2014. március 12., szerda

P7_TA(2014)0230

Az egyesült államokbeli NSA megfigyelési programjáról, a különféle tagállamokban megfigyelést végző szervekről és az uniós polgárok alapvető jogaira, valamint a transzatlanti bel- és igazságügyi együttműködésre gyakorolt hatásukról

Az Európai Parlament 2014. március 12-i állásfoglalása 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 (2013/2188(INI))

(2017/C 378/14)

Az Európai Parlament,

— tekintettel az Európai Unióról szóló szerződésre (EUSZ) és különösen annak 2., 3., 4., 5., 6., 7., 10., 11. és 21. cikkére,

— tekintettel az Európai Unió működéséről szóló szerződésre (EUMSZ) és különösen annak 15., 16. és 218. cikkére, valamint V. címére,

— tekintettel az átmeneti rendelkezésekről szóló 36. jegyzőkönyvre és annak 10. cikkére, valamint e jegyzőkönyvről szóló 50. sz. nyilatkozatra,

— tekintettel az Európai Unió Alapjogi Chartájára és különösen annak 1., 3., 6., 7., 8., 10., 11., 20., 21., 42., 47., 48. és 52. cikkére,

— tekintettel az emberi jogok európai egyezményére és különösen annak 6., 8., 9., 10. és 13. cikkére, valamint a kapcsolódó jegyzőkönyvekre,

— tekintettel az Emberi Jogok Egyetemes Nyilatkozatára és különösen annak 7., 8., 10., 11., 12. és 14. cikkére ([1]),

— tekintettel a Polgári és Politikai Jogok Nemzetközi Egyezségokmányára és különösen annak 14., 17., 18. és 19. cikkére,

— tekintettel az Európa Tanács adatvédelmi egyezményére (ETS 108. sz.) és a személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezményhez csatolt, a felügyeleti hatóságokról és a határokon átnyúló adatáramlásról szóló, 2001. november 8-i kiegészítő jegyzőkönyvre (ETS 181. sz.),

— tekintettel a diplomáciai kapcsolatokról szóló bécsi egyezményre, és különösen annak 24., 27. és 40. cikkére,

— tekintettel az Európa Tanács számítástechnikai bűnözésről szóló egyezményére (ETS 185. sz.),

— tekintettel az ENSZ emberi jogoknak és alapvető szabadságoknak a terrorizmus elleni küzdelem vonatkozásában való előmozdításával és védelmével foglalkozó különleges előadójának 2010. május 17-én benyújtott jelentésére ([2]),

— tekintettel az „Internetpolitika és internetirányítás: Európa szerepe az internetirányítás jövőjének alakításában” című bizottsági közleményre (COM(2014)0072);

— tekintettel az ENSZ lelkiismereti és véleménynyilvánítási szabadsághoz való jog előmozdításával és védelmével foglalkozó különleges előadójának 2013. április 17-én benyújtott jelentésére ([3]),

— tekintettel az Európa Tanács Miniszteri Bizottságának az emberi jogokra és a terrorizmus elleni küzdelemre vonatkozó, 2002. július 11-én elfogadott iránymutatásaira,

([1]) http://www.un.org/en/documents/udhr/.
([2]) http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G10/134/10/PDF/G1013410.pdf?OpenElement.
([3]) http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

— tekintettel a Parlamenti Bizottságok 6. Konferenciája által elfogadott, az Európai Unió tagállamai hírszerző és biztonsági szolgálatainak felügyeletére vonatkozó, 2010. október 1-jei Brüsszeli Nyilatkozatra,

— tekintettel az Európa Tanács Parlamenti Közgyűlésének a nemzetbiztonságról és az információkhoz való hozzáférésről szóló 1954 (2013) sz. állásfoglalására,

— tekintettel a Velencei Bizottság által 2007. június 11-én elfogadott, a biztonsági szolgálatok demokratikus felügyeletéről szóló jelentésre ([1]), és komoly érdeklődéssel tekintve annak 2014 tavaszán esedékes aktualizálása elé,

— tekintettel a belga, holland, dán és norvég hírszerzési felügyeleti bizottságok képviselőinek nyilatkozataira,

— tekintettel a francia ([2]), lengyel és brit ([3]) bíróságok, valamint az Emberi Jogok Európai Bírósága ([4]) előtt indított, tömeges megfigyelésre alkalmas rendszerekkel kapcsolatos keresetekre,

— tekintettel a Tanács által az Európai Unióról szóló szerződés 34. cikkével összhangban létrehozott, az Európai Unió tagállamai közötti kölcsönös bűnügyi jogsegélyről szóló egyezményre ([5]) és különösen annak III. címére,

— tekintettel az Egyesült Államok Kereskedelmi Minisztériuma által kiadott „biztonságos kikötő” adatvédelmi elvek által biztosított védelem megfelelőségéről és az ezzel kapcsolatos gyakran felvetődő kérdésekről szóló, 2000. július 26-i 2000/520/EK bizottsági határozatra,

— tekintettel a védett adatkikötőre vonatkozó alapelvek végrehajtásáról szóló, 2002. február 13-i (SEC(2002)0196) és 2004. október 20-i (SEC(2004)1323) bizottsági értékelő jelentésekre,

— tekintettel a védett adatkikötőnek az uniós polgárok és az unióban letelepedett társaságok szempontjából való működéséről szóló, 2013. november 27-i bizottsági közleményre (COM(2013)0847), valamint az Európai Unió és az Egyesült Államok közötti adatáramlás vonatkozásában a bizalom újjáépítéséről szóló, 2013. november 27-i bizottsági közleményre (COM(2013)0846),

— tekintettel az Egyesült Államok Kereskedelmi Minisztériuma által kiadott „biztonságos kikötő” adatvédelmi elvek által biztosított védelem megfelelőségéről és az ezzel kapcsolatos gyakran felvetődő kérdésekről szóló bizottsági határozattervezetről szóló, 2000. július 5-i állásfoglalására ([6]), amely arra az álláspontra helyezkedett, hogy a rendszer megfelelősége nem megerősíthető, továbbá tekintettel a 29. cikk szerinti munkacsoport véleményeire és különösen 2000. május 16-i 04/2000. számú véleményére ([7]),

— tekintettel az Amerikai Egyesült Államok és az Európai Unió közötti, az utas-nyilvántartási adatállomány (PNR) felhasználásáról és továbbításáról szóló, 2004., 2007. ([8]) és 2012. évi megállapodásokra ([9]),

— tekintettel az Európai Unió és az Amerikai Egyesült Államok közötti, az utas-nyilvántartási adatállomány (PNR) adatainak feldolgozásáról és az Egyesült Államok Belbiztonsági Minisztériuma részére történő továbbításáról szóló megállapodás végrehajtásának közös felülvizsgálatára ([10]), amely az Európai Parlamenthez és a Tanácshoz intézett, közös felülvizsgálatról szóló bizottsági jelentést (COM(2013)0844) kíséri,

---

([1]) http://www.venice.coe.int/webforms/documents/CDL-AD(2007)016.aspx.
([2]) Az Emberi Jogi Szervezetek Nemzetközi Szövetsége és a francia emberi és állampolgári jogvédő szövetség kontra X; párizsi fellebbviteli bíróság.
([3]) A Privacy International és a Liberty által indított ügyek a nyomozati szervekkel foglalkozó bíróságon (Investigatory Powers Tribunal).
([4]) A 34. cikk alapján benyújtott közös kereset: Big Brother Watch, Open Rights Group, English Pen, Dr Constanze Kurz (felperes) kontra Egyesült Királyság (alperes).
([5]) HL C 197., 2000.7.12., 1. o.
([6]) HL C 121., 2001.4.24., 152. o.
([7]) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp32en.pdf.
([8]) HL L 204., 2007.8.4., 18. o.
([9]) HL L 215., 2012.8.11., 5. o.
([10]) SEC(2013)0630, 2013.11.27.

2014. március 12., szerda

— tekintettel Cruz Villalón főtanácsnok véleményére, amelyben arra a következtetésre jut, hogy a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről szóló 2006/24/EK irányelv teljes egészében összeegyeztethetetlen az Európai Unió Alapjogi Chartája 52. cikkének (1) bekezdésével, az irányelv 6. cikke pedig összeegyeztethetetlen a Charta 7. cikkével és 52. cikkének (1) bekezdésével ([1]),

— tekintettel az Európai Unió és az Amerikai Egyesült Államok között az Európai Unióból származó pénzügyi üzenetadatoknak a terrorizmus finanszírozásának felderítését célzó program céljából történő feldolgozásáról és az Amerikai Egyesült Államok részére való átadásáról szóló megállapodás megkötéséről szóló, 2010. július 13-i 2010/412/EU tanácsi határozatra ([2]), valamint a Bizottság és a Tanács azt kísérő nyilatkozataira,

— tekintettel az Európai Unió és az Amerikai Egyesült Államok közötti, kölcsönös jogsegélyről szóló megállapodásra ([3]),

— tekintettel a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében bűncselekmények, köztük terrorcselekmények megelőzése, kivizsgálása, felderítése és büntetőeljárás lefolytatása céljából átadott és feldolgozott személyes adatok védelméről szóló, az Európai Unió és az Amerikai Egyesült Államok közötti keretmegállapodásról (átfogó megállapodásról) szóló, folyamatban lévő tárgyalásokra,

— tekintettel a harmadik ország által elfogadott jogszabályoknak az ország területén kívüli alkalmazásának hatásáról és az ilyen jogszabályon alapuló vagy abból eredő intézkedések elleni védelemről szóló, 1996. november 22-i 2271/96/EK tanácsi rendeletre ([4]),

— tekintettel a Brazil Szövetségi Köztársaság elnöke által az ENSZ-közgyűlés 68. ülésszakának 2013. szeptember 24-i megnyitóján tett nyilatkozatra, valamint a brazil szövetségi szenátus által létrehozott, a kémkedés kivizsgálásával foglalkozó parlamenti bizottság munkájára,

— tekintettel a George W. Bush elnök által 2001. október 26-án aláírt USA Patriot Act törvényre,

— tekintettel a külföldi hírszerzés felügyeletéről szóló 1978. évi törvényre (FISA), valamint a FISA módosításáról szóló 2008. évi törvényre,

— tekintettel az Egyesült Államok elnöke által 1981-ben kiadott és 2008-ban módosított 12333. sz. végrehajtási utasításra,

— tekintettel a rádióelektronikai felderítési tevékenységekről szóló, Barack Obama elnök által 2014. január 17-én közzétett elnöki rendeletre (PPD-28),

— tekintettel az Egyesült Államok Kongresszusa által jelenleg vizsgált jogalkotási javaslatokra, ideértve az USA Freedom Act törvénytervezetet, a hírszerzési felügyeletről és a megfigyelés reformjáról szóló törvénytervezeteket és más jogszabályokat,

— tekintettel az adatvédelmi és állampolgári jogi felügyeleti bizottság, az Egyesült Államok Nemzetbiztonsági Tanácsa, valamint az elnök hírszerzési és kommunikációs technológiákkal foglalkozó felülvizsgálati csoportja által végzett felülvizsgálatokra és különösen ez utóbbi által 2013. december 12-én közzétett, „Szabadság és biztonság a változó világban” című jelentésre,

— tekintettel az Egyesült Államok Columbia Szövetségi Kerületi Körzeti Bírósága által a 13-0851. sz. Klayman és társai kontra Obama és társai polgári perben 2013. december 16-án hozott ítéletre, valamint az Egyesült Államok New York Déli Körzet Körzeti Bírósága által a 13-3994. sz. ACLU és társai kontra James R. Clapper és társai polgári ügyben 2013. június 11-én hozott ítéletre,

— tekintettel az EU–USA eseti munkacsoport uniós társelnökeinek adatvédelmi megállapításairól szóló, 2013. november 27-i jelentésre ([5]),

([1]) Cruz Villalón főtanácsnok 2013. december 12-i véleménye a C-293/12. sz. ügyben.
([2]) HL L 195., 2010.7.27., 3. o.
([3]) HL L 181., 2003.7.19., 34. o.
([4]) HL L 309., 1996.11.29., 1. o.
([5]) 16987/2013. számú tanácsi dokumentum.

— tekintettel a magán- és kereskedelmi jellegű közlések lehallgatására szolgáló globális rendszer (ECHELON lehallgatórendszer) létezéséről szóló, 2001. szeptember 5-i ([1]) és 2002. november 7-i ([2]) állásfoglalásaira,

— tekintettel „Az EU Alapjogi Chartája: a tömegtájékoztatás szabadságára vonatkozó irányadó szabályozás az EU-ban” című, 2013. május 21-i állásfoglalására ([3]),

— tekintettel az egyesült államokbeli NSA megfigyelési programjáról, a különféle tagállamokban megfigyelést végző szervekről és az uniós polgárok magánéletére gyakorolt hatásukról szóló, 2013. július 4-i állásfoglalására ([4]), amelyben megbízta az Állampolgári Jogi, Bel- és Igazságügyi Bizottságot, hogy végezzen alapos vizsgálatot az ügyben,

— tekintettel az Egyesült Államok és az EU megfigyelési programjairól és azoknak az uniós polgárok alapvető jogaira gyakorolt hatásairól szóló 1. sz. munkadokumentumra,

— tekintettel az Unióban és az Egyesült Államokban folytatott megfigyelési gyakorlatok és az uniós adatvédelmi rendelkezések közötti kapcsolatról szóló 3. sz. munkadokumentumra,

— tekintettel az Egyesült Államok uniós adatokat érintő megfigyelési tevékenységéről és annak a transzatlanti megállapodásokra és együttműködésre gyakorolt lehetséges jogi következményeiről szóló 4. sz. munkadokumentumra,

— tekintettel a tagállamok hírszerző szolgálatainak és az EU hírszerző szerveinek demokratikus felügyeletéről szóló 5. sz. munkadokumentumra,

— . tekintettel az AFET bizottságnak „Az európai uniós polgárok tömeges elektronikus megfigyeléséről szóló vizsgálat külpolitikai szempontjai” című munkadokumentumára,

— tekintettel „A szervezett bűnözés, a korrupció és a pénzmosás problémája: megvalósítandó intézkedésekre és kezdeményezésekre vonatkozó ajánlások” című, 2013. október 23-i állásfoglalására ([5]),

— tekintettel a TFTP-megállapodásnak az egyesült államokbeli NSA megfigyelési programja miatt történő felfüggesztéséről szóló, 2013. október 23-i állásfoglalására ([6]),

— tekintettel „A számítási felhőben rejlő potenciál felszabadításáról Európában” című, 2013. december 10-i állásfoglalására ([7]),

— tekintettel az Európai Parlament és a Tanács között létrejött, a közös kül- és biztonságpolitikától eltérő kérdésekkel kapcsolatos tanácsi minősített adatoknak az Európai Parlament részére történő továbbításáról és ezen adatoknak az Európai Parlament általi kezeléséről szóló intézményközi megállapodásra ([8]),

— tekintettel eljárási szabályzata VIII. mellékletére,

— tekintettel eljárási szabályzata 48. cikkére,

— tekintettel az Állampolgári Jogi, Bel- és Igazságügyi Bizottság jelentésére (A7-0139/2014),

A tömeges megfigyelés hatásai

A. mivel az adatvédelem és a magánélet védelme alapvető jogok; mivel a biztonsági intézkedéseket és köztük a terrorizmus elleni intézkedéseket ezért a jogállamiság és az alapvető jogokkal kapcsolatos kötelezettségek, így többek közt a magánélet és az adatok védelméhez fűződő jogok tiszteletben tartásával kell megtenni;

([1]) HL C 72. E, 2002.3.21., 221. o.
([2]) HL C 16. E, 2004.1.22., 88. o.
([3]) Elfogadott szövegek, P7_TA(2013)0203.
([4]) Elfogadott szövegek, P7_TA(2013)0322.
([5]) Elfogadott szövegek, P7_TA(2013)0444.
([6]) Elfogadott szövegek, P7_TA(2013)0449.
([7]) Elfogadott szövegek, P7_TA(2013)0535.
([8]) HL C 353. E, 2013.12.3., 156. o.

2014. március 12., szerda

B. mivel a mindennapi életet uraló és bármely személy integritásának részét képező információáramlást és az adatokat ugyanolyan védetté kell tenni a behatolással szemben, mint a magánlakásokat;

C. mivel az Európa és az Amerikai Egyesült Államok közötti kapcsolatok a demokrácia és a jogállamiság, a szabadság, a jogérvényesülés és a szolidaritás szellemén és elvén alapulnak;

D. mivel az USA és az Európai Unió és tagállamai közötti terrorizmusellenes együttműködés mindkét fél biztonsága és védelme szempontjából továbbra is nélkülözhetetlen;

E. mivel a kölcsönös bizalom és megértés a transzatlanti párbeszéd és partnerség kulcsfontosságú tényezői;

F. mivel 2001. szeptember 11-ét követően a terrorizmus elleni küzdelem a kormányzatok többsége számára kiemelt prioritássá vált; mivel az Edward Snowden, egykori NSA-alvállalkozó által kiszivárogtatott dokumentumok alapján feltárt információk arra kényszerítették a politikai vezetőket, hogy kezeljék a hírszerző ügynökségek megfigyelési tevékenységek tekintetében történő felügyeletével és ellenőrzésével kapcsolatos kihívásokat, és értékeljék tevékenységük alapvető jogokra és a jogállamiságra gyakorolt hatásait a demokratikus társadalomban;

G. mivel a 2013 júniusa óta feltárt információk számos esetben aggodalmat váltottak ki az Unióban az alábbiak vonatkozásában:

— a feltárt megfigyelési rendszerek nagyságrendje mind az Egyesült Államokban, mind pedig az uniós tagállamokban;

— az uniós jogi normák, az alapvető jogok és az adatvédelmi előírások megsértése;

— az EU és az USA mint transzatlanti partnerek közötti bizalom szintje;

— egyes uniós tagállamok együttműködésének és közreműködésének mértéke az Egyesült Államok megfigyelési programjaiban vagy azzal egyenértékű programokban nemzeti szinten, a média által feltártak szerint;

— az egyesült államokbeli politikai hatóságok és egyes uniós tagállamok részéről a saját hírszerző szervezeteik felett gyakorolt ellenőrzés és hatékony felügyelet hiánya;

— annak lehetősége, hogy e tömeges megfigyelésre irányuló műveleteket a nemzetbiztonságtól és a szigorú értelemben vett terrorizmus elleni küzdelemtől eltérő okokból, így például gazdasági és ipari kémkedés vagy politikai alapú profilalkotás céljából is alkalmazzák;

— a sajtószabadság és a titoktartási kötelezettséggel járó szakmákat gyakorlókkal – köztük az ügyvédekkel és az orvosokkal – folytatott kommunikáció veszélyeztetése;

— a hírszerző ügynökségek, valamint a magánkézben lévő informatikai és távközlési társaságok szerepe és közreműködésének mértéke;

— fokozottan elmosódó határok a bűnüldözés és a hírszerző tevékenységek között, aminek következtében minden polgárt gyanúsítottként kezelnek és megfigyelnek;

— a magánélet védelmére jelentett veszélyek a digitális korszakban és a tömeges megfigyelés hatásai a polgárokra és a társadalmakra;

H. mivel a feltárt kémkedési tevékenység példátlan nagyságrendje teljes körű kivizsgálást tesz szükségessé az egyesült államokbeli hatóságok, az európai intézmények, valamint a tagállamok kormányzatai, nemzeti parlamentjei és igazságügyi hatóságai részéről;

I. mivel az egyesült államokbeli hatóságok a feltárt információk egy részét cáfolták, túlnyomó többségüket azonban nem vitatták; mivel az Egyesült Államokban és egyes uniós tagállamokban nagyszabású nyilvános vita alakult ki; mivel az uniós kormányzatok és parlamentek túlságosan gyakran némaságba burkolóznak, és nem indítanak megfelelő vizsgálatokat;

J. mivel Obama elnök nemrég bejelentette az NSA és megfigyelési programjai reformját;

K. mivel az uniós intézmények és egyes uniós tagállamok által meghozott intézkedésekkel összevetve az Európai Parlament rendkívül komolyan vette azzal kapcsolatos kötelezettségét, hogy nyilvánosságra hozza az uniós polgárok nem célirányos, tömeges megfigyelésének gyakorlatára vonatkozóan feltárt információkat, és az egyesült államokbeli NSA megfigyelési programjáról, a különféle tagállamokban megfigyelést végző szervekről és az uniós polgárok magánéletére gyakorolt hatásukról szóló, 2013. július 4-i állásfoglalásában megbízta az Állampolgári Jogi, Bel- és Igazságügyi Bizottságot, hogy végezzen alapos vizsgálatot az ügyben;

L. mivel az európai intézmények kötelessége annak biztosítása, hogy az uniós jogot maradéktalanul végrehajtsák az európai polgárok javára, az uniós szerződések jogi erejét pedig ne veszélyeztesse a harmadik országok normái vagy fellépései területen kívüli hatályának érdektelen elfogadása;

A hírszerzési reform egyesült államokbeli fejleményei

M. mivel a Columbia Szövetségi Kerületi Körzeti Bíróság 2013. december 16-i döntésében úgy határozott, hogy a metaadatok nagytömegű gyűjtése az NSA részéről sérti az Egyesült Államok alkotmányának negyedik kiegészítését ([1]); mivel azonban New York Déli Körzet Körzeti Bírósága 2013. december 27-i határozatában jogszerűnek minősítette az ilyen adatgyűjtést;

N. mivel a Michigan Keleti Körzet Körzeti Bírósága határozatában kimondta, hogy a negyedik alkotmánykiegészítés minden házkutatásra, illetve motozásra vonatkozóan megköveteli, hogy az ésszerű legyen, hogy az ésszerű házkutatásról, illetve motozásról előzetesen kiadott végzés rendelkezzen, hogy a végzéseket az előzetesen fennálló gyanúok alapján adják ki, továbbá hogy a személyek, helyek és tárgyak pontosan legyenek megjelölve, valamint hogy a végrehajtásban közreműködő tisztviselők és a polgárok között álljon egy pártatlan bíró ([2]);

O. mivel 2013. december 12-i jelentésében az elnök hírszerzési és kommunikációs technológiákkal foglalkozó felülvizsgálati csoportja 46 ajánlást fogalmazott meg az Egyesült Államok elnöke számára; mivel az ajánlások hangsúlyozzák a nemzetbiztonság, valamint a személyes adatok és a polgári szabadságjogok egyidejű védelmének szükségességét; mivel ezzel összefüggésben az ajánlások felkérik az Egyesült Államok kormányát, hogy: vessen véget az egyesült államokbeli személyek által folytatott telefonbeszélgetések tömeges gyűjtésének az USA Patriot Act törvény 215. szakasza értelmében. amint az megvalósítható; végezze el az NSA és az Egyesült Államok hírszerzésre vonatkozó jogi keretek mélyreható felülvizsgálatát annak érdekében, hogy garantálja a magánélethez való jog tiszteletben tartását; vessen véget a kereskedelmi szoftverek kijátszására vagy sérülékennyé tételére irányuló erőfeszítéseknek („hátsó ajtók" (backdoor) és rosszindulatú programok (malware)); fokozzák az adattitkosítás alkalmazását, különösen a továbbított adatok esetében, és ne veszélyeztessék az adattitkosítási szabványok kialakítására irányuló erőfeszítéseket; nevezzenek ki a közérdek védelmében eljáró képviselőt, aki a magánélethez való jog és a polgári szabadságjogok védelme érdekében jár el a külföldi hírszerzési tevékenységek megfigyelésével foglalkozó bíróság (FISC) előtt; a magánélet védelmével és a polgári szabadságjogok felügyeletével foglalkozó bizottságot pedig hatalmazzák fel arra, hogy a hírszerző szervezeteknek ne csupán a terrorizmus elleni küzdelem, hanem a külföldi hírszerzés céljából végzett tevékenységeit is felügyelje; továbbá hogy fogadja a visszaélést jelentő személyek panaszait, és használja fel a kölcsönös jogsegélyről szóló szerződéseket az elektronikus közlések megszerzésére, valamint hogy ne alkalmazzon megfigyelést az ipari vagy üzleti titkok ellopása céljából;

P. mivel a korábbi NSA felsővezetők/a Veteran Intelligence Professionals for Sanity (VIPS) (veterán hírszerző szakemberek a hiteles tájékoztatásért) szervezet által 2014. január 7-én Obama elnöknek küldött nyílt feljegyzés ([3]) értelmében a tömeges adatgyűjtés nem javítja a jövőbeli terroristatámadások megelőzésére való képességet; mivel a szerzők hangsúlyozzák, hogy az NSA által végzett tömeges megfigyelés egyetlen támadást sem előzött meg, valamint hogy dollár milliárdokat költöttek olyan programokra, amelyek a 2001-ben létrehozott, THINTHREAD elnevezésű belső technológiánál kevésbé hatékonyak és jóval nagyobb mértékben avatkoznak be a polgárok magánéletébe;

Q. mivel a FISA 702. szakaszán alapuló, a nem egyesült államokbeli személyekre irányuló hírszerzési tevékenységek vonatkozásában az USA elnökéhez intézett ajánlások elismerik az Emberi Jogok Egyetemes Nyilatkozatának 12. cikkében, valamint a Polgári és Politikai Jogok Nemzetközi Egyezségokmányának 17. cikkében foglalt, a magánélet és az emberi méltóság tiszteletben tartásának alapvető elvét; mivel nem javasolják, hogy a nem egyesült államokbeli személyek számára ugyanolyan jogokat és védelmet biztosítsanak, mint az egyesült államokbeli személyek számára;

([1]) Klayman és társai kontra Obama és társai, 13-0851. sz. polgári per, 2013. december 16.
([2]) ACLU kontra NSA, 06-CV-10204. sz. ügy, 2006. augusztus 17.
([3]) http://consortiumnews.com/2014/01/07/nsa-insiders-reveal-what-went-wrong.

2014. március 12., szerda

R. mivel a rádióelektronikai felderítési tevékenységekről szóló, 2014. január 17-i elnöki rendeletében és az ahhoz kapcsolódó beszédében Barack Obama amerikai elnök kijelentette, hogy az Egyesült Államoknak nemzetbiztonságának, állampolgárainak, valamint az USA szövetségesei és partnerei állampolgárainak védelme, illetve külpolitikai érdekeinek előmozdítása érdekében szüksége van a tömeges elektronikus megfigyelésre; mivel ez az elnöki rendelet tartalmaz a jelhírszerzési adatok gyűjtésére, felhasználására és megosztására vonatkozóan bizonyos elveket, és egyes biztosítékokat az egyesült államokbeli állampolgárokkal részben egyenlő elbánást biztosítva a nem egyesült államokbeli személyekre is kiterjeszt, ideértve többek közt a személyes adatokra vonatkozó, állampolgárságra vagy lakóhelyre való tekintet nélkül irányadó biztosítékokat; mivel azonban Obama elnök nem kérte konkrét, különösen a tömeges megfigyelés betiltására és a nem amerikai állampolgárok által igénybe vehető közigazgatási és bírósági jogorvoslat bevezetésére vonatkozó javaslatok kidolgozását;

Jogi keretek

Alapvető jogok

S. mivel az EU–USA eseti munkacsoport uniós társelnökeinek adatvédelmi megállapításairól szóló jelentés áttekintést nyújt az egyesült államokbeli jogi helyzetről, azonban elmulasztotta megállapítani az egyesült államokbeli megfigyelési programokkal kapcsolatos tényeket; mivel nem bocsátottak rendelkezésre információkat az úgynevezett „másodvonalbeli" munkacsoportról, amelynek keretében a tagállamok kétoldalúan megvitatják az egyesült államokbeli hatóságokkal a nemzetbiztonsági vonatkozású kérdéseket;

T. mivel az Európai Unió Alapjogi Chartájában és az Emberi Jogok Európai Egyezményében foglalt alapvető jogok, nevezetesen a véleménynyilvánítás szabadsága, a sajtószabadság, a gondolatszabadság, a lelkiismeret szabadsága, a vallás és az egyesülés szabadsága, a magánélethez és az adatvédelemhez, valamint a hatékony jogorvoslathoz való jog, az ártatlanság vélelme, a tisztességes eljáráshoz és a megkülönböztetésmentességhez való jog a demokrácia sarokkövei; mivel az emberek tömeges megfigyelése összeegyeztethetetlen ezekkel a sarokkövekkel;

U. mivel valamennyi tagállamban jogszabály véd az ügyvéd és ügyfele között bizalmasan közölt információk feltárásával szemben, és ezt az elvet az Európai Unió Bírósága is elismerte ([1]);

V. mivel a szervezett bűnözésről, a korrupcióról és a pénzmosásról szóló 2013. október 23-i állásfoglalásában a Parlament felszólította a Bizottságot, hogy nyújtson be jogalkotási javaslatot az állami és a magánszférát érintő visszaélést jelentő személyekre irányuló, hatékony és átfogó európai védelmi programra vonatkozóan az unió pénzügyi érdekeinek védelme érdekében, továbbá hogy vizsgálja meg annak lehetőségét, hogy a jövőbeli javaslatok más uniós hatáskörbe tartozó területekre is kiterjedjenek;

A biztonság területén fennálló uniós hatáskörök

W. mivel az EUMSZ 67. cikkének (3) bekezdése értelmében az Unió „a biztonság magas szintjének garantálásán munkálkodik"; mivel a Szerződés rendelkezései (különösen az EUSZ 4. cikkének (2) bekezdése, az EUMSZ 72. cikke és az EUMSZ 73. cikke) arra utalnak, hogy az EU rendelkezik bizonyos hatáskörökkel az Unió kollektív biztonságát érintő kérdésekben; mivel az Unió a belső biztonsági kérdésekben hatáskörrel rendelkezik (az EUMSZ 4. cikkének j) pontja), és e hatáskörét oly módon gyakorolta, hogy több jogalkotási eszközről is határozott, valamint nemzetközi megállapodásokat kötött (PNR, TFTP) a súlyos bűncselekmények és a terrorizmus elleni küzdelem céljából, továbbá azáltal is, hogy kidolgozott egy belső biztonsági stratégiát, és e területen ügynökségeket hozott létre;

X. mivel az Európai Unió működéséről szóló szerződés (az EUMSZ 73. cikke) kimondja, hogy „[a] tagállamok számára nyitva áll a lehetőség, hogy egymás között és saját hatáskörükben, az általuk legcélszerűbbnek ítélt módon közigazgatásaiknak a nemzeti biztonság védelméért felelős, hatáskörrel rendelkező szervezeti egységei közötti együttműködés és koordináció formáit megszervezzék";

Y. mivel az EUMSZ 276. cikke kimondja, hogy „[a] harmadik résznek a szabadságon, a biztonságon és a jog érvényesülésén alapuló térségről szóló V. címe 4. és 5. fejezete rendelkezéseire vonatkozó hatásköreinek gyakorlása során az Európai Unió Bírósága nem rendelkezik hatáskörrel egy tagállam rendőrsége vagy más bűnüldöző szolgálata által végrehajtott intézkedések érvényességének vagy arányosságának, illetve a közrend fenntartásával és a belső biztonság megőrzésével kapcsolatos tagállami hatáskörök gyakorlásának felülvizsgálatára";

([1]) A C-155/79. sz. AM & S Europe Limited kontra az Európai Közösségek Bizottsága ügyben hozott, 1982. május 18-i ítélet.

Z. mivel a „nemzetbiztonság”, a „belső biztonság”, „az Unió belső biztonsága” és a „nemzetközi biztonság” fogalmai között átfedés figyelhető meg; mivel a szerződések jogáról szóló bécsi egyezmény, a tagállamok közötti lojális együttműködés elve, valamint azon emberi jogi elv, miszerint a kivételeket szigorúan kell értelmezni, mind a „nemzetbiztonság” fogalmának korlátozó jellegű értelmezésére utalnak, és megkövetelik a tagállamoktól, hogy tartózkodjanak az uniós hatáskörökbe történő beavatkozástól;

AA. mivel az európai Szerződések „a Szerződések őrének” szerepével ruházzák fel az Európai Bizottságot, és ezért az uniós jog esetleges megsértése eseteinek kivizsgálása az Európai Bizottság jogi kötelezettsége;

AB. mivel az EUSZ-nek az Európai Unió Alapjogi Chartájára és az EJEE-re utaló 6. cikkével összhangban a nemzetbiztonság területén működő tagállami ügynökségeknek és magánfeleknek egyaránt tiszteletben kell tartaniuk az abban rögzített jogokat, legyen szó akár saját állampolgáraikról, akár más országok állampolgárairól;

Területen kívüli hatály

AC. mivel egy harmadik ország törvényeinek, rendeleteinek és más jogalkotási vagy végrehajtási eszközeinek extraterritoriális alkalmazása az Unió vagy tagállamainak joghatósága alá tartozó helyzetekben hatással lehet a kialakult jogrendre és a jogállamiságra, vagy akár sértheti a nemzetközi vagy az uniós jogot, köztük a természetes és jogi személyek jogait, figyelembe véve az ilyen alkalmazás mértékét, valamint deklarált vagy tényleges célját; mivel ilyen körülmények között szükség van az uniós szintű fellépésre annak biztosítása érdekében, hogy az Unión belül tiszteletben tartják az EUSZ 2. cikkében, az Alapjogi Chartában, az EJEE-ben foglalt uniós értékeket, azaz az alapvető jogokat, a demokráciát és a jogállamiságot, valamint a természetes és jogi személyeknek az ezen alapelveket alkalmazó másodlagos jogszabályokban foglalt jogait, például azáltal, hogy felszámolják, semlegesítik, meggátolják vagy más formában ellensúlyozzák az érintett külföldi jogszabály hatásait;

Nemzetközi adattovábbítás

AD. mivel a személyes adatoknak az uniós intézmények, szervek, hivatalok, ügynökségek vagy a tagállamok által az Egyesült Államok részére bűnüldözési célból történő továbbítása az uniós polgárok alapvető jogainak – különösen a magánélethez és a személyes adatok védelméhez való jog – tiszteletben tartására vonatkozó megfelelő garanciák és biztosítékok hiányában, az EUMSZ 340. cikke vagy az EUB állandó ítélkezési gyakorlata ([1]) alapján felelősségre vonhatóvá tenné az adott uniós intézményt, szervet, hivatalt, ügynökséget vagy tagállamot az uniós jog megsértéséért, ami az Európai Unió Alapjogi Chartájában rögzített alapvető jogok bárminemű megsértését is magában foglalja;

AE. mivel az adattovábbítás földrajzilag nem behatárolt, és különösen a fokozódó globalizáció és a világszintű kommunikáció fényében az uniós jogalkotó új kihívásokkal szembesül a személyes adatok és a kommunikáció védelme során; mivel ezért kiemelkedően fontos a közös normákra vonatkozó jogi keretek kidolgozásának támogatása;

AF. mivel a személyes adatok kereskedelmi céllal, valamint a terrorizmus és a súlyos nemzetközi bűnözés elleni küzdelem keretében történő tömeges gyűjtése veszélyezteti az uniós polgárok személyes adatait és magánélethez való jogát;

Adatok továbbítása az Egyesült Államok részére az Egyesült Államok védett adatkikötőre vonatkozó alapelvei (Safe Harbour) alapján

AG. mivel az USA adatvédelmi jogi keretei nem biztosítanak megfelelő szintű védelmet az uniós polgárok számára;

AH. mivel annak érdekében, hogy az adatkezelők számára lehetővé tegyék a személyes adatok továbbítását egy egyesült államokbeli szervezethez, a Bizottság 2000/520/EK határozatában megfelelőnek minősítette az Egyesült Államok Kereskedelmi Minisztériuma által kiadott, védett adatkikötőre vonatkozó elvek által biztosított védelmet és az ezzel kapcsolatos gyakran felvetődő kérdéseket a személyes adatoknak az Unióból az Egyesült Államokban leletelepedett olyan szervezetek számára történő továbbítása esetén, amelyek csatlakoztak a védett adatkikötőre vonatkozó elvekhez;

([1]) Lásd mindenekelőtt a C-6/90. és a C-9/90. sz., Francovich és társai kontra Olaszország egyesített ügyekben 1991. november 19-én hozott ítéletet.

2014. március 12., szerda

AI. mivel a Parlament 2000. július 5-i állásfoglalásában kételyeket és aggályokat fogalmazott meg a védett adatkikötő megfelelőségét illetően, és felszólította a Bizottságot, hogy idejében vizsgálja felül a határozatot a tapasztalatok és a jogalkotási fejlemények tükrében;

AJ. mivel az Egyesült Államok uniós adatokat érintő megfigyelési tevékenységéről és annak a transzatlanti megállapodásokra és együttműködésre gyakorolt lehetséges jogi következményeiről szóló, 2013. december 12-i 4. sz. parlamenti munkadokumentumban az előadók kételyeket és aggályokat fogalmaztak meg a védett adatkikötő megfelelőségét illetően, és felszólították a Bizottságot, hogy helyezze hatályon kívül a védett adatkikötő megfelelőségére vonatkozó határozatot, és találjon új jogi megoldásokat;

AK. mivel a Bizottság 2000/520/EK határozata kimondja, hogy a tagállamok illetékes hatóságai gyakorolhatják meglévő hatáskörüket az olyan szervezet felé irányuló adatáramlás felfüggesztésére, amely önmaga tanúsította a védett adatkikötőre vonatkozó elvek elfogadását, annak érdekében, hogy védjék az egyéneket a személyes adatok kezelése tekintetében olyan esetekben, ahol a védett adatkikötőre vonatkozó elvek megsértésének nagy a valószínűsége, vagy a folytatódó adattovábbítás az érintettek súlyos károsodásának közvetlen veszélyével fenyeget;

AL. mivel a Bizottság 2000/520/EK határozata azt is kimondja, hogy amennyiben bebizonyosodik, hogy az elveknek való megfelelés biztosításáért felelős bármely szerv nem hatékonyan tölti be szerepét, a Bizottság köteles tájékoztatni az Egyesült Államok Kereskedelmi Minisztériumát, és szükség esetén intézkedéseket előterjeszteni e határozat visszavonása, felfüggesztése vagy hatályának korlátozása céljából;

AM. mivel a védett adatkikötő végrehajtásáról szóló, 2002-ben és 2004-ben közzétett első két jelentésében a Bizottság több hiányosságot is azonosított a védett adatkikötő megfelelő végrehajtását illetően, és több ajánlást is megfogalmazott az egyesült államokbeli hatóságok számára e hiányosságok kiküszöbölése érdekében;

AN. mivel 2013. november 27-i harmadik végrehajtási jelentésében – kilenc évvel a második jelentést követően és anélkül, hogy az abban a jelentésben azonosított hiányosságokat orvosolták volna – a Bizottság további gyengeségek és hiányosságok széles körét azonosította a védett adatkikötő vonatkozásában, és arra a következtetésre jutott, hogy a jelenlegi megvalósítás nem tartható fenn; mivel a Bizottság hangsúlyozta, hogy az egyesült államokbeli hírszerző ügynökségek széles körű hozzáférése a védett adatkikötőre vonatkozó tanúsítvánnyal rendelkező szervezetek által az Egyesült Államokba továbbított adatokhoz további súlyos kérdéseket vet fel az uniós érintettek adatai védelmének folytonosságát illetően; mivel a Bizottság 13 ajánlást intézett az egyesült államokbeli hatóságokhoz, és vállalta, hogy 2014 nyaráig az egyesült államokbeli hatóságokkal közösen azonosítja a mihamarabb megvalósítandó korrekciókat, ami a védett adatkikötőre vonatkozó elvek működésének teljes körű felülvizsgálatának alapjául szolgál;

AO. mivel az Európai Parlament Állampolgári Jogi, Bel- és Igazságügyi Bizottságának (LIBE bizottság) 2013. október 28–31-én Washingtonba látogató küldöttsége találkozott az Egyesült Államok Kereskedelmi Minisztériumának és az Egyesült Államok Szövetségi Kereskedelmi Bizottságának képviselőivel; mivel a Kereskedelmi Minisztérium elismerte, hogy léteznek olyan szervezetek, amelyek ugyan önmaguk tanúsították a védett adatkikötőre vonatkozó elvek betartását, ám státuszuk egyértelműen elévült, ami azt jelenti, hogy az ilyen társaságok nem teljesítik a védett adatkikötőre vonatkozó követelményeket, noha az Unióból továbbra is személyes adatokat kapnak; mivel a Szövetségi Kereskedelmi Bizottság elismerte, hogy a védett adatkikötő felülvizsgálatára van szükség annak javítása érdekében, különös tekintettel a panaszkezelési és az alternatív vitarendezési rendszerekre;

AP. mivel a védett adatkikötőre vonatkozó elvek „a nemzetbiztonság, a közérdek vagy a bűnüldözés követelményeinek teljesítéséhez szükséges mértékben” korlátozhatók; mivel alapvető jog alóli kivételként egy ilyen kivételt minden esetben megszorítóan kell értelmezni, és arra kell korlátozni, ami egy demokratikus társadalomban szükséges és arányos, a törvénynek pedig világosan meg kell határoznia a feltételeket és biztosítékokat e korlátozás jogossá tétele érdekében; mivel az Egyesült Államoknak és az Uniónak, elsősorban a Bizottságnak pontosan meg kellett volna határoznia az ilyen kivétel alkalmazási körét az olyan értelmezés vagy végrehajtás elkerülése érdekében, amely érdemben semmissé teszi a többek között a magánélet és az adatok védelméhez való alapvető jogot; mivel következésképpen e kivételt nem szabad olyan módon alkalmazni, hogy az veszélyeztesse vagy semmissé tegye az Alapjogi Charta, az EJEE, az uniós adatvédelmi jogszabályok és a védett adatkikötőre vonatkozó elvek által biztosított védelmet; kitart amellett, hogy a nemzetbiztonsági kivételre való hivatkozás esetén meg kell határozni, hogy az pontosan melyik nemzeti jogszabályon alapul;

AQ. mivel az egyesült államokbeli hírszerző ügynökségek széles körű hozzáférése súlyosan gyengítette a transzatlanti bizalmat, és kedvezőtlenül befolyásolta az Unióban tevékenykedő egyesült államokbeli szervezetek iránti bizalmat; mivel mindezt tovább súlyosbítja, hogy az Egyesült Államok joga nem biztosít bírósági és közigazgatási jogorvoslatot az uniós polgárok számára, különösen a hírszerzés céljából végzett megfigyelési tevékenységek esetében;

Harmadik országokba történő adattovábbítás a megfelelőségi határozat alapján

AR. mivel a feltárt információk és a LIBE bizottság által végzett vizsgálat megállapításai alapján az új-zélandi, kanadai és ausztrál nemzetbiztonsági ügynökségek közreműködtek az elektronikus közlések nagyszabású, tömeges megfigyelésében, valamint aktívan együttműködtek az Egyesült Államokkal az úgynevezett „Öt szem" (Five Eyes) program keretében, és az is lehetséges, hogy kicserélték egymás között az uniós polgárok Unióból továbbított egyéb személyes adatait;

AS. mivel a 2013/65/EU bizottsági határozat ([1]) és a 2002/2/EK bizottsági határozat ([2]) kinyilvánította az új-zélandi adatvédelmi törvény és a személyes információk védelméről és az elektronikus dokumentumokról szóló kanadai törvény által biztosított védelmi szint megfelelőségét; mivel a fent említett feltárt információk egyúttal súlyosan befolyásolják az ezen országok jogrendszerébe vetett bizalmat az uniós polgárok számára biztosított védelem folytonosságát illetően; mivel a Bizottság ezt a szempontot nem vizsgálta;

Szerződési feltételeken és egyéb megállapodásokon alapuló adattovábbítás

AT. mivel az 95/46/EK irányelv kimondja, hogy egy harmadik országba irányuló adattovábbítás egyedi megállapodások alapján is megvalósulhat, amennyiben az adatkezelő megfelelő garanciákat teremt az egyének magánéletének, alapvető jogainak és szabadságainak védelme, valamint a kapcsolódó jogok gyakorlása tekintetében;

AU. mivel ilyen garanciákat jelenthetnek különösen a megfelelő szerződési feltételek;

AV. mivel a 95/46/EK irányelv felhatalmazza a Bizottságot annak megállapítására, hogy egyes általános szerződési feltételek megfelelő biztosítékot nyújtanak az irányelvben előírtak szerint, és mivel a Bizottság ennek alapján az általános szerződési feltételek három mintáját fogadta el a harmadik országbeli adatkezelőknek és adatfeldolgozóknak (és további feldolgozóknak) való adattovábbításra vonatkozóan;

AW. mivel az általános szerződési feltételeket megállapító bizottsági határozatok kimondják, hogy az illetékes tagállami hatóságok élhetnek azzal a jogukkal, hogy felfüggesztik az adattovábbítást olyan esetekben, ha megállapítást nyer, hogy az adatátvevőre vagy a további feldolgozóra irányadó jog olyan követelményeket támaszt vele szemben, amelyek értelmében el kell térnie az alkalmazandó adatvédelmi jogtól, valamint amelyek a 95/46/EK irányelv 13. cikkében foglalt, a demokratikus társadalomban szükséges korlátozásokat túllépik, és amennyiben ezek a követelmények vélhetően jelentős hátrányos hatással lesznek az alkalmazandó adatvédelmi jog és az általános szerződési feltételek által nyújtott garanciákra, vagy ha nagy a valószínűsége annak, hogy a mellékletben szereplő általános szerződési feltételeknek nem tesznek eleget vagy nem fognak eleget tenni, és az adattovábbítás folytatása az érintettek súlyos károsodásának közvetlen veszélyével járna;

AX. mivel a nemzeti adatvédelmi hatóságok kötelező erejű vállalati szabályokat (BCR) dolgoztak ki annak érdekében, hogy elősegítsék a nemzetközi adattovábbítást a multinacionális vállalatokon belül, megfelelő biztosítékok kíséretében az egyének magánéletének, alapvető jogainak és szabadságainak védelme, valamint a kapcsolódó jogok gyakorlása tekintetében; mivel alkalmazásukat megelőzően a kötelező erejű vállalati szabályokat a tagállamok illetékes hatóságainak kell engedélyezniük, miután e hatóságok értékelték az uniós adatvédelmi jogszabályoknak való megfelelőségüket; mivel a LIBE bizottság általános adatvédelmi rendeletről szóló jelentése elutasította az adatfeldolgozókra vonatkozó kötelező erejű vállalati szabályokat, mivel azok nyomán az adatkezelőnek és az érintettnek semmilyen beleszólása nem lenne abba, hogy adatait mely joghatóságon belül dolgozzák fel;

([1]) HL L 28., 2013.1.30., 12. o.
([2]) HL L 2., 2002.1.4., 13. o.

2014. március 12., szerda

AY. mivel az Európai Parlament az EUMSZ 218. cikke által előírt hatásköre alapján köteles folyamatosan nyomon követni azon nemzetközi megállapodások értékét, amelyekhez hozzájárulását adta;

Adattovábbítás a terrorizmus finanszírozásának felderítését célzó programról (TFTP) és az utas-nyilvántartási adatállományról (PNR) szóló megállapodások alapján

AZ. mivel 2013. október 23-i állásfoglalásában a Parlament komoly aggodalmának adott hangot az NSA által végzett, a nemzetközi fizetési üzenetekhez és a kapcsolódó adatokhoz való közvetlen hozzáféréshez fűződő tevékenységekről feltárt információk miatt, ami a TFTP-megállapodás egyértelmű megsértésének minősülne, különös tekintettel annak 1. cikkére;

BA. mivel a terrorizmus finanszírozásának felderítése olyan létfontosságú eszköz a terrorizmus finanszírozása és a súlyos bűncselekmények elleni küzdelemben, amely lehetővé teszi, hogy a terrorizmus elleni küzdelemmel foglalkozó nyomozók felderítsék a célszemélyek és más, gyaníthatóan a terrorizmust finanszírozó szélesebb terroristahálózatokkal kapcsolatban álló lehetséges gyanúsítottak közötti kapcsolatokat;

BB. mivel a Parlament felkérte a Bizottságot a megállapodás felfüggesztésére, és kérte, hogy a parlamenti tanácskozáshoz valamennyi vonatkozó információt és dokumentumot haladéktalanul bocsássák rendelkezésére; mivel a Bizottság egyik kérést sem teljesítette;

BC. mivel a médiában megjelent állításokat követően a Bizottság úgy határozott, hogy a TFTP-megállapodás 19. cikke értelmében konzultációt indít az Egyesült Államokkal; mivel 2013. november 27-én Malström biztos arról tájékoztatta a LIBE bizottságot, hogy az egyesült államokbeli hatóságok képviselőivel tartott találkozókat követően, valamint az egyesült államokbeli hatóságok részéről a leveleikben és a találkozók során adott válaszok tükrében a Bizottság úgy határozott, hogy nem folytatja a konzultációkat azon okból kifolyólag, hogy nem került sor arra utaló elemek feltárására, hogy az Egyesült Államok kormánya a megállapodásban foglalt rendelkezésekkel ellentétes módon járt volna el, és az Egyesült Államok írásban is megerősítette, hogy nem valósult meg a TFTP-megállapodás rendelkezéseivel ellentétes közvetlen adatgyűjtés; mivel nem egyértelmű, hogy az Egyesült Államok hatóságai az ilyen adatokhoz más módon történő hozzáféréssel – amelyről az Egyesült Államok hatóságai 2013. szeptember 18-i levelükben ([1]) tájékoztattak – megkerülték-e a megállapodást;

BD. mivel a LIBE bizottság küldöttsége 2013. október 28–31-i washingtoni látogatása során a találkozott az Egyesült Államok Pénzügyminisztériumának képviselőivel; mivel az Egyesült Államok Pénzügyminisztériuma kijelentette, hogy a TFTP-megállapodás hatálybalépése óta kizárólag a TFTP keretében rendelkezik hozzáféréssel az uniós SWIFT-adatokhoz; mivel az Egyesült Államok Pénzügyminisztériuma nem volt hajlandó nyilatkozni arra vonatkozóan, hogy bármely más egyesült államokbeli kormányzati szerv vagy minisztérium hozzáférhetett-e a SWIFT-adatokhoz a TFTP keretein kívül, illetve hogy az Egyesült Államok kormányának volt-e tudomása az NSA tömeges megfigyelésre irányuló tevékenységeiről; mivel 2013. december 18-án Glenn Greenwald azt nyilatkozta a LIBE bizottság vizsgálata során, hogy az NSA és a brit Kormányzati Kommunikációs Központ (GCHQ) a SWIFT-hálózatokat vették célba;

BE. mivel a belga és a holland adatvédelmi hatóságok 2013. november 13-án úgy határoztak, hogy közös vizsgálatot folytatnak a SWIFT fizetési hálózatainak biztonságára vonatkozóan annak megállapítása érdekében, hogy harmadik felek jogosulatlanul vagy jogellenesen hozzáférhetnek-e az európai polgárok banki adataihoz ([2]);

BF. mivel az Európai Unió és az Egyesült Államok közötti PNR-megállapodás közös felülvizsgálata szerint az Egyesült Államok Belbiztonsági Minisztériuma (DHS) eseti alapon 23 alkalommal közölt PNR-adatokat a Nemzetbiztonsági Ügynökséggel a terrorizmus elleni harchoz fűződő ügyek alátámasztása érdekében, a megállapodás egyedi feltételeinek megfelelő módon;

BG. mivel a közös felülvizsgálat elmulasztja megemlíteni annak tényét, hogy a személyes adatok hírszerzési céllal történő feldolgozása esetén az egyesült államokbeli törvények értelmében a nem amerikai állampolgároknak nem áll rendelkezésükre bírósági vagy közigazgatási út saját jogaik védelmére, az alkotmányos védelem pedig kizárólag az egyesült államokbeli személyeket illeti meg; mivel az ilyen igazságszolgáltatási vagy közigazgatási jogok hiánya semmissé teszi a hatályos PNR-megállapodásban foglalt, az uniós polgárok védelmére vonatkozó rendelkezéseket;

([1]) A levélben foglaltak szerint „az Egyesült Államok kormánya pénzügyi információkat kutat fel és szerez … [amelyeket] szabályozási, bűnüldözési, diplomáciai és hírszerzési csatornák útján, valamint külföldi partnerekkel folytatott információcsere útján gyűjt”, továbbá „az Egyesült Államok kormánya a TFTP-t a más forrásokból nem megszerezhető SWIFT-adatok megszerzésére alkalmazza”.

([2]) http://www.privacycommission.be/fr/news/les-instances-europ%C3%A9ennes-charg%C3%A9es-de-contr%C3%B4ler-le-respect-de-la-vie-priv%C3%A9e-examinent-la.

2014. március 12., szerda

Adattovábbítás az Európai Unió és az Egyesült Államok közötti kölcsönös bűnügyi jogsegélyről szóló megállapodás alapján

BH. mivel az Európai Unió és az Egyesült Államok közötti kölcsönös bűnügyi jogsegélyről szóló, 2003. június 6-i megállapodás ([1]) 2010. február 1-jén hatályba lépett, és célja az, hogy elősegítse az Európai Unió és az Egyesült Államok közötti együttműködést a hatékonyabb bűnözés elleni küzdelem érdekében, kellő figyelemmel az egyének jogaira és a jogállamiságra;

Adatvédelmi keretmegállapodás a rendőrségi és igazságügyi együttműködés terén („átfogó megállapodás").

BI. mivel ezen általános megállapodás célja a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében a kizárólagosan a bűncselekmények – köztük a terrorcselekmények – megelőzésének, kivizsgálásának, felderítésének és büntetőeljárás lefolytatásának céljából az Unió és az Egyesült Államok között továbbított személyes adatokra vonatkozó jogi keretek kialakítása; mivel a tárgyalásokat a Tanács 2010. december 2-án engedélyezte; mivel ez a megállapodás kiemelkedően fontos, és a rendőrségi és igazságügyi együttműködés keretében, valamint a büntetőügyekkel összefüggésben történő adattovábbítás megkönnyítésének alapjául szolgálna;

BJ. mivel ezen megállapodásnak egyértelmű és részletes, jogilag kötelező érvényű adatfeldolgozási elveket kell megállapítania, és különösen fontos, hogy elismerje az uniós polgároknak a személyes adataikhoz való bírósági hozzáférésre, azok helyesbítésére vagy törlésére vonatkozó jogait az Egyesült Államokban, valamint az uniós polgároknak az Egyesült Államokban egy hatékony közigazgatási és bírósági jogorvoslati mechanizmushoz való jogát, továbbá az adatfeldolgozási tevékenységek független felügyeletét;

BK. mivel 2013. november 27-i közleményében a Bizottság kifejtette, hogy az átfogó megállapodásnak a polgárok magas szintű védelmét kell eredményeznie az Atlanti-óceán mindkét partján, és meg kell erősítenie az európaiak bizalmát az Unió és az Egyesült Államok közötti adatcserék vonatkozásában, alapot szolgáltatva az Unió és az Egyesült Államok közötti biztonsági együttműködés és partnerség továbbfejlesztéséhez;

BL. mivel a megállapodásról szóló tárgyalásokban nem történt előrelépés, mert az Egyesült Államok kormánya kitartóan ragaszkodik álláspontjához, miszerint nem hajlandó elismerni az uniós polgárok hatékony közigazgatási és bírósági jogorvoslathoz való jogát, és mert széles körben eltéréseket kíván biztosítani a megállapodásban foglalt adatvédelmi elvektől, így például a célhoz kötöttségre, az adatmegőrzésre, illetve belföldi vagy külföldi viszonylatban a harmadik fél részére történő adattovábbításra vonatkozó elvektől;

Adatvédelmi reform

BM. mivel az uniós adatvédelmi jogi keretrendszer jelenleg felülvizsgálat alatt áll az Unióban történő valamennyi adatfeldolgozási tevékenységre vonatkozó átfogó, következetes, modern és szilárd rendszer kialakítása érdekében; mivel a Bizottság 2012 januárjában jogalkotási javaslatcsomagot terjesztett elő: egy általános adatvédelmi rendeletet ([2]), amely a 95/46/EK irányelv helyébe lép majd és Unió-szerte egységes jogot teremt, valamint egy irányelvet ([3]), amely harmonizálja a bűnüldöző hatóságok által bűnüldözés céljából végzett valamennyi adatfeldolgozási tevékenység kereteit, és csökkenti a nemzeti jogszabályok között jelenleg fennálló különbségeket;

BN. mivel a LIBE bizottság 2013. október 21-én elfogadta a két javaslatról szóló jogalkotási jelentéseit, és határozatot hozott a Tanáccsal folytatott tárgyalások megnyitásáról azzal a céllal, hogy a jogszabályok elfogadására még a jelenlegi jogalkotási ciklusban sor kerüljön;

BO. mivel jóllehet a 2013. október 24–25-i Európai Tanács felhívott egy erős, általános uniós adatvédelmi keretrendszer elfogadására a polgárok és a vállalkozások digitális gazdaság iránti bizalmának előmozdítása érdekében, a Tanácsnak két év tanácskozás után még mindig nem sikerült általános megközelítést elfogadnia az általános adatvédelmi rendeletre és az irányelvre vonatkozóan ([4]);

([1]) HL L 181., 2003.7.19., 25. o.
([2]) COM(2012)0011, 2012.1.25.
([3]) COM(2012)0010, 2012.1.25.
([4]) http://register.consilium.europa.eu/pdf/hu/13/st00/st00169.hu13.pdf.

2014. március 12., szerda

Az informatikai biztonság és a számítási felhő

BP. mivel a Parlament fent említett, 2013. december 10-i állásfoglalása hangsúlyozza a számítási felhőre épülő üzletágban rejlő gazdasági lehetőségeket a növekedés és a foglalkoztatás szempontjából; mivel az előrejelzések szerint a felhőalapú piac értéke 2016-ra eléri az évi 207 milliárd USD-t, azaz értéke 2012-höz képest megduplázódik;

BQ. mivel a felhőalapú számítástechnikai környezetben az adatvédelem szintje nem lehet alacsonyabb a más adatfeldolgozási módok vonatkozásában előírtaknál; mivel az uniós adatvédelmi jog – tekintve, hogy az technológiailag semleges – jelenleg is teljes körűen alkalmazandó az Unióban működő számításifelhő-szolgáltatásokra;

BR. mivel a tömeges megfigyelésre irányuló tevékenységek hozzáférést biztosítanak a hírszerző ügynökségek számára az uniós egyének által a legnagyobb egyesült államokbeli számításifelhő-szolgáltatókkal kötött, számításifelhő-szolgáltatásokra vonatkozó megállapodások alapján tárolt vagy más módon feldolgozott személyes adatokhoz; mivel az egyesült államokbeli hírszerző hatóságok már hozzáfértek az Unió területén található szervereken tárolt vagy más módon feldolgozott személyes adatokhoz azáltal, hogy behatoltak a Yahoo és a Google belső hálózatába; mivel az ilyen tevékenységek sértik a nemzetközi kötelezettségeket és az európai alapjogi normákat, többek közt a magán- és családi élethez való jogot, a közlések titkosságát, az ártatlanság vélelmét, a szólásszabadságot, az információszabadságot, a gyülekezési és egyesülési szabadságot, valamint a vállalkozás szabadságát; mivel nem kizárt, hogy a hírszerző hatóságok a tagállami hatóságok, vállalkozások és intézmények által a számításifelhő-szolgáltatásokban tárolt információkhoz is hozzáfértek;

BS. mivel az egyesült államokbeli hírszerző ügynökségek szisztematikusan gyengítik a titkosítási protokollokat és termékeket, hogy még a titkosított közléseket is le tudják hallgatni; mivel az Egyesült Államok Nemzetbiztonsági Ügynöksége nagyszámú úgynevezett „nulladik napi exploitot”, azaz olyan informatikai biztonsági sérülékenységeket gyűjtött össze, amely a nyilvánosság vagy a termék eladója számára még nem ismert; mivel ezek a tevékenységek számottevően aláássák az informatikai biztonság javítására irányuló globális erőfeszítéseket;

BT. mivel az a tény, hogy a hírszerző ügynökségek online szolgáltatásokat igénybe vevő felhasználók személyes adataihoz fértek hozzá, súlyosan torzította a polgárok ilyen szolgáltatások iránti bizalmát, és ezért kedvezőtlen hatást gyakorol az „óriási méretű adathalmazokat” és az új alkalmazásokat, például a „tárgyak internetét” használó új szolgáltatások fejlesztésébe befektető vállalkozásokra;

BU. mivel az informatikai eszközök értékesítői gyakran olyan termékeket kínálnak, amelyeket az informatikai biztonság szempontjából nem vizsgáltak meg megfelelően, illetve amelyekbe bizonyos esetekben az értékesítő szándékosan úgynevezett „hátsó ajtó” (backdoor) programot is telepített; mivel a szoftverértékesítőkre vonatkozó felelősségi szabályok hiánya olyan helyzetet teremtett, amelyet a hírszerző ügynökségek is kihasználnak, egyúttal azonban más szervezetektől érkező támadások kockázatát is felveti;

BV. mivel a polgárok fokozott bizalmának fenntartása érdekében elengedhetetlen, hogy az ilyen új szolgáltatásokat és alkalmazásokat kínáló vállalatok tiszteletben tartsák az adatvédelmi szabályokat és az adatgyűjtés, -feldolgozás és -elemzés tárgyát képező érintettek magánéletét;

A hírszerző szolgálatok demokratikus felügyelete

BW. mivel a demokratikus társadalmakban a hírszerző szolgálatokat különleges jogokkal és képességekkel ruházzák fel az alapvető jogok, a demokrácia és a jogállamiság, a polgári jogok és az állam súlyos belső és külső fenyegetésekkel szembeni védelmezése érdekében, valamint e szolgálatok demokratikusan elszámoltathatók és bírói felügyelet alatt állnak; mivel kizárólag e célból ruházzák fel őket különleges jogokkal és képességekkel; mivel e jogokat kizárólag az alapvető jogok, a demokrácia és a jogállamiság által megszabott jogi korlátok között kell gyakorolni, és alkalmazásukat szigorúan ellenőrizni kell, mivel másként elvesztik legitimitásukat és a demokráciát veszélyeztethetik;

BX. mivel az a tény, hogy a hírszerző szolgálatok számára bizonyos fokú titoktartást engedélyeznek – ami ahhoz szükséges, hogy elkerüljék a folyamatban lévő műveletek veszélyeztetését, a működési módok feltárását vagy az ügynökök életének kockáztatását – nem igazolja, hogy az ilyen titoktartás felülírja vagy kizárja a tevékenységeik demokratikus vagy bírói ellenőrzésére és vizsgálatára, valamint a többek között az alapvető jogokkal, a demokráciával és a jogállamisággal összefüggésben az átláthatóságra vonatkozó szabályokat, amelyek mind a demokratikus társadalom sarokköveit képezik;

BY. mivel a meglévő nemzeti felügyeleti mechanizmusok és szervek többségét az 1990-es években hozták létre vagy alakították át, és azokat nem feltétlenül igazították az elmúlt évtizedben végbement gyors politikai és technológiai fejlődéshez, amely – többek közt a személyes adatok tömeges cseréje által – fokozott nemzetközi hírszerzési együttműködéshez, és gyakran a hírszerzési és a bűnüldözési tevékenység közötti határvonal elmosódásához vezetett;

BZ. mivel a hírszerzési tevékenység demokratikus felügyelete továbbra is csak nemzeti szinten valósul meg annak ellenére, hogy egyre fokozódik az információcsere az uniós tagállamok, valamint a tagállamok és harmadik országok között; mivel egyre növekszik a szakadék egyrészről a nemzetközi együttműködés szintje, másrészről pedig a nemzeti szintre korlátozódó felügyeleti képességek között, ami elégtelen és csekély hatékonyságú demokratikus ellenőrzéshez vezet;

CA. mivel a nemzeti felügyeleti szervek gyakran nem férnek hozzá teljes körűen a külföldi hírszerző ügynökségtől kapott információkhoz, aminek nyomán olyan rések keletkezhetnek, amelyek megfelelő ellenőrzés nélkül teszik lehetővé az információk nemzetközi cseréjét; mivel ezt a problémát tovább súlyosbítja az úgynevezett „harmadik felekre vonatkozó szabály", illetve az „átadó fél általi ellenőrzés" elve, amelynek célja annak lehetővé tétele, hogy az átadó fél tartsa fent az ellenőrzést saját érzékeny információinak további terjesztése felett, ezt azonban sajnos gyakran úgy értelmezik, hogy a fogadó fél szolgálatai általi felügyeletre is vonatkozik;

CB. mivel a magán- és a közszféra átláthatóságának reformjára irányuló kezdeményezések kulcsszerepet játszanak a hírszerző ügynökségek tevékenységei iránti lakossági bizalom biztosításában; mivel a jogrendszerek nem akadályozhatják meg, hogy a vállalatok nyilvánosságra hozzák a felhasználói adatokhoz való hozzáférésre irányuló, valamennyi típusú kormányzati kérelem és bírósági határozat kezelésének módjára vonatkozó információkat, ideértve a jóváhagyott és az elutasított kérelmek és határozatok számára vonatkozó összesített információk közzétételének lehetőségét;

Főbb megállapítások

1. úgy véli, hogy a visszaélést jelentő személyek és az újságírók által a közelmúltban a sajtóban felfedett információk az e vizsgálat során szerzett szakértői bizonyítékokkal, egyes hatóságok beismeréseivel, valamint az állításokra vonatkozó kielégítő válaszok hiányával együtt meggyőző bizonyítékkal szolgálnak olyan kiterjedt, bonyolult és technológiailag magasan fejlett rendszerek létezésére, amelyeket az Egyesült Államok és egyes tagállamok hírszerző szolgálatai alakítottak ki annak érdekében, hogy példátlan nagyságrendben, válogatás nélkül és nem gyanúra alapozva összegyűjtsék, tárolják és elemezzék világszerte valamennyi polgár közléseit, köztük tartalmi adatokat, helymeghatározó adatokat és metaadatokat;

2. rámutat különösen az egyesült államokbeli NSA hírszerzési programjaira, amelyek lehetővé teszik az uniós polgárok tömeges megfigyelését az alábbiak révén: közvetlen hozzáférés az egyesült államokbeli vezető internetes társaságok központi szervereihez (PRISM program), a tartalmak és metaadatok elemzése (Xkeyscore program), az online adattitkosítás megkerülése (BULLRUN), a számítógépes és telefonos hálózatokhoz és a helymeghatározó adatokhoz, valamint a GCHQ egyesült királyságbeli hírszerző ügynökség rendszereihez, így például az üvegszálas kábeleken áramló adatokra irányuló („upstream") megfigyelési tevékenységhez (Tempora program) való hozzáférés, a dekódoló/titkosítást visszafejtő program (Edgehill), az információs rendszerek elleni célzott közbeékelődéses támadások (Quantumtheory és Foxacid programok) és napi 200 millió szöveges üzenet gyűjtése és megőrzése (Dishfire program);

3. felhívja a figyelmet az arra vonatkozó állításokra, hogy a GCHQ egyesült királyságbeli hírszerző ügynökség „feltörte" a Belgacom rendszereit, illetve azokba behatolt; tudomásul veszi a Belgacom kijelentéseit, miszerint sem megerősíteni, sem cáfolni nem tudja, hogy ez az uniós intézményeket célozta vagy érintette, az alkalmazott rosszindulatú szoftver pedig rendkívül összetett volt: kifejlesztése és használata olyan kiterjedt pénzügyi és személyi erőforrásokat igényel, amelyek nem állnak magánszervezetek vagy hackerek rendelkezésére;

4. hangsúlyozza, hogy alapjaiban megrendült a bizalom: a két transzatlanti partner közötti bizalom, a polgárok és kormányaik közötti bizalom, a demokratikus intézmények működésébe vetett bizalom az Atlanti-óceán mindkét partján, a jogállamiság tiszteletben tartásába vetett bizalom, valamint az informatikai szolgáltatások és kommunikáció biztonságába vetett bizalom; úgy véli, hogy bizalom valamennyi említett dimenziójának újjáépítése érdekében haladéktalanul szükség van egy intézkedések sorozatát tartalmazó és szükség esetén nyilvánosság általi ellenőrzésnek alávetett átfogó reagálási tervre;

5. megjegyzi, hogy több kormányzat is azt állítja, hogy e tömeges megfigyelési programokra szükség van a terrorizmus elleni küzdelem érdekében; erőteljesen elítéli a terrorizmust, azonban határozottan úgy véli, hogy a terrorizmus elleni küzdelem sosem indokolhatja a nem célirányos, titkos vagy egyenesen jogellenes tömeges megfigyelési programokat; úgy véli, hogy az ilyen programok egy demokratikus társadalomban összeegyeztethetetlenek a szükségesség és arányosság elveivel;

2014. március 12., szerda

6. emlékeztet arra, hogy az Unió szilárdan hisz abban, hogy szükség van a biztonsági intézkedések és a polgári szabadságjogok és az alapvető jogok védelme közötti megfelelő egyensúly megteremtésére, a magánélet és az adatvédelem legteljesebb tiszteletben tartása mellett;

7. úgy véli, hogy egy ilyen nagyságrendű adatgyűjtés komoly kétségeket vet fel azzal kapcsolatban, hogy e tevékenységet pusztán a terrorizmus elleni küzdelem vezérli-e, mivel valamennyi polgárról minden lehetséges adat összegyűjtésével jár; rámutat ezért egyéb célok – többek között a politikai és a gazdasági kémkedés – esetleges létezésére, melyeket minden részletre kiterjedően fel kell számolni;

8. megkérdőjelezi egyes tagállamok kiterjedt gazdasági kémkedési tevékenységeinek összeegyeztethetőségét az Európai Unió működéséről szóló szerződés I. és VII. címében foglaltak szerinti uniós belső piaccal és versenyjoggal; ismét megerősíti az Európai Unióról szóló szerződés 4. cikkének (3) bekezdésében foglalt lojális együttműködés elvét, valamint azt az elvet, miszerint a tagállamok „tartózkodnak minden olyan intézkedéstől, amely veszélyeztetheti az Unió célkitűzéseinek megvalósítását”;

9. megjegyzi, hogy a nemzetközi szerződéseknek, az uniós és egyesült államokbeli jogszabályoknak, valamint a nemzeti felügyeleti mechanizmusoknak nem sikerült biztosítaniuk a megfelelő fékeket és ellensúlyokat, illetve a demokratikus elszámoltathatóságot;

10. elítéli ártatlan emberek személyes adatainak nagyszabású, rendszerszerű és átfogó összegyűjtését, amely gyakran bizalmas személyes információkra is kiterjed; hangsúlyozza, hogy a hírszerző szolgálatok által alkalmazott tömeges és válogatás nélküli megfigyelésre szolgáló rendszerek súlyos beavatkozást jelentenek a polgárok alapvető jogaiba; hangsúlyozza, hogy a magánélethez való jog nem luxusjog, hanem a szabad és demokratikus társadalom alapköve; rámutat továbbá arra, hogy a tömeges megfigyelés potenciálisan súlyosan kihat a sajtószabadságra, a gondolat- és szólásszabadságra, valamint a gyülekezés és az egyesülés szabadságára, valamint magában hordozza az összegyűjtött információk politikai ellenfelekkel szembeni visszaélésszerű felhasználásának komoly lehetőségét; hangsúlyozza, hogy e tömeges megfigyelési tevékenységek a hírszerző ügynökségek részéről jogellenes fellépéseket is magukban foglalnak, és a nemzeti jogszabályok területen kívüli hatályát érintő kérdéseket vetnek fel;

11. alapevő fontosságúnak tartja az ügyvédekre, újságírókra, orvosokra és más szabályozott szakmákra vonatkozó szakmai titoktartási kötelezettség védelmét a tömeges megfigyelési tevékenységekkel szemben; hangsúlyozza különösen, hogy az ügyvédek és ügyfeleik közötti kommunikáció bizalmasságával kapcsolatos bármely bizonytalanság hátrányosan érintheti az uniós polgárok jogi tanácsadáshoz és az igazságszolgáltatáshoz való hozzáféréshez, valamint tisztességes eljáráshoz való jogát;

12. meglátása szerint a megfigyelési programok újabb lépést jelentenek az alábbi eredményekhez vezető úton: egy önálló preventív állam kialakítása, a büntetőjog bevett paradigmájának megváltoztatása a demokratikus társadalmakban, amelynek értelmében a gyanúsítottak alapvető jogaiba való minden beavatkozáshoz alapos gyanún alapuló bírói vagy ügyészi engedély szükséges, és azt jogilag szabályozni kell, ehelyett pedig a bűnüldözés és a hírszerzési tevékenységek egyfajta kombinációjának előmozdítása homályos és meggyengült jogi garanciákkal, ami gyakran nem áll összhangban a demokratikus fékek és ellensúlyok kívánalmával és az alapvető jogokkal, különös tekintettel az ártatlanság vélelmére; e tekintetben emlékeztet arra, hogy a Német Szövetségi Alkotmánybíróság ítéletében ([1]) megállapította a preventív adatbányászat („präventive Rasterfahndung”) alkalmazásának tilalmát, azon esetek kivételével, amikor igazolható egyéb kiemelten fontos és jogi védelemben részesülő jogok konkrét fenyegetettsége, általános fenyegetettség vagy nemzetközi feszültségek azonban nem elegendőek ilyen intézkedések igazolásához;

13. kitart amellett, hogy a titkos jogszabályok és bíróságok sértik a jogállamiságot; rámutat arra, hogy egy Unión kívüli ország bírósága vagy törvényszéke által hozott ítélet és közigazgatási hatósága által hozott határozat, amely – közvetlen vagy közvetett módon – engedélyezi személyes adatok továbbítását, semmilyen módon nem ismerhető el vagy hajtható végre, kivéve ha a kérelmező harmadik ország és az Unió vagy valamely tagállama között kölcsönös jogsegélyről szóló szerződés vagy nemzetközi megállapodás van hatályban, valamint az illetékes ellenőrző hatóság előzetes engedélyt adott; emlékeztet arra, hogy egy Unión kívüli ország titkos bírósága vagy törvényszéke által hozott ítélet és közigazgatási hatósága által hozott határozat, amely – közvetlen vagy közvetett módon – titokban engedélyez megfigyelési tevékenységeket, nem ismerhető el vagy hajtható végre;

([1]) 1 BvR 518/02, 2006. április 4.

14. rámutat arra, hogy a fent említett aggályokat tovább súlyosbítják a gyors technológiai és társadalmi fejlemények, hiszen az internet és a mobil eszközök mindenütt jelen vannak a modern mindennapi életben („helyfüggetlen számítástechnika"), az internetes társaságok többségének üzleti modellje pedig a személyes adatok feldolgozásán alapul; úgy véli, hogy a probléma nagyságrendje példa nélküli; megjegyzi, hogy ez olyan helyzetet teremthet, amelyben a politikai rendszer változása esetén lehetőség nyílik a tömeges adatgyűjtésre és -feldolgozásra használt infrastruktúrával való visszaélésre;

15. megjegyzi, hogy sem az uniós közintézmények, sem pedig a polgárok számára nincs garancia arra, hogy informatikai biztonságuk vagy személyes adataik megvédhetők a jól felszerelt behatolók támadásaival szemben („nem létezik 100 %-os informatikai biztonság"); megjegyzi, hogy a maximális informatikai biztonság elérése érdekében az európai polgároknak hajlandóságot kell mutatniuk arra, hogy az informatika területén elegendő – emberi és pénzügyi – erőforrást fordítsanak Európa függetlenségének és önállóságának megőrzésére;

16. határozottan elutasítja azt az elképzelést, hogy a tömeges megfigyelési programokhoz kapcsolódóan minden esetben pusztán nemzetbiztonsági kérdésekről van szó, így azok a tagállamok kizárólagos hatáskörébe tartoznak; ismételten hangsúlyozza, hogy a tagállamoknak nemzetbiztonságuk védelmében eljárva teljes mértékben tiszteletben kell tartaniuk az uniós jogot és az EJEE-t; emlékeztