen a személyes adatoknak többek között olyan hatóságok általi kezelése felett, mint a Központi Korrupcióellenes Hivatal és a Belbiztonsági Ügynökség;

n) hajtsa végre a visszaéléseket bejelentő személyek védelméről szóló uniós irányelvet;

o) tartózkodjon az elektronikus kommunikációval kapcsolatos új jogszabályok azon elemeinek bevezetésétől, amelyek ellentétesek az emberi jogok európai egyezményével;

p) gondoskodjon róla, hogy hatékony jogorvoslati lehetőségek álljanak azon lengyel

polgárok rendelkezésére, akiket hátrányosan érint a lengyel alkotmánnyal és az emberi jogok európai egyezményével ellentétes jogszabályok bevezetése;

q) kérje fel az Europolt, hogy vizsgálja ki a kémszoftverekkel való állítólagos visszaélések minden esetét;

r) garantálja a lengyel törvények független alkotmányos felülvizsgálatát;

s) állítsa vissza a legfőbb ügyész igazságügyi minisztertől való függetlenségét annak érdekében, hogy az alapvető jogok állítólagos megsértésével kapcsolatos vizsgálatok mentesek legyenek a politikai megfontolásoktól;

16. sürgeti a Bizottságot, hogy vizsgálja meg, kompatibilis-e a bűnmegelőzés és a bűnözés elleni küzdelem keretében feldolgozott személyes adatok védelméről szóló 2018-as lengyel törvény az EU bűnüldözésben érvényesítendő adatvédelemről szóló irányelvével, és ha szükséges, indítson kötelezettségszegési eljárást;

17. megállapítja, hogy Magyarországon súlyosan megsértették az uniós jogot, és hivatali visszásságokat követtek el annak végrehajtása során;

18. felszólítja Magyarországot, hogy:

a) sürgősen állítsa helyre az elégséges intézményi és jogi biztosítékokat, beleértve a hatékony, kötelező érvényű előzetes és utólagos ellenőrzést, valamint a független felügyeleti mechanizmusokat; beleértve a megfigyelési tevékenységek bírósági felülvizsgálatát; hangsúlyozza, hogy a hatékony előzetes ellenőrzés keretében az operatív megfigyelés iránti kérelemnek, valamint az ilyen megfigyelésre vonatkozó bírósági határozatnak egyértelműen meg kell indokolnia és jeleznie kell a megfigyeléshez használandó technikai eszközöket, és hogy a hatékony utólagos ellenőrzés keretében ellenőrizni kell azon kötelezettség teljesítését, hogy a megfigyelés alá vont személyt tájékoztatni kell az operatív megfigyelés során szerzett adatok feldolgozásának tényéről, időtartamáról, hatóköréről és módjáról;

b) tartsa be az EJEB különböző ítéleteit, például a Roman Zakharov kontra Oroszország ügyben 2015-ben hozott ítéletet, amely hangsúlyozza a szigorú megfigyelési kritériumok, a megfelelő bírói engedélyezés és felügyelet, a nem releváns adatok azonnali megsemmisítésének, a sürgősségi eljárások bírói ellenőrzésének és a célszemélyek értesítésének szükségességét, továbbá a Klass és mások kontra Németország ügyben 1978-ban hozott ítéletet, amely szerint a megfigyelésnek kellően fontosnak kell lennie ahhoz, hogy szükségessé tegye a magánéletbe való ilyen jellegű beavatkozást, továbbá a megfigyelt személyek értesítésére vonatkozó követelményt;

c) tartsa be az EUB és az EJEB valamennyi, az igazságszolgáltatás függetlenségével és az uniós jog elsőbbségével kapcsolatos ítéletét;

d) az EJEB Hüttl kontra Magyarország ügyben hozott ítéletével összhangban állítsa vissza a független felügyeleti szerveket, amelyben a bíróság megállapítja, hogy a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) nem képes ellátni a kémszoftverek használatának független felügyeletét, mivel a titkosszolgálatok a titoktartásra hivatkozva jogosultak megtagadni a hozzáférést bizonyos

dokumentumokhoz;

e) állítsa helyre az igazságszolgáltatás és valamennyi érintett felügyeleti szerv – például az ombudsman és az adatvédelmi hatóságok – teljes függetlenségét annak biztosítása érdekében, hogy valamennyi felügyeleti szerv teljes együttműködésben részesüljön, és hozzáférjen az információkhoz, valamint hogy valamennyi célszemély teljes körű tájékoztatást kapjon;

f) helyezze vissza a független alkalmazottakat a felügyeleti szervek, például az Alkotmánybíróság, a Legfelsőbb Bíróság, a Számvevőszék, az ügyészség, a Magyar Nemzeti Bank és a Nemzeti Választási Bizottság vezető tisztségeibe;

g) hajtsa végre a visszaéléseket bejelentő személyek védelméről szóló uniós irányelvet;

h) kérje fel az Europolt, hogy vizsgálja ki a kémszoftverekkel való állítólagos visszaélések minden esetét;

i) tartózkodjon az elektronikus kommunikációval kapcsolatos új jogszabályok azon elemeinek bevezetésétől, amelyek ellentétesek az emberi jogok európai egyezményével;

j) gondoskodjon róla, hogy hatékony jogorvoslati lehetőségek álljanak azon magyar polgárok rendelkezésére, akiket hátrányosan érint a magyar alkotmánnyal és az emberi jogok európai egyezményével ellentétes jogszabályok bevezetése;

19. megállapítja, hogy Görögországban megsértették az uniós jogot, és hivatali visszásságokat követtek el annak végrehajtása során;

20. felszólítja Görögországot, hogy:

a) sürgősen állítsa helyre és erősítse meg az intézményi és jogi biztosítékokat, beleértve a hatékony előzetes és utólagos ellenőrzést, valamint a független felügyeleti mechanizmusokat;

b) sürgősen vonja vissza az összes olyan exportengedélyt, amely nincs teljes összhangban a kettős felhasználású termékekről szóló rendelettel, és vizsgálja ki a többek között Szudánba irányuló jogellenes kivitelre vonatkozó állításokat;

c) biztosítsa, hogy a hatóságok szabadon és akadálytalanul kivizsgálhassák a kémszoftverek használatával kapcsolatos összes állítást;

d) sürgősen vonja vissza a 2472/1997. sz. törvény 826/145. sz. módosítását, amely eltörölte, hogy a Görög Kommunikációbiztonsági és Adatvédelmi Hatóság (ADAE) értesítheti a polgárokat a közlések titkosságának feloldásáról; módosítsa az 5002/2022. sz. törvényt annak érdekében, hogy a megfigyelés befejezését követően kérelemre helyreállítsa a célszemélyek azonnali tájékoztatáshoz való jogát, és módosítsa a biztosítékokat, az ellenőrzést és az elszámoltathatóságot gyengítő egyéb rendelkezéseket;

e) állítsa helyre az igazságszolgáltatás és valamennyi érintett felügyeleti szerv – például az ombudsman és az adatvédelmi hatóságok – teljes függetlenségét, és teljes mértékben

tartsa tiszteletben az ADAE függetlenségét annak biztosítása érdekében, hogy valamennyi felügyeleti és ellenőrző szerv teljes együttműködésben részesüljön, és hozzáférjen az információkhoz, valamint hogy valamennyi célszemély teljes körű tájékoztatást kapjon;

f) gondoskodjon róla, hogy az ADAE létrehozhasson egy elektronikus nyilvántartást, hogy elvégezhesse a feladatát;

g) sürgősen tisztázza a kémszoftverekkel kapcsolatos görögországi visszaélések körülményeit, hogy ne lehessen kétségbe vonni a közelgő választások tisztaságát;

h) vonja vissza a 2019-es törvénymódosítást, amely a Nemzeti Hírszerző Szolgálatot (EYP) a miniszterelnök közvetlen ellenőrzése alá helyezte; gondoskodjon az alkotmányos garanciák helyreállításáról, és tegye lehetővé működésének parlamentáris ellenőrzését, és ne hivatkozzon az információk bizalmasságának ürügyére;

i) biztosítsa az Országos Átláthatósági Hatóság (EAD) vezetőségének függetlenségét;

j) biztosítsa, hogy az igazságszolgáltatás számára rendelkezésre álljon az összes eszköz és támogatás a kémszoftverekkel való állítólagos visszaélések kivizsgálásához, és a tárgyi bizonyítékok lefoglalásához a kémszoftverfertőzésekben érintett megbízottakkal, közvetítőkkel és kémszoftver-forgalmazókkal kapcsolatban;

k) kérje fel az Europolt, hogy azonnal csatlakozzon a nyomozáshoz;

l) ne gyakoroljon politikai nyomást a legfőbb ügyészre;

21. arra a következtetésre jut, hogy Spanyolország szabályozási kerete összességében összhangban van a Szerződésekben meghatározott követelményekkel; rámutat azonban arra, hogy szükség van bizonyos reformokra, és a gyakorlati végrehajtásnak teljes mértékben összhangban kell lennie az alapvető jogokkal, és biztosítania kell a nyilvánosság részvételének védelmét;

22. felszólítja ezért Spanyolországot, hogy:

a) végezzen teljes körű, tisztességes és hatékony vizsgálatot, amelynek során teljes mértékben tisztázzák a kémszoftverek használatával kapcsolatos valamennyi állítólagos esetet, beleértve azt a 47 esetet is, amelyekben továbbra sem egyértelmű, hogy az érintett személyeket bírósági végzés alapján figyelte-e meg a Spanyol Nemzeti Hírszerzési Ügynökség (CNI), vagy más hatóság kapott-e bírósági végzést azok jogszerű megfigyelésére, valamint a kémszoftvereknek a miniszterelnökkel és a kormány tagjaival szembeni használatáról, és hogy a megállapításokat a lehető legszélesebb körben ismertesse, az alkalmazandó jogszabályokkal összhangban;

b) biztosítson megfelelő hozzáférést a célszemélyek számára a Legfelsőbb Bíróság által a CNI számára kiadott, 18 személy megfigyelésére vonatkozó bírósági felhatalmazáshoz;

c) működjön együtt a bíróságokkal annak biztosítása érdekében, hogy a kémszoftverekkel célba vett személyek valódi és érdemi jogorvoslathoz férjenek hozzá, valamint hogy a bírósági vizsgálatokat késedelem nélkül, pártatlan és alapos módon lezárják, amihez

elegendő forrást kell biztosítani;

d) a 2022 májusában bejelentetteknek megfelelően kezdje meg a CNI jogi keretének reformját;

e) kérje fel az Europolt, hogy technikai szakértelemmel járuljon hozzá a nyomozásokhoz;

23. megállapítja, hogy bizonyíték van rá, hogy Cipruson hivatali visszásságokat követtek el a kettős felhasználású termékekről szóló uniós jog végrehajtása során, ami szigorú ellenőrzést igényel;

24. felszólítja Ciprust, hogy:

a) alaposan vizsgálja meg a kémszoftverekre kiadott összes exportengedélyt, és adott esetben helyezze hatályon kívül azokat;

b) alaposan vizsgálja ki a kémszoftverekhez használt anyagok szállítását az EU belső piacán, a tagállamok között, és térképezze fel az ebben a tevékenységben érintett izraeli cégeket, amelyeket izraeli állampolgárok működtetnek, de Cipruson vannak bejegyezve;

c) a bizottság ciprusi hivatalos látogatása során megfogalmazott kérésnek megfelelően tegye közzé a különleges nyomozó által a „Spyware Van” ügyben készített jelentést;

d) az Europol segítségével teljes körűen vizsgálja ki a kémszoftverek jogellenes használatára és kivitelére vonatkozó valamennyi állítást, különösen amikor újságírók, ügyvédek, a civil társadalom szereplői és a ciprusi polgárok ellen használták a szoftvert;

25. úgy véli, hogy a többi tagállamban kialakult helyzet is aggodalomra ad okot, különösen a jövedelmező és bővülő kémszoftveripar jelenléte miatt, amely kihasználja az Unió jó hírnevét, az egységes piacot és a szabad mozgást, lehetővé téve az olyan tagállamok, mint például Ciprus és Bulgária számára, hogy a kémszoftverek exportközpontjává váljanak a világ autokrata rendszerei felé;

26. úgy véli, hogy az, hogy egyes nemzeti hatóságok elmulasztják vagy megtagadják az uniós polgárok megfelelő védelmének biztosítását, illetve a szabályozási kiskapuk és a jogi eszközök hiánya a szükséges egyértelműséggel bizonyítja, hogy uniós szintű fellépés elengedhetetlen a Szerződések betartatása és az uniós jogszabályok tiszteletben tartása érdekében, hogy a polgárok a biztonságos létkörnyezethez, az emberi méltósághoz, a magánélethez, a személyes adatokhoz és a magántulajdonhoz való jogát tiszteletben tartsák, amit a 2012/29/EU irányelv is előír, amely szerint a bűntettek minden áldozatának jár az egyéni igényeinek megfelelő támogatás és védelem;

27. megállapítja, hogy a Bizottság és az Európai Külügyi Szolgálat (EKSZ) nagymértékű mulasztásokat követett el az uniós jog végrehajtása során, amikor nem uniós országoknak – többek között, de nem kizárólagosan a Száhel-övezet 10 ilyen országának – támogatást nyújtott, hogy lehetővé tegye számukra a megfigyelési

képességek fejlesztését[29];

28. álláspontja szerint a kémszoftverek kereskedelmét és használatát szigorúan szabályozni kell; elismeri ugyanakkor, hogy a jogalkotási folyamat hosszabb időt vehet igénybe, de a visszaéléseket azonnal fel kell számolni; felszólít a kémszoftverek jogszerű használatára, értékesítésére, beszerzésére és átadására vonatkozó feltételek elfogadására; kitart amellett, hogy a kémszoftverek további használata érdekében a tagállamoknak 2023. december 31-ig teljesíteniük kell az alábbi feltételek mindegyikét:

a) a kémszoftverekkel való állítólagos visszaélések minden esetét a megfelelő bűnüldöző, ügyészi és igazságügyi hatóságok teljes körűen kivizsgálják és haladéktalanul megoldják;

b) bizonyítják, hogy a kémszoftverek használatát szabályozó keretrendszer összhangban van a Velencei Bizottság által meghatározott normákkal, valamint az EUB és az EJEB idevágó ítélkezési gyakorlatával;

c) kifejezett kötelezettségvállalást tesznek arra, hogy bevonják az Europolt a vizsgálatokba az Europol-rendelet 4., 5. és 6. cikke alapján a kémszoftverek jogellenes használatára vonatkozó állítások kivizsgálását illetően; és

d) visszavonnak minden olyan exportengedélyt, amely nem felel meg teljes mértékben a kettős felhasználású termékekről szóló rendeletnek;

29. úgy véli, hogy e feltételek teljesülését a Bizottságnak 2023. november 30-ig értékelnie kell; úgy véli továbbá, hogy az értékelés eredményeit jelentés formájában a nyilvánosság számára közzé kell tenni;

30. hangsúlyozza, hogy bár a súlyos bűncselekmények és a terrorizmus elleni küzdelem és az ehhez kapcsolódó képességek rendkívül lényegesek a tagállamok számára, az alapvető jogok és a demokrácia védelme is alapvető fontosságú; hangsúlyozza továbbá, hogy a tagállamoknak kizárólag arányosan szabad kémszoftvereket használniuk, és ez nem lehet önkényes, megfigyelést pedig csak szigorúan definiált, előre meghatározott esetekben szabad engedélyezni; úgy véli, hogy a személyhez fűződő szabadságjogok védelme érdekében hatékony ex ante mechanizmusokra és igazságszolgáltatási ellenőrzésre van szükség; megismétli, hogy a megfigyelési eszközökhöz való korlátlan hozzáférés engedélyezése nem sodorhatja veszélybe a személyhez fűződő jogokat; rámutat, hogy az is fontos, hogy az igazságszolgáltatás hatékony és érdemi utólagos ellenőrzéseket végezhessen a nemzetbiztonsági célú megfigyelési kérelmek kapcsán, és ellenérveket fogalmazhasson meg, ha a kormányzatok aránytalan módon szeretnék használni a kémszoftvereket;

31. hangsúlyozza, hogy a kémszoftverek bűnüldözési célú használatát közvetlenül szabályozni kell az EUMSZ büntetőügyekben folytatott igazságügyi együttműködésről szóló 5. címének 4. fejezetén alapuló intézkedések révén; hangsúlyozza, hogy az EU-ba importált és más módon forgalomba hozott kémszoftverek konfigurációját az EUMSZ 114. cikkén alapuló intézkedéssel kell szabályozni; megjegyzi, hogy a kémszoftverek

[29] Az 1904/2021/MHZ ügyben hozott határozat, elérhető a következő internetcímen: https://www.ombudsman.europa.eu/hu/decision/hu/163491.

nemzetbiztonsági célú használata csak közvetetten szabályozható, például az alapvető jogok és az adatvédelemre vonatkozó szabályok révén;

32. úgy véli, hogy a kémszoftverek használatának transznacionális és uniós dimenziója miatt uniós szinten összehangolt és átlátható ellenőrzésre van szükség nemcsak az uniós polgárok védelmének biztosítása érdekében, hanem a kémszoftverek révén a határokon átnyúló ügyekben gyűjtött bizonyítékok érvényességének biztosítása érdekében is, és hogy egyértelműen szükség van közös uniós normákra az EUMSZ 5. címének 4. fejezete alapján, amely a kémszoftverek tagállami szervek általi használatát szabályozza, az EUB, az EJEB, a Velencei Bizottság és az Alapjogi Ügynökség által meghatározott normák alapján[30]; úgy véli, hogy ezeknek az uniós előírásoknak legalább a következő elemekre kell kiterjedniük:

a) a kémszoftverek használatát kizárólag kivételes és konkrét esetekben szabad engedélyezni, ha erre a nemzetbiztonság védelme érdekében szükség van, és a kémszoftverek tervezett használatához egy minden releváns információhoz hozzáférő, pártatlan és független igazságügyi hatóság vagy más független demokratikus felügyeleti intézmény által kiadott érvényes, kötelező és érdemi előzetes bírósági engedélyt kell kérni, amely igazolja a tervezett intézkedés szükségességét és arányosságát;

b) a kémszoftverrel végzett támadás csak addig tarthat, ameddig feltétlenül szükséges, a bírósági engedélyben minden feltört készülékre vonatkozóan előzetesen meg kell határozni a pontos alkalmazási kört és időtartamot, és a feltöréses támadás csak akkor hosszabbítható meg, ha újabb bírósági engedélyt adnak egy másik meghatározott időtartamra, tekintettel a kémszoftver jellegére és a visszamenőleges megfigyelés lehetőségére; a tagállami hatóságok a továbbiakban kizárólag egyéni végfelhasználói készülékeket vagy fiókokat vehetnek célba, és tartózkodniuk kell az internet- és más technológiai szolgáltatók feltörésétől, így kerülve el a nem célszemély felhasználók érintettségét;

c) a kémszoftverek használatára vonatkozó engedélyt csak kivételes esetekben, pontosan és egyértelműen meghatározott bűncselekmények egy korlátozott körű és zárt listájával kapcsolatos nyomozás tekintetében lehet megadni, amelyek valódi nemzetbiztonsági fenyegetést jelentenek, és a kémszoftverek csak olyan személyek ellen használhatók, akik esetében elegendő jel utal arra, hogy ilyen súlyos bűncselekményeket követtek el vagy terveznek elkövetni;

d) tilos kémszoftverekkel hozzáférni olyan adatokhoz, amelyek számára védelmet biztosítanak a bizonyos foglalkozási kategóriákhoz (például politikusok, orvosok stb.) tartozó immunitások, bizonyos védett kapcsolatok (például az ügyvédi titoktartás), vagy a sajtó- és véleményszabadság értelmében a büntetőjogi felelősséget korlátozó szabályok, kivéve, ha bírói ellenőrzés mellett bizonyítást nyer, hogy ezek a személyek bűncselekményekben vagy nemzetbiztonsági jelentőségű ügyekben vesznek részt, amelyekhez egyébiránt közös keretrendszert kell kidolgozni;

[30] Alapjogi Ügynökség, „*Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU" (A hírszerző szolgálatok általi megfigyelés: az alapvető jogokkal kapcsolatos garanciák és jogorvoslatok az EU-ban) – II. kötet, összefoglaló*, 2017, https://fra.europa.eu/en/publication/2017/surveillance-intelligence-services-fundamental-rights-safeguards-and-remedies-eu.

e) egyedi szabályokat kell kidolgozni a kémszoftver-technológiával végzett megfigyelésre, mivel az korlátlan visszamenőleges hozzáférést tesz lehetővé az üzenetekhez, fájlokhoz és metaadatokhoz;

f) a tagállamoknak közzé kell tenniük legalább a jóváhagyott és elutasított megfigyelési kérelmek számát, valamint a vizsgálat típusát és célját, és minden egyes vizsgálatot anonim módon, egyedi azonosítóval rögzíteniük kell egy nemzeti nyilvántartásban, hogy visszaélés gyanúja esetén az ügy kivizsgálható legyen;

g) a nemzeti ellenőrző szerveknek jelentést kell tenniük a tagállamoknak, majd ezt követően a tagállamoknak rendszeresen értesíteniük kell a Bizottságot ezekről az információkról; a Bizottságnak éves jogállamisági jelentésében fel kell használnia ezeket az információkat, hogy lehetővé tegye a kémszoftverek tagállamokban történő használatának összehasonlítását;

h) a megfigyelt személy értesítéshez való joga: a megfigyelés befejezése után a hatóságoknak értesíteniük kell a személyt arról, hogy a hatóságok kémszoftvert használtak ellene, amely értesítés tartalmazza a megfigyelés időpontjára és időtartamára, a megfigyelési műveletre kiadott parancsra, a megszerzett adatokra, az adatok felhasználásának módjára és az adatokat felhasználó szereplőkre vonatkozó információkat, valamint az adatok törlésének időpontját és a közigazgatási és törvényi jogorvoslati lehetőségekhez való jogot, és e jog gyakorlásának módját az illetékes hatóságoknál; megjegyzi, hogy ezt az értesítést indokolatlan késedelem nélkül kell megtenni, kivéve, ha egy független igazságügyi hatóság engedélyezi az értesítés elhalasztását, amely esetben az azonnali értesítés súlyosan veszélyeztetné a megfigyelés célját;

i) azoknak a személyeknek az értesítéshez való joga, akik nem voltak a művelet célpontjai, mégis hozzáfértek az adataikhoz; a megfigyelés engedélyezésének lejárta után a hatóságoknak értesíteniük kell azokat a személyeket, akiknek a magánélet tiszteletben tartásához való jogát a kémszoftverek használata súlyosan érintette, de nem voltak a művelet célpontjai; a hatóságoknak értesíteniük kell e személyt arról, hogy adataihoz hozzáfértek, és az értesítésnek tartalmaznia kell a megfigyelés időpontjára és időtartamára, a megfigyelési műveletre kiadott parancsra, a megszerzett adatokra, az adatok felhasználásának módjára és az adatokat felhasználó szereplőkre vonatkozó információkat, valamint az adatok törlésének időpontját; megjegyzi, hogy ezt az értesítést indokolatlan késedelem nélkül kell megtenni, kivéve, ha egy független igazságügyi hatóság engedélyezi az értesítés elhalasztását, amely esetben az azonnali értesítés súlyosan veszélyeztetné a megfigyelés célját;

j) a kémszoftverek használatának hatékony, kötelező és független utólagos felügyelete, amelyhez a felelős szerveknek rendelkezniük kell minden szükséges eszközzel és hatáskörrel az érdemi felügyelet gyakorlásához, és amelyet parlamenti felügyelettel kell párosítani, amelynek tagsága felöleli az összes, megfelelő betekintési engedéllyel rendelkező pártot, amelyek teljes körűen hozzáférnek az annak megállapításához elegendő információkhoz, hogy a megfigyelés jogszerű és arányos volt, és a szükséges infrastruktúra, folyamatok és biztonsági engedélyek kialakításával meg kell valósítani az érzékeny vagy bizalmas információk parlamenti felügyeletét; a nemzetbiztonság fogalmának meghatározásától vagy kijelölésétől függetlenül a nemzeti felügyeleti

szerveknek hatáskörrel kell rendelkezniük a nemzetbiztonság teljes körére;

k) a megfigyeléshez használt kémszoftverek kapcsán elfogadott rendelkezések központi elemévé kell tenni a jogszerű eljárásmód és az igazságszolgáltatási ellenőrzés alapelveit;

l) érdemi jogorvoslat a közvetlen és közvetett célpontok számára, azon személyek számára pedig, akik azt állítják, hogy a megfigyelés hátrányosan érintette őket, egy független szerven keresztül jogorvoslatot kell biztosítani; ezért kéri, hogy vezessék be az állami hatóságok számára előírt értesítési kötelezettséget, beleértve az értesítés megfelelő határidejét is, amely szerint a kézbesítésre a biztonsági fenyegetés elmúltával kerül sor;

m) a jogorvoslatnak mind jogilag, mind ténylegesen hatékonynak kell lennie, továbbá ismertté és hozzáférhetővé kell tenni; hangsúlyozza, hogy ezek a jogorvoslati intézkedések egy független felügyeleti szerv által lefolytatott gyors, alapos és pártatlan vizsgálatot követelnek meg, és ennek a szervnek hozzáféréssel, szakértelemmel és technikai képességekkel kell rendelkeznie az összes releváns adat kezelése érdekében, hogy meg tudja állapítani, hogy a hatóságok által egy adott személyről készített biztonsági értékelés megbízható és arányos-e; azokban az esetekben, ahol megerősítést nyert a visszaélés ténye, a tagállam vonatkozó nemzeti jogának megfelelő büntetőjogi vagy közigazgatási szankciókat kell elfogadni;

n) a technológiai szakértelemhez való ingyenes hozzáférés – a technológiai folyamatok, például a kriminalisztikai elemzések fokozott elérhetősége és megfizethetősége révén való – javulása lehetővé tenné a célszemélyek számára, hogy megalapozottabb ügyeket terjesszenek elő a bíróságon, és a jogi képviselet és az igazságszolgáltatás technológiai kapacitásépítése révén javítaná a célszemélyek képviseletét, továbbá a bíróságok megfelelőbb tanácsokat tudnának adni a célszemélyeknek, jobban tudnák azonosítani a jogsértéseket, valamint megfelelőbben tudnák felügyelni a kémszoftverekkel való visszaélést és elszámoltathatóságot;

o) a védelemhez és a tisztességes eljáráshoz való jog megerősítésével elérhető, hogy a bűncselekményekkel megvádolt személyek megvizsgálhassák az ellenük felhozott bizonyítékok pontosságát, hitelességét, megbízhatóságát és jogszerűségét, és így tiltakozhatnak a nemzetbiztonsági titoktartási szabályok túlzottan általános alkalmazása ellen;

p) a megfigyelés során a hatóságoknak törölniük kell minden adatot, amely nem releváns a jóváhagyott nyomozás szempontjából, és az engedélyezett megfigyelés és a vizsgálat befejezése után a hatóságoknak törölniük kell az adatokat, valamint minden kapcsolódó dokumentumot, például az ezen időszak alatt készült feljegyzéseket; a törlést rögzíteni kell, és ellenőrizhetőnek kell lennie;

q) a kémszoftverek segítségével beszerzett releváns információkhoz csak a jogosult hatóságok kaphatnak hozzáférést, és ők is csak egy konkrét nyomozás kapcsán; ezt a hozzáférést a bírósági eljárás során lefektetett konkrét időintervallumra kell korlátozni;

r) minimumszabályokat kell lefektetni arra vonatkozóan, hogy milyen feltételek mellett használhatók fel a magánszemélyek ellen büntetőeljárások során a kémszoftverek segítségével gyűjtött bizonyítékok; a büntető eljárásjogban teret kell adni annak a

lehetőségnek, hogy a kémszoftverek használata hamis vagy manipulált információkhoz vezet (hasonmássággal való visszaélés);

s) a tagállamoknak értesíteniük kell egymást, ha egy másik tagállam állampolgárait vagy lakosait, illetve egy másik tagállam mobilszámát figyelik;

t) a megfigyelési szoftverben el kell helyezni egy nyomkövetőt, amely alapján a felügyeleti szervek visszaélés gyanúja esetén egyértelműen azonosítani tudják a szoftvert alkalmazó felet; a kémszoftverek alkalmazásához kapcsolódó kötelező aláírásnak tartalmaznia kell az eljáró hatóság egyedi címkéjét, a használt kémszoftver típusát, valamint egy anonimizált ügyszámot;

33. felhívja a tagállamokat, hogy folytassanak konzultációt az érdekelt felekkel, gondoskodjanak a jogalkotási folyamat átláthatóságáról, és a kémszoftverek használatával és értékesítésével foglalkozó új jogszabályok elfogadása során vegyék figyelembe az uniós normákat és biztosítékokat;

34. hangsúlyozza, hogy csak olyan kémszoftverek hozhatók forgalomba a belső piacon, illetve fejleszthetők ki vagy használhatók az Unióban, amelyek úgy vannak kialakítva, hogy lehetővé teszik és megkönnyítik a (29) bekezdés szerinti jogi keretnek megfelelő működést; megerősíti, hogy a kémszoftverek forgalomba hozataláról szóló, az EUMSZ 114. cikkén alapuló „beépített jogállamiságot” előíró rendeletnek magas szintű védelmet kell biztosítania az uniós polgárok számára; indokolatlannak tartja, hogy bár a kettős felhasználású termékekről szóló rendelet 2021 óta védelmet biztosít a nem uniós országok állampolgárai számára az EU-ból származó kémszoftver-exporttal szemben, az uniós polgárok számára nem biztosít ezzel egyenértékű védelmet;

35. úgy véli, hogy az EU-ban működő vállalatoktól csak a lehallgatási és kinyerési technológiát vásárolhatják meg a tagállamok, nem pedig a „a feltörést, mint szolgáltatást”, amely magában foglalja a megfigyelési technológia technikai, operatív és módszertani támogatását, és lehetővé teszi a szolgáltató számára az aránytalan mennyiségű adathoz való hozzáférést, ami összeegyeztethetetlen az arányosság, a szükségesség, a legitimitás, a jogszerűség és a megfelelőség elvével; kéri a Bizottságot, hogy ezzel kapcsolatban terjesszen elő jogalkotási javaslatot;

36. hangsúlyozza, hogy a kémszoftverek csak úgy hozhatók forgalomba, hogy azokat a hatóságok egy zárt listája számára értékesítik és csak ők használhatják, amely hatóságok utasításai között szerepel azon bűncselekmények kivizsgálása vagy a nemzetbiztonsági érdekek védelme, amelyek esetében a kémszoftverek használata engedélyezett; úgy véli, hogy a hírszerzési ügynökségeknek csak akkor szabad kémszoftvereket használniuk, ha az Alapjogi Ügynökség valamennyi ajánlását[31] végrehajtották;

37. rámutat arra a kötelezettségre, hogy a kémszoftverek olyan változatát kell használni, amely úgy van tervezve, hogy minimalizálja az eszközön tárolt összes adathoz való hozzáférést, és hogy azokat úgy kellene tervezni, hogy az adatokhoz való hozzáférést az engedélyezett vizsgálat céljához feltétlenül szükséges minimumra korlátozzák;

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

38. úgy véli, hogy ha egy tagállam kémszoftvert vásárolt, a beszerzésnek ellenőrizhetőnek kell lennie, amelyet egy független, pártatlan, megfelelő engedéllyel rendelkező ellenőrző szervnek végez el;

39. hangsúlyozza, hogy a belső piacon kémszoftvereket forgalomba hozó valamennyi szervezetnek meg kell felelnie a kellő gondosságra vonatkozó szigorú követelményeknek, és a közbeszerzési eljárásban beszállítóként pályázó vállalatoknak átvilágítási folyamaton kell átesniük, amely magában foglalja a vállalatnak a szoftvereivel elkövetett emberi jogi jogsértésekre adott válaszát, valamint azt, hogy a technológia nem demokratikus és visszaélésszerű megfigyelési gyakorlatok során gyűjtött adatokra támaszkodik-e; hangsúlyozza, hogy az illetékes nemzeti felügyeleti hatóságoknak évente jelentést kell tenniük a Bizottságnak a megfelelésről;

40. hangsúlyozza, hogy az állami szereplőknek felügyeleti technológiákat vagy szolgáltatásokat kínáló vállalatoknak közölniük kell az illetékes nemzeti felügyeleti hatóságokkal a kiviteli engedélyek jellegét;

41. rámutat, hogy a tagállamoknak meg kell állapítaniuk egy olyan türelmi időszakot, ameddig a kormányzati szervek vagy ügynökségek egykori alkalmazottai egy ideig nem dolgozhatnak kémszoftverrel foglalkozó vállalatoknak;

A nemzetbiztonság korlátozásának szükségessége

42. aggodalmát fejezi ki amiatt, hogy a „nemzetbiztonságra” való hivatkozást indokként használják a kémszoftverek telepítésére és használatára, amivel teljes titoktartást és az elszámoltathatóság hiányát érik el; üdvözli a Bizottság az EIB ítélkezési gyakorlatának[32] megfelelő nyilatkozatát, miszerint a nemzetbiztonságra való puszta hivatkozás nem értelmezhető úgy, mint az uniós jogszabályok alóli korlátlan kivétel és egyértelmű indok szükséges hozzá, és felszólítja a Bizottságot, hogy visszaélésre utaló jelek esetén kövesse ezt a nyilatkozatot; úgy véli, hogy egy olyan demokratikus, átlátható társadalomban, amely tiszteletben tartja a jogállamiságot, a nemzetbiztonság nevében történő ilyen korlátozások inkább kivételnek, mintsem szabálynak minősülnek;

43. úgy véli, hogy különbséget kell tenni a korlátozottabb hatáskörű nemzetbiztonság és a belső biztonság fogalma között, amely utóbbi tágabb hatókörrel rendelkezik, és magában foglalja a polgárokat fenyegető kockázatok megelőzését és különösen a büntetőjog érvényesítését;

44. sajnálja az abból fakadó nehézségeket, hogy a nemzetbiztonság fogalmának nincs közös jogi meghatározása, amely lefekteti a nemzetbiztonsági kérdésekben alkalmazandó jogrend meghatározására szolgáló kritériumokat, és egyértelműen kijelöli azt a területet,

[32] A C-623/17. sz., Privacy International kontra Secretary of State for Foreign and Commonwealth Affairs és társai ügyben 2020. október 6-án hozott ítélet (EU:C:2020:790) 44. pontja, valamint a C-511/18., C-512/18. és C-520/18. sz., La Quadrature du Net és társai kontra Premier ministre és társai egyesített ügyekben 2020. október 6-án hozott ítélet (EU:C:2020:791) 99. pontja: „noha alapvető biztonsági érdekeik meghatározása, valamint a külső és belső biztonságukat szolgáló, megfelelő intézkedések meghozatala a tagállamok feladatkörébe tartozik, önmagában az a tény, hogy egy nemzeti intézkedést a nemzetbiztonság védelme érdekében fogadtak el, még nem eredményezi az uniós jog alkalmazhatatlanságát és nem mentesíti a tagállamokat az uniós jog kellő tiszteletben tartása alól”;

ahol egy ilyen különleges rendszer alkalmazható;

45. úgy véli, hogy a kémszoftverek használata az alapvető jogok korlátozásának minősül; úgy véli továbbá, hogy amennyiben egy fogalmat olyan jogi összefüggésben használnak, amely jogok átruházását és kötelezettségek előírását (és különösen az egyének alapvető jogainak korlátozását) vonja maga után, a fogalomnak világosnak és előre értelmezhetőnek kell lennie minden érintett személy számára; emlékeztet arra, hogy az Alapjogi Charta előírja, hogy az alapvető jogok az 52. cikk (1) bekezdése szerint csak törvény által korlátozhatók; ezért szükségesnek tartja a „nemzetbiztonság” fogalmának egyértelmű meghatározását; hangsúlyozza, hogy a pontos meghatározástól függetlenül a nemzetbiztonság területét teljes egészében független, kötelező erejű és hatékony felügyeletnek kell alávetni;

46. hangsúlyozza, hogy ha a hatóságok nemzetbiztonsági okokra hivatkoznak a kémszoftverek használatának indokolásaként, akkor a (29) bekezdésben meghatározott kereten felül bizonyítaniuk kell az uniós jognak való megfelelést, beleértve az arányosság, a szükségesség, a jogszerűség, a megalapozottság és a megfelelőség elvének betartását; kiemeli, hogy az indokolásnak könnyen hozzáférhetőnek kell lennie, és értékelés céljából a nemzeti ellenőrző szervek rendelkezésére kell állnia;

47. e tekintetben megismétli, hogy valamennyi tagállam aláírta a 108+ egyezményt, amely szabályokat és kötelezettségeket állapít meg az egyének védelmére vonatkozóan a személyes adatok kezelése tekintetében, beleértve a nemzetbiztonsági célú adatkezelést is; rámutat, hogy a 108+ egyezmény kötelező erejű európai keret, amely a hírszerzési és biztonsági szolgálatok általi adatfeldolgozással foglalkozik; sürgeti az összes tagállamot, hogy haladéktalanul ratifikálják ezt az egyezményt, és a nemzeti jogban már most hajtsák végre az abban foglalt szabályokat, illetve nemzetbiztonsági kérdésekben ennek megfelelően járjanak el;

48. hangsúlyozza, hogy az egyezmény korlátozott számú rendelkezése alóli kivételek és az azokkal kapcsolatos korlátozások csak akkor megengedettek, ha összhangban vannak az egyezmény 11. cikkében említett követelményekkel, ami azt jelenti, hogy a 108+ egyezmény végrehajtása során minden egyes konkrét kivételről és korlátozásról jogszabályban kell rendelkezni, tiszteletben kell tartani az alapvető jogok és szabadságok lényegét, és igazolni kell, hogy azok „a demokratikus társadalomban szükséges és arányos intézkedésnek minősülnek” a 11. cikkben[33] felsorolt jogos okok valamelyikére tekintettel, és az ilyen kivételek és korlátozások nem befolyásolhatják az érintett fél nemzeti jogszabályai szerinti független és hatékony felülvizsgálatot és felügyeletet;

49. megjegyzi továbbá, hogy a 108+ egyezmény hangsúlyozza, hogy a felügyelet „magában foglalja a vizsgálati és beavatkozási hatáskört”; úgy véli, hogy a hatékony felülvizsgálat és felügyelet kötelező erejű hatásköröket feltételez azokban az esetekben, ahol az

[33] Ezt az értékelést az EJEB ítélkezési gyakorlata írja elő, amely a bizonyítási terhet az államra/jogalkotóra hárítja. Az EJEB vonatkozó ítélkezési gyakorlata többek között a következő ítéleteket foglalja magában: Roman Zakharov kontra Oroszország (47143/06. sz. kérelem), 2015. december 4.; Szabó és Vissy kontra Magyarország (37138/14. sz. kérelem), 2016. január 12.; Big Brother Watch és mások kontra Egyesült Királyság (58170/13., 62322/14. és 24969/15. sz. kérelem), 2021. május 25., valamint Centrum för rättvisa kontra Svédország (35252/08. sz. kérelem), 2021. május 25.

alapvető jogokra gyakorolt hatás a legnagyobb, különösen a személyes adatok feldolgozásának hozzáférési, elemzési és tárolási szakaszában;

50. úgy véli, hogy a nemzetbiztonság területén működő felügyeleti szervek kötelező erejű hatásköreinek hiánya összeegyeztethetetlen a 108+ egyezményben meghatározott kritériummal, amely szerint ez „szükséges és arányos intézkedésnek minősül egy demokratikus társadalomban”;

51. rámutat arra, hogy a 108+ egyezmény a 15. cikk tekintetében igen korlátozott számú kivételt megenged, de nem tesz lehetővé ilyen kivételt a (2) bekezdés [figyelemfelhívással kapcsolatos kötelezettségek], a (3) bekezdés [konzultáció a jogalkotási és közigazgatási intézkedésekről], a (4) bekezdés [az egyének kérelmei és panaszai], az (5) bekezdés [függetlenség és pártatlanság], a (6) bekezdés [a feladatok hatékony ellátásához szükséges erőforrások], a (7) bekezdés [időszakos jelentéstétel], a (8) bekezdés [bizalmasság], a (9) bekezdés [fellebbezési lehetőség] és a (10) bekezdés [az igazságszolgáltatási minőségükben eljáró szervek feletti hatáskör hiánya] tekintetében;

A hatályos jogszabályok végrehajtásának és érvényesítésének javítása

52. hangsúlyozza a nemzeti jogi keretek hiányosságait és azt, hogy e hiányosságok ellensúlyozása érdekében javítani kell a hatályos uniós jogszabályok végrehajtását; a következő uniós jogszabályokat jelöli meg, amelyek relevánsnak, de végrehajtásuk és/vagy érvényesítésük túl gyakran nem megfelelő: a pénzmosás elleni irányelv, a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv, a közbeszerzési szabályok, a kettős felhasználású termékekről szóló rendelet, az ítélkezési gyakorlat (a megfigyeléssel és a nemzetbiztonsággal kapcsolatos határozatok) és a visszaéléseket bejelentő személyek védelméről szóló irányelv; felszólítja a Bizottságot, hogy vizsgálja meg a végrehajtás és az érvényesítés hiányosságait, tegyen jelentést azokról, és legkésőbb 2023 augusztusáig terjesszen elő ütemtervet ezek kijavítására;

53. döntős fontosságúnak tartja az adatvédelemre vonatkozó uniós jogi keret – különösen a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv, az általános adatvédelmi rendelet és az elektronikus hírközlési adatvédelmi irányelv – megfelelő végrehajtását és szigorú érvényesítését; ugyanilyen fontosnak tartja az EUB vonatkozó ítéleteinek teljes körű végrehajtását, ami több tagállamban még mindig nem történt meg; emlékeztet arra, hogy a Bizottságnak központi szerepe van az uniós jog érvényesítésében és Unió-szerte egységes alkalmazásának biztosításában, és tartós meg nem felelés esetén minden rendelkezésre álló eszközt – többek között a kötelezettségszegési eljárásokat is – igénybe kell vennie;

54. felhív arra, hogy a Wassenaari Megállapodás váljon valamennyi résztvevőjére nézve kötelező érvényű megállapodássá, azzal a céllal, hogy nemzetközi szerződéssé alakítsák;

55. felszólítja Ciprust és Izraelt, hogy váljanak a Wassenaari Megállapodás részes államaivá; emlékezteti a tagállamokat, hogy minden erőfeszítést meg kell tenni annak érdekében, hogy Ciprus és Izrael csatlakozhasson a Wassenaari Megállapodáshoz;

56. hangsúlyozza, hogy a Wassenaari Megállapodásnak olyan emberi jogi keretet kell

tartalmaznia, amely kiterjed a kémszoftver-technológiák engedélyezésére és amelynek része a kémszoftver-technológiákat gyártó vállalatok megfelelésének értékelése és felülvizsgálata, továbbá hogy a résztvevőknek meg kell tiltaniuk a megfigyelési technológiák vásárlását olyan államoktól, amelyek nem részesei a Megállapodásnak;

57. hangsúlyozza, hogy a kémszoftvereket érintő leleplezések fényében a Bizottságnak és a tagállamoknak alaposan meg kell vizsgálnia a kémszoftverek használatára vonatkozóan a kettős felhasználású termékekről szóló rendelet alapján kiadott exportengedélyeket, és a Bizottságnak ezen értékelés eredményeit meg kell osztania a Parlamenttel;

58. kiemeli a kémszoftverexport nyomon követhetőségének és elszámoltathatóságának szükségességét, és emlékeztet arra, hogy biztosítani kell, hogy az uniós vállalatok csak olyan kémszoftvereket exportálhassanak, amelyek megfelelő nyomonkövethetőségi tulajdonságokkal rendelkeznek, hogy a felelősség mindig megállapítható legyen;

59. hangsúlyozza, hogy a Bizottságnak rendszeresen ellenőriznie kell és megfelelően végre kell hajtania a kettős felhasználású termékekről szóló átdolgozott rendeletet annak elkerülése érdekében, hogy a szereplők az Unióban a legkedvezőbb exportrendszert válasszák ki, ahogyan az jelenleg Bulgáriában és Cipruson történik, és hogy a Bizottságnak megfelelő forrásokkal kell rendelkeznie ehhez a feladathoz;

60. felhívja a Bizottságot, hogy biztosítson elegendő személyzeti kapacitást a kettős felhasználású termékekről szóló rendelet felügyeletéért és végrehajtásáért felelős egységek számára;

61. felszólít a kettős felhasználású termékekről szóló rendelet módosítására, hogy a 15. cikkben pontosításra kerüljön, hogy a kettős felhasználású termékekre vonatkozó exportengedély nem adható ki, ha a termékeket belső elnyomással és/vagy az emberi jogok és a nemzetközi humanitárius jog súlyos megsértésével összefüggő felhasználásra szánják vagy szánhatják; felszólít egy teljes körű emberi jogi ellenőrzés és átvilágítás végrehajtására az engedélyezési eljárás során, valamint további javulást kér például az emberi jogi visszaélések áldozatai számára jogorvoslat biztosítása és az elvégzett átvilágításra vonatkozó átlátható jelentéstétel terén;

62. kéri a kettős felhasználású termékekről szóló rendelet módosítását annak biztosítása érdekében, hogy a tranzitot megtiltsák azokban az esetekben, ha a termékeket belső elnyomásra és/vagy az emberi jogok és a nemzetközi humanitárius jog súlyos megsértésére szánják vagy szánhatják;

63. hangsúlyozza, hogy a kettős felhasználású termékekről szóló rendelet jövőbeli módosítása során a kettős felhasználású termékekre vonatkozó exportengedélyek jóváhagyásáért és elutasításáért felelős kijelölt nemzeti hatóságoknak részletes jelentést kell készíteniük, amely információkat tartalmaz a szóban forgó kettős felhasználású termékekről; a kérelmezett engedélyek számáról, az exportáló ország nevéről, az exportáló vállalat leírásáról és arról hogy ez a vállalat leányvállalat-e; a végfelhasználó és a rendeltetési hely leírásáról; az exportengedély értékéről; valamint az exportengedély megadásának vagy megtagadásának okáról; hangsúlyozza, hogy ezeket a jelentéseket negyedévente nyilvánosságra kell hozni; felszólít arra, hogy a parlamenti felügyelet céljából állítsanak fel egy külön erre a célra létrehozott állandó parlamenti bizottságot, amelynek a Bizottság hozzáférést ad a minősített információkhoz;

64. hangsúlyozza, hogy a kettős felhasználású termékekről szóló rendelet jövőbeni módosítása során meg kell szüntetni a Bizottsággal szembeni információszolgáltatási kötelezettség alól az üzleti adatok bizalmas jellegére, védelmi és külpolitikai vagy nemzetbiztonsági okokra hivatkozva biztosított kivételt; ehelyett úgy véli, hogy annak érdekében, hogy az érzékeny információk ne váljanak nem uniós országok számára hozzáférhetővé, a Bizottság dönthet úgy, hogy éves jelentésében bizonyos információkat minősített információként kezel;

65. hangsúlyozza, hogy a kettős felhasználású termékekről szóló rendelet átdolgozásában a kibertér-megfigyelési termékek fogalommeghatározása nem értelmezhető leszűkítően, hanem annak minden technológiát magában kell foglalnia ezen a területen, mint amilyenek például a mobil telekommunikációs szolgáltatások lehallgatására vagy zavarására szolgáló berendezések, a behatoló szoftverek, az IP-hálózati közléseket megfigyelő rendszerek vagy berendezések, a kifejezetten a bűnüldöző szervek által végzett megfigyelésre vagy elemzésre tervezett vagy módosított szoftverek, a lézeres akusztikai érzékelőberendezések, az olyan kriminalisztikai eszközök, amelyek nyers adatokat nyernek ki egy számítástechnikai vagy kommunikációs eszközből, és kijátsszák az eszköz általi „hitelesítést” vagy engedély-ellenőrzést, az olyan elektronikus rendszerek vagy berendezések, amelyeket az elektromágneses spektrum katonai hírszerzési vagy biztonsági célú megfigyelésére és nyomon követésére terveztek, valamint a megfigyelés végzésére alkalmas pilóta nélküli légi járművek;

66. olyan további európai jogszabályokat kér, amelyek megkövetelik a megfigyelési technológiákat gyártó és/vagy exportáló vállalati szereplőktől, hogy az üzleti vállalkozások emberi jogi felelősségére vonatkozó ENSZ-irányelvekkel összhangban emberi jogi és átvilágítási keretrendszereket vezessenek be;

Nemzetközi együttműködés a polgárok védelme érdekében

67. felszólít egy közös EU–USA kémprogram-stratégiára, amely magában foglalja azon kémprogram-értékesítők közös fehérlistáját és/vagy feketelistáját, amelyek eszközeivel rossz emberi jogi teljesítménnyel rendelkező külföldi kormányok részéről visszaéltek, vagy fennáll a visszaélés veszélye a tekintetben, hogy eszközeikkel rosszindulatúan kormányzati tisztviselőket, újságírókat és a civil társadalmat vesznek célba, amelyek az Unió biztonság- és külpolitikája ellen tevékenykednek, vagy amelyek nem rendelkeznek felhatalmazással a hatóságok részére történő értékesítésre, valamint az értékesítők valamely listára való felvételének közös kritériumait, az ágazatról szóló közös EU–USA jelentéstételre vonatkozó megállapodásokat, a közös ellenőrzést, az értékesítőkre vonatkozó közös átvilágítási kötelezettségeket, valamint a kémprogramok nem állami szereplők részére történő értékesítésének bűncselekménnyé nyilvánítását;

68. felszólítja az EU–USA Kereskedelmi és Technológiai Tanácsot, hogy a közös EU–USA stratégia és előírások kidolgozása érdekében folytasson széles körű és nyílt konzultációt a civil társadalommal, többek között a közös fehérlistáról és/vagy feketelistáról;

69. felszólít arra, hogy kezdjenek tárgyalásokat más országokkal – különösen Izraellel – a kémszoftverek forgalmazására és az exportengedélyekre vonatkozó keret létrehozása érdekében, beleértve az átláthatóságra vonatkozó szabályokat, a jogosult országok listáját és a kellő gondosságra vonatkozó rendelkezéseket;

70. megjegyzi, hogy uniós szinten nem tettek megfelelő lépéseket a kémszoftverek behozatala és az exportszabályok végrehajtása tekintetében az USA-hoz képest, ahol az NSO-t gyorsan feketelistára vették, és ahol az Egyesült Államok elnöke elnöki rendeletet írt alá, amely kimondja, hogy az NSO nem használhat operatívan olyan kereskedelmi kémszoftvereket, amelyek jelentős kémelhárítási vagy biztonsági kockázatot jelentenek az Egyesült Államok kormánya számára, vagy amelyek külföldi kormány vagy külföldi személy általi nem megfelelő használata jelentős kockázatot jelent;

71. megállapítja, hogy az uniós exportszabályokat és azok érvényesítését meg kell erősíteni az emberi jogok harmadik országokban történő védelme érdekében, továbbá hogy biztosítani kell a rendelkezések hatékony végrehajtásához szükséges eszközöket; emlékeztet, hogy az EU-nak törekednie kell arra, hogy egyesítse erőit az USA-val és más szövetségesekkel a kémszoftverek kereskedelmének szabályozása és az együttes piaci erejüknek a változás kikényszerítésére való felhasználása érdekében, valamint szilárd normákat kell meghatároznia a megfigyelési technológia alkalmazásával kapcsolatos átláthatóságra, nyomonkövethetőségre és elszámoltathatóságra vonatkozóan, aminek egy ENSZ-szintű kezdeményezésben kell kiteljesednie;

Nulladik napi sebezhetőségek

72. felszólít a sebezhetőségek felfedezésének, megosztásának, javításának és kiaknázásának, valamint a feltárási eljárásoknak a szabályozására, ezáltal kiteljesítve az (EU) 2022/2555 irányelv[34] (NIS 2 irányelv) és a kiberrezilienciáról szóló jogszabályra irányuló javaslat[35] által biztosított alapot;

73. úgy véli, hogy a kutatók számára lehetővé kell tenni, hogy polgári jogi és büntetőjogi felelősségre vonás nélkül kutathassák a sebezhetőségeket, és megosszák eredményeiket, többek között a kiberbűnözésről szóló irányelv és a szerzői jogról szóló irányelv alapján;

74. felszólítja a főbb iparági szereplőket, hogy teremtsenek ösztönzőket a kutatók számára a sebezhetőségek kutatásában való részvételre, mégpedig azzal, hogy befektetnek a sebezhetőségek kezelésére vonatkozó tervekbe, valamint az iparágon belüli és a civil társadalommal közös feltárási gyakorlatokba, továbbá pénzjutalommal ösztönzött hibakeresési programokat indítanak;

75. felhívja a Bizottságot, hogy növelje a pénzjutalommal ösztönzött hibakeresési programok és a biztonsági sebezhetőségek keresésére és javítására irányuló egyéb projektek tekintetében általa nyújtott támogatást és finanszírozást, és vezessen be összehangolt megközelítést a sebezhetőségek tagállamok körében való kötelező feltárására vonatkozóan;

---

[34] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről, a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (OJ L 333., 2022.12.27., 80. o.).

[35] A digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről és az (EU) 2019/1020 rendelet módosításáról szóló európai parlamenti és tanácsi rendeletre irányuló, 2022. szeptember 15-i javaslat (COM(2022)0454).

76. felszólít a valamely rendszerben talált sebezhetőségek értékesítésének tiltására abban az esetben, ha az értékesítés célja nem a rendszer biztonságának megerősítése, valamint kéri, hogy a sebezhetőségi kutatások eredményeit olyan összehangolt és felelősségteljes módon tegyék közzé, amely előmozdítja a közbiztonságot, és minimálisra csökkenti a sebezhetőség kihasználásának kockázatát;

77. felszólítja az állami és a magánszervezeteket, hogy hozzanak létre egy nyilvánosan elérhető kapcsolattartó pontot, ahol a sebezhetőségeket összehangoltan és felelős módon lehet bejelenteni, és kéri, hogy azok a szervezetek, amelyek információt kapnak a rendszerükben lévő sebezhetőségekről, azonnal tegyenek lépéseket a javítás érdekében; úgy véli, hogy ha rendelkezésre áll javítás, a szervezeteket kötelezni kell arra, hogy rendelkezzenek a gyors és garantált alkalmazás biztosításához szükséges megfelelő eszközökkel, ami egy összehangolt és elszámoltatható feltárási folyamat része lenne;

78. úgy véli, hogy a tagállamoknak elegendő pénzügyi, technikai és emberi erőforrást kell elkülöníteniük a biztonsági kutatásra és a sebezhetőségek javítására;

79. felhívja a tagállamokat, hogy jogszabályban dolgozzanak ki a sebezhetőségekre vonatkozó méltányossági eljárásokat, amelyek meghatározzák, hogy alapesetben a sebezhetőségeket fel kell tárni, és azokat nem szabad kihasználni, és az ettől való eltérésre vonatkozó minden döntésnek kivételt kell képeznie, és azt a szükségesség és arányosság követelményei alapján kell értékelni – beleértve annak mérlegelését is, hogy a sebezhetőség által érintett infrastruktúrát a lakosság nagy része használja-e –, és független felügyeleti szerv szigorú felügyelete, valamint átlátható eljárások és határozatok hatálya alá kell vonni;

Távközlési hálózatok

80. hangsúlyozza, hogy vissza kell vonni minden olyan szolgáltató engedélyét, amelyről megállapítást nyert, hogy a hálózat minden generációján (jelenleg 2G-től 5G-ig) elősegíti a nemzeti és/vagy nemzetközi mobil jelzőinfrastruktúrához való jogellenes hozzáférést;

81. hangsúlyozza, hogy a tiltott tevékenységek leplezésének megnehezítése érdekében jobban kellene szabályozni azokat az eljárásokat, amelyek révén rosszindulatú szereplők a világ minden táján új telefonszámokat hozhatnak létre;

82. hangsúlyozza, hogy a távközlési szolgáltatóknak biztosítaniuk kell, hogy képesek legyenek észlelni a harmadik felek által a működési helyük szerinti tagállamban kötött kereskedelmi vagy egyéb megállapodások révén megszerzett, a jelzőinfrastruktúrákhoz való hozzáféréssel, az ellenőrzéssel vagy a tényleges végfelhasználással való esetleges visszaéléseket;

83. felhívja a tagállamokat annak biztosítására, hogy az illetékes nemzeti hatóságok a második kiberbiztonsági irányelv rendelkezéseivel összhangban értékeljék a távközlési szolgáltatók jogosulatlan behatolásokkal szembeni ellenálló képességének szintjét;

84. felszólítja a távközlési szolgáltatókat, hogy tegyenek határozott és bizonyítható intézkedéseket a valamely hálózati elem által indított távközlési forgalom engedély nélküli emulálásának olyan különböző formái ellen, amelyek célja a legitim

felhasználónak szánt adatokhoz vagy szolgáltatásokhoz való hozzáférés, valamint azon egyéb tevékenységek ellen, amelyek a mobilhálózati elemek és infrastruktúra normál működésének rosszindulatú szereplők – beleértve az állami szintű szereplőket és a bűnözői csoportokat is – által megfigyelési céllal történő manipulálásával járnak;

85. felhívja a tagállamokat, hogy tegyenek lépéseket annak biztosítása érdekében, hogy a stratégiai infrastruktúrák ne kerülhessenek az alapvető jogokat tiszteletben nem tartó nem uniós állami szereplők irányítása alá vagy e szereplők ne lehessenek ilyen infrastruktúra végfelhasználói, illetve ne befolyásolhassák az Unión belüli stratégiai infrastruktúrával – ideértve a távközlési infrastruktúrát is – kapcsolatos döntéseket;

86. felhívja az összes tagállamot, hogy a magánélet tiszteletben tartásához való jog megsértése, az adatszivárgás és az engedély nélküli behatolással szembeni védelem hiányosságainak kezelése céljából, a polgárok alapvető jogainak védelme érdekében kezeljék prioritásként a kritikus infrastruktúrák – például a nemzeti távközlési rendszerek – védelmét célzó nagyobb beruházásokat;

87. felhívja az illetékes nemzeti hatóságokat, hogy aktívan mozdítsák elő a szolgáltatók képességeinek és reagálási képességeinek megerősítését az illegálisan célba vett személyek azonosításának, az értesítéseknek és az események bejelentésének jobb támogatása érdekében, hogy folyamatosan, mérhetően bizonyosságot nyújtsanak és mérsékeljék a biztonsági hiányosságok nem uniós és hazai rosszindulatú szereplők általi kihasználását;

Elektronikus adatvédelem

88. felszólít az elektronikus hírközlési adatvédelmi rendelet gyors, olyan módon történő elfogadására, amely teljes mértékben tükrözi a nemzetbiztonsági korlátozásokra vonatkozó ítélkezési gyakorlatot és a megfigyelési technológiákkal való visszaélések megelőzésének szükségességét, amely erősíti a magánélethez való alapvető jogot, valamint erős garanciákról és hatékony végrehajtásról rendelkezik; rámutat arra, hogy a jogszerű lehallgatás hatóköre nem terjedhet túl az elektronikus hírközlési adatvédelemről szóló 2002/58/EK irányelven;

89 felszólít minden elektronikus hírközlés, tartalom és metaadat védelmére a személyes adatokkal és a magáncélú kommunikációval való, magánvállalatok és kormányzati hatóságok által elkövetett visszaélésekkel szemben; rámutat arra, hogy nem szabad gyengíteni a beépített biztonságot biztosító digitális eszközöket, például a végpontok közötti titkosítást;

90. felhívja a Bizottságot, hogy EU-szerte értékelje az elektronikus hírközlési adatvédelmi irányelv tagállamok általi végrehajtását, és jogsértés esetén indítson kötelezettségszegési eljárást;

Az Europol szerepe

91. megjegyzi, hogy az Europol 2023 áprilisában levelet küldött a PEGA bizottság elnökének, amelyben arról tájékoztatja a Bizottságot, hogy az Europol felvette a kapcsolatot Görögországgal, Magyarországgal, Bulgáriával, Spanyolországgal és Lengyelországgal annak megállapítása érdekében, hogy folyamatban vagy tervben van-

e bármely olyan bűnügyi nyomozás vagy a nemzeti jog alkalmazandó rendelkezései szerinti más vizsgálat, amelyet az Europol támogathat; hangsúlyozza, hogy a tagállamoknak nyújtott segítség nem jelenti bűnügyi nyomozás 6. cikk szerinti megindítását, lefolytatását vagy koordinálását;

92. felhívja az Europolt, hogy teljes mértékben használja ki az (EU) 2022/991 rendelet 6. cikkének (1a) bekezdése alapján újonnan szerzett hatásköreit, amelyek lehetővé teszik számára, hogy adott esetben az érintett tagállamok illetékes hatóságainak javaslatot tegyen nyomozás megindítására, lefolytatására vagy koordinálására; rámutat arra, hogy a 6. cikk értelmében a tagállamokra tartozik az ilyen javaslat elutasítása;

93. felszólítja az összes tagállamot, hogy egyértelműen kötelezzék el magukat az Európai Parlament és a Tanács felé amellett, hogy bevonják az Europolt a kémszoftverek állítólagos jogellenes használatával kapcsolatos nemzeti szintű nyomozásokba, különösen ha az (EU) 2022/991 rendelet 6. cikkének (1a) bekezdése szerinti javaslat megtételére került sor;

94. felszólítja a tagállamokat, hogy hozzanak létre egy nyilvántartást az Europolon belül a kémszoftverek felhasználásával végzett nemzeti bűnüldözési műveletekről, amelyben minden műveletet egy kóddal kell azonosítani, és hogy a kémszoftverek kormányok általi felhasználása szerepeljen az Europol által az internetes szervezett bűnözés általi fenyegetettségről készített éves értékelő jelentésben;

95. úgy véli, hogy el kell gondolkodni az Europol abban az esetben játszott szerepéről, ha a nemzeti hatóságok elmulasztják vagy megtagadják a nyomozást, és egyértelmű fenyegetést jelentenek az EU érdekeire és biztonságára nézve;

Uniós fejlesztési politikák

96. felszólítja a Bizottságot és az EKSZ-t, hogy vezessenek be szigorúbb ellenőrzési mechanizmusokat annak biztosítása érdekében, hogy az uniós fejlesztési támogatások – beleértve a megfigyelési technológia adományozását és a megfigyelési szoftverek alkalmazásával kapcsolatos képzést – ne finanszírozzanak vagy mozdítsanak elő olyan eszközöket és tevékenységeket, amelyek sérthetik a demokrácia, a felelősségteljes kormányzás, a jogállamiság és az emberi jogok tiszteletben tartásának elveit, vagy veszélyt jelentenek a nemzetközi biztonságra vagy az Unió és tagállamai alapvető biztonságára; megjegyzi, hogy az uniós jognak, különösen a költségvetési rendeletnek való megfelelés Bizottság által elvégzett értékelésének konkrét ellenőrzési kritériumokat és végrehajtási mechanizmusokat kell tartalmaznia az ilyen visszaélések megelőzése érdekében, beleértve konkrét projektek lehetséges átmeneti felfüggesztését, ha ezen elvek megsértésére derül fény;

97. felhívja a Bizottságot és az EKSZ-t, hogy [a PEGA ajánlásainak közzétételét követő] egyéves időtartamon belül minden emberi jogi és alapjogi hatásvizsgálatba foglaljanak bele a megfigyeléssel való lehetséges visszaélések nyomon követésére irányuló eljárást, amely teljes mértékben figyelembe veszi az Alapjogi Charta 51. cikkét; hangsúlyozza, hogy ezt az eljárást be kell mutatni a Parlamentnek és a Tanácsnak, és hogy a nem uniós országoknak nyújtott bármely támogatás előtt el kell végezni ezt a hatásvizsgálatot;

98. felszólítja az EKSZ-t, hogy tegyen jelentést az emberijog-védők ellen elkövetett

kémszoftveres visszaélésekről az emberi jogok és a demokrácia helyzetéről szóló éves uniós jelentésben;

Uniós pénzügyi szabályozás

99. hangsúlyozza, hogy a pénzügyi szektorban erősíteni kell az emberi jogok tiszteletben tartását; hangsúlyozza, hogy az üzleti vállalkozások emberi jogi felelősségére vonatkozó ENSZ-irányelvek 10+ ajánlását át kell ültetni az uniós jogba, és hogy teljes mértékben alkalmazni kell a pénzügyi szektorra az átvilágításról szóló irányelvet, hogy a pénzügyi szektorban biztosított legyen a demokrácia, az emberi jogok és a jogállamiság tiszteletben tartása;

100. aggodalmát fejezi ki a pénzügyi rendszerek pénzmosás vagy terrorizmusfinanszírozás céljára való felhasználásának megelőzéséről szóló (EU) 2018/843 irányelvvel[36] kapcsolatos EUB-határozat következményei miatt, amely érvénytelennek minősítette a gazdasági társaságok és más jogi entitások tényleges tulajdonosaira vonatkozó, a tényleges tulajdonosok nemzeti és nyilvánosan hozzáférhető nyilvántartásában szereplő információkat[37]; hangsúlyozza, hogy az EUB határozatát figyelembe véve a jövőbeli irányelvnek a lehető legnagyobb mértékben lehetővé kell tennie a nyilvánosság általi hozzáférhetőséget, hogy nehezebbé váljon a kémszoftverek vásárlásának vagy értékesítésének közvetítőkön és közvetítő vállalatokon keresztül történő elrejtése;

A Parlament állásfoglalásainak nyomon követése

101. felhív az egyesült államokbeli NSA megfigyelési programjáról, a különféle tagállamokban megfigyelést végző szervekről és az uniós polgárok alapvető jogaira gyakorolt hatásukról, valamint a transzatlanti bel- és igazságügyi együttműködésről szóló, 2014. március 12-i parlamenti állásfoglalás nyomon követésére; hangsúlyozza, hogy az abban foglalt ajánlásokat sürgősen végre kell hajtani;

102. hangsúlyozza, hogy jóllehet a hírszerző szolgálatok tevékenységének felügyeletét egyrészről a demokratikus legitimitásra (erős jogi keret, előzetes engedélyezés és utólagos ellenőrzés), másrészről pedig megfelelő műszaki képességekre és szakértelemre kell alapozni, az Unióban és az Egyesült Államokban jelenleg működő felügyeleti szervek többsége esetében kirívó e két tényező – és különösen a műszaki képességek – hiánya;

103. felkéri a nemzeti parlamenteket – amint azt az Echelon rendszer esetében is tette –, hogy amennyiben azt eddig elmulasztották, vezessék be a hírszerző tevékenységek parlamenti képviselők vagy vizsgálati hatáskörökkel felruházott szakértői testületek által megvalósított érdemi felügyeletét; felszólítja a nemzeti parlamenteket annak biztosítására, hogy az ilyen felügyeleti bizottságok/szervek elegendő erőforrással, műszaki szakértelemmel és jogi eszközzel rendelkezzenek a hírszerző szolgálatok hatékony ellenőrzéséhez, ideértve a helyszíni látogatásokhoz való jogot is;

104. kéri egy olyan magas szintű munkacsoport felállítását, amely átlátható módon és a parlamentekkel együttműködve ajánlásokat tenne és további lépéseket javasolna a

[36] 2022. július 12-i Profit Europe ítélet, C-37/20 és C-398/20, EU:C:2018:912.
[37] EUB. 188/22. sz. sajtóközlemény. A Bíróság ítélete a C-37/20. és a C-601/20. sz. egyesített ügyekben.

hírszerző szolgálatok feletti demokratikus felügyelet – többek között a parlamenti felügyelet – megerősítése, valamint különösen annak határon átnyúló dimenziója tekintetében az EU-n belüli fokozott felügyeleti együttműködés érdekében;

105. úgy véli, hogy e magas szintű munkacsoportnak:

a) európai minimumszabályokat vagy iránymutatásokat kell meghatároznia a hírszerző szolgálatok (előzetes és utólagos) felügyeletére vonatkozóan a meglévő bevált gyakorlatok és a nemzetközi szervek (mint például az ENSZ és az Európa Tanács) ajánlásai alapján, ideértve a felügyeleti szervek „harmadik felekre vonatkozó szabály” szerinti harmadik félként való kezelésének kérdését, illetve az „átadó fél általi ellenőrzés” elvét, amely a hírszerzés külföldi országból történő felügyeletére és elszámoltathatóságára vonatkozik;

b) az átláthatóság növelésére vonatkozó kritériumokat kell kidolgoznia, az információkhoz való hozzáférés általános elvére és az úgynevezett „Tshwane elvekre”[38] építve;

106. arra készül, hogy konferenciát szervez a nemzeti – akár parlamenti vagy független – felügyeleti testületek közreműködésével;

107. felszólítja a tagállamokat, hogy a bevált gyakorlatokból merítve javítsák felügyeleti szerveik hozzáférését a hírszerzési tevékenységekre vonatkozó információkhoz (a minősített információkat és más szolgálatoktól származó információkat is beleértve), továbbá biztosítsanak hatáskört helyszíni látogatásokhoz, valamint erős hatásköröket kérdések feltételéhez, megfelelő erőforrásokat és műszaki szakértelmet, illetve az adott ország kormányzatával szembeni szigorú függetlenséget és a parlamenttel szembeni jelentéstételi kötelezettséget;

108. felszólítja a tagállamokat, hogy alakítsanak ki együttműködést a felügyeleti szervek között;

109. felszólítja a Bizottságot, hogy terjesszen elő javaslatot egy minden uniós tisztségviselőre vonatkozó uniós biztonsági ellenőrzési eljárásra vonatkozóan, mivel a jelenlegi rendszer, amely az állampolgárság szerinti tagállam által elvégzett biztonsági ellenőrzésre hagyatkozik, a nemzeti rendszereken belül eltérő követelményeket és eljárási időt tesz lehetővé, ezáltal pedig állampolgárságuktól függően a parlamenti képviselőkkel és személyzetükkel való eltérő bánásmódhoz vezet;

110. emlékeztet az Európai Parlament és a Tanács között létrejött, a közös kül- és biztonságpolitikától eltérő kérdésekkel kapcsolatos tanácsi minősített adatoknak a Parlament részére történő továbbításáról és ezen adatoknak az Európai Parlament általi kezeléséről szóló intézményközi megállapodás rendelkezéseire, amelyet fel kell használni az uniós szintű felügyelet javítása érdekében;

Uniós kutatási programok

111. szigorúbb és hatékonyabb ellenőrzési mechanizmusok bevezetésére szólít fel annak

[38] The Global Principles on National Security and the Right to Information (A nemzetbiztonság globális elvei és az információhoz való jog), 2013. június.

biztosítása érdekében, hogy az uniós kutatási alapok ne finanszírozzanak vagy mozdítsanak elő olyan eszközöket, többek között kémszoftvereket és megfigyelési eszközöket, amelyek sértik az uniós értékeket; megjegyzi, hogy az uniós jognak való megfelelés értékelésének konkrét ellenőrzési kritériumokat kell tartalmaznia az ilyen visszaélések megelőzése érdekében; felszólít az olyan szervezetek számára nyújtott uniós kutatási források megszüntetésére, amelyek érintettek voltak emberi jogok megfigyelési eszközök révén történő megsértésének közvetlen vagy közvetett elősegítésében;

112. hangsúlyozza, hogy az uniós kutatási finanszírozást, például a Horizont Európa keretében nem uniós országokkal, különösen Izraellel kötött megállapodásokat nem szabad olyan módon felhasználni, amely hozzájárul a kémszoftverek és az azzal egyenértékű technológiák fejlesztéséhez;

Az EU technológiai laboratóriuma

113. felszólítja a Bizottságot, hogy késedelem nélkül kezdeményezze egy függetlenül működtetett európai interdiszciplináris kutatóintézet létrehozását, amely az információs és kommunikációs technológia, az alapvető jogok és a biztonság összefüggéseinek kutatására és fejlesztésére összpontosít; hangsúlyozza, hogy ennek az intézetnek együtt kell dolgoznia a szakértőkkel, tudósokkal és a civil társadalom képviselőivel, és nyitottnak kell lennie a tagállami szakértők és különféle intézmények részvétele felé;

114. hangsúlyozza, hogy az intézet hozzájárulna a tudatosság, a felelősségvállalás és az elszámoltathatóság javításához Európában és azon kívül, valamint növelné az európai tehetségbázist és annak jobb megértését szolgálná, hogy a kémszoftver-forgalmazók hogyan fejlesztik, tartják fenn, értékesítik és teljesítik szolgáltatásaikat harmadik feleknek;

115. úgy véli, hogy az intézetet meg kell bízni azzal, hogy feltárja és felfedje a szoftverek tiltott megfigyelés céljára való jogellenes használatát, hogy hozzáférhető és ingyenes jogi és technológiai támogatást nyújtson – beleértve az okostelefonok átvizsgálását azon személyek számára, akik azt gyanítják, hogy kémprogramokkal vették célba őket, valamint a kémszoftverek felderítéséhez szükséges eszközöket –, hogy igazságügyi nyomozásokhoz szükséges igazságügyi elemző kutatásokat végezzen, valamint rendszeres jelentéseket tegyen a kémszoftverek Unión belüli használatáról és a velük való visszaélésekről, figyelembe véve a technológiai frissítéseket; úgy véli, hogy ezt a jelentést évente hozzáférhetővé kell tenni, és továbbítani kell a Bizottságnak, a Parlamentnek és a Tanácsnak;

116. azt ajánlja, hogy a Bizottság az uniós intézmények, szervek és hivatalok hálózatbiztonsági vészhelyzeteket elhárító csoportjával (CERT-EU) és az ENISA-val szoros együttműködésben hozza létre az EU technológiai laboratóriumát, és ennek során konzultáljon az érintett szakértőkkel, hogy tanuljon a tudományos terület bevált gyakorlataiból;

117. hangsúlyozza annak fontosságát, hogy biztosított legyen az EU technológiai laboratóriumának megfelelő finanszírozása;

118. ajánlja, hogy a Bizottság terjesszen elő egy tanúsítási rendszert a kriminalisztikai

anyagok elemzésére és hitelesítésére vonatkozóan;

119. felhívja a Bizottságot, hogy világszerte támogassa a civil társadalom képességét a kémprogramok elleni támadásokkal szembeni reziliencia, valamint a polgároknak nyújtott segítség és szolgáltatások megerősítése érdekében;

Jogállamiság

120. hangsúlyozza, hogy a kémszoftverek jogellenes használatának hatása sokkal erőteljesebb azokban a tagállamokban, ahol az állam foglyul ejtette azokat a hatóságokat, amelyek általában a nyomozással, a célba vett személyek számára jogorvoslat nyújtásával és az elszámoltathatóság biztosításával foglalkoznak, és ahol válságban van a jogállamiság, valamint veszélyben van az igazságszolgáltatás függetlensége, és ott a nemzeti hatóságokra nem lehet támaszkodni;

121. ezért felszólítja a Bizottságot, hogy biztosítsa jogállamisági eszköztárának hatékony végrehajtását, különösen az alábbiak révén:

a) a jogállamiság átfogóbb nyomon követésének bevezetése, beleértve a kémszoftverek tagállamok általi jogellenes használatával kapcsolatos országspecifikus ajánlásokat a Bizottság éves jogállamisági jelentésében, annak értékelése, hogy az állami intézmények menyiben készek jogorvoslatot nyújtani a célba vett személyek számára, valamint a Parlament többszöri kérésének megfelelően a jogállamiságról szóló éves jelentés hatályának kiterjesztése és abban a demokráciával, a jogállamisággal és az EUSZ 2. cikkében foglalt alapvető jogokkal kapcsolatos valamennyi kihívás szerepeltetése;

b) a tagállamok ellen a jogállamiság hiányosságai – például az igazságszolgáltatás függetlenségének, valamint a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés összefüggésében a rendőrség és az ügyészség hatékony működésének veszélyeztetése – miatt indított kötelezettségszegési eljárások proaktív megindítása és összevonása;

Peres ügyekben pénzügyi támogatást nyújtó uniós alap

122. felszólít arra, hogy indokolatlan késedelem nélkül hozzanak létre egy peres ügyekben pénzügyi támogatást nyújtó uniós alapot, amely fedezi a tényleges perköltségeket, és lehetővé teszi a kémszoftverek által célba vett személyek számára, hogy megfelelő jogorvoslatért folyamodjanak, beleértve a kémszoftverek ellenük való jogellenes használata miatti kártérítést, összhangban a Parlament által 2017-ben elfogadott előkészítő intézkedéssel, amely előirányozza egy uniós alap létrehozását „a demokrácia, a jogállamiság és az alapvető jogok megsértésével kapcsolatos ügyekre irányuló peres eljárásokban nyújtott pénzügyi támogatáshoz”;

Uniós intézmények

123. aggodalmának ad hangot amiatt, hogy a Bizottság eddig tétlenkedett, és sürgeti a Bizottságot, hogy a Szerződések őreként teljes mértékben használja ki minden hatáskörét, és folytasson átfogó és mélyreható vizsgálatot a kémszoftverekkel való visszaélésekről és a kémszoftverekkel folytatott kereskedelemről az Unión belül;

124. sürgeti a Bizottságot, hogy végezzen teljes körű vizsgálatot minden olyan állítással és gyanúval kapcsolatban, amely szerint tisztviselői ellen kémszoftvereket használtak, és tegyen jelentést a Parlamentnek, valamint szükség esetén az illetékes bűnüldöző hatóságoknak;

125. felhívja a Bizottságot, hogy állítson fel egy különleges munkacsoportot a nemzeti választási bizottságok részvételével a 2024-es európai választások Unió-szerte történő védelme érdekében; emlékeztet arra, hogy nemcsak a külföldi, hanem a belső beavatkozás is fenyegetést jelent az európai választási eljárásokra; hangsúlyozza, hogy az olyan átfogó megfigyelési eszközökkel való visszaélés, mint a Pegasus, a választásokra hatással lehet;

126. megjegyzi, hogy a PEGA bizottság csak a jelentéstervezet közzétételének előestéjén, körülbelül négy hónappal a Parlament levelei után kapott kollektív választ a Tanácstól az Európai Parlamentnek az egyes tagállamokhoz intézett kérdéseire; megdöbbenésének ad hangot az Európai Tanács és a Miniszterek Tanácsának tétlensége miatt, és az európai demokráciát fenyegető veszély nagyságrendjére való tekintettel kéri az Európai Tanács külön csúcstalálkozójának összehívását;

127. felhívja a Tanácsot, hogy az EUSZ 7. cikkének (1) bekezdése alapján szervezett meghallgatások során foglalkozzon a kémszoftverek használatával kapcsolatos fejleményekkel és annak az EUSZ 2. cikkében foglalt értékekre gyakorolt hatásával;

128. álláspontja szerint a Parlamentnek teljes körű vizsgálati hatáskörrel kell rendelkeznie, beleértve a minősített és nem minősített információkhoz való jobb hozzáférést, a tanúk beidézésére, a tanúk eskü alatti vallomástételre és a kért információk meghatározott határidőn belül történő átadására való hivatalos felszólítására vonatkozó hatásköröket; megismétli a Parlamentnek az Európai Parlament vizsgálati jogának gyakorlására vonatkozó részletes rendelkezésekről és a 95/167/EK, Euratom, ESZAK európai parlamenti, tanácsi és bizottsági határozat hatályon kívül helyezéséről szóló európai parlamenti rendeletre irányuló javaslatában[39] foglalt álláspontját; felhívja a Tanácsot, hogy haladéktalanul tegyen lépéseket e rendeletre irányuló javaslattal kapcsolatban az Európai Parlament megfelelő vizsgálati jognak biztosítása érdekében;

129. elismeri a Parlament kémprogramfertőzések felderítésére irányuló erőfeszítéseit; úgy véli azonban, hogy meg kell erősíteni a személyzet védelmét, tekintettel a kémkedést elszenvedők kiváltságaira és mentességeire; emlékeztet arra, hogy a képviselők politikai jogai elleni bármely támadás egyben az intézmény függetlensége és szuverenitása elleni támadás, valamint a választók jogai elleni támadás is;

130. felhívja a Parlament Elnökségét, hogy fogadjon el eljárásrendet azokra az esetekre vonatkozóan, amikor a Parlament tagjai vagy személyzete kémszoftverek közvetlen vagy közvetett célpontjává válnak, és hangsúlyozza, hogy a Parlamentnek minden esetet jelentenie kell az illetékes bűnüldöző hatóságoknak; hangsúlyozza, hogy a Parlamentnek ilyen esetekben jogi és technikai segítséget kell nyújtania;

131. úgy határoz, hogy kezdeményezi egy olyan intézményközi konferencia összehívását, amelyen a Parlamentnek, a Tanácsnak és a Bizottságnak olyan irányítási reformokra

[39] HL C 264. E, 2013.9.13., 41. o.

kell törekednie, amelyek megerősítik az Unió intézményi kapacitását, hogy megfelelően tudjon reagálni a demokrácia és a jogállamiság ellen belülről érkező támadásokra, és amelyek biztosítják, hogy az Unió hatékony szupranacionális módszerekkel rendelkezzen a Szerződések és a másodlagos jog érvényesítésére, ha a tagállamok nem felelnek meg ezeknek;

132. felhív az Unió intézményeiben, szerveiben, hivatalaiban és ügynökségeiben a kiberbiztonság magas közös szintjét célzó intézkedések megállapításáról szóló európai parlamenti és tanácsi rendeletre irányuló bizottsági javaslat (COM(2022)0122) gyors elfogadására, majd azt követően annak gyors alkalmazására és szigorú érvényesítésére az uniós intézmények személyzete és a politikusok által használt eszközök és rendszerek kémszoftverfertőzési kockázatának csökkentése érdekében;

133. felhívja az EU-t, hogy csatlakozzon a 108+ egyezményhez;

134. felhívja az európai ombudsmant, hogy kezdeményezzen megbeszéléseket az Ombudsmanok Európai Hálózatán belül a széles körű megfigyeléssel való visszaélésnek a demokratikus folyamatokra és a polgárok jogaira gyakorolt hatásáról; felhívja a hálózatot, hogy dolgozzon ki ajánlásokat az egész EU-ban biztosítandó hatékony és érdemi jogorvoslatról;

Jogalkotási intézkedések

135. felhívja a Bizottságot, hogy ezen ajánlás melléklete alapján sürgősen terjesszen elő jogalkotási javaslatokat;

°

° °

136. utasítja elnökét, hogy továbbítsa ezt az állásfoglalást a tagállamoknak, a Tanácsnak, a Bizottságnak és az Europolnak.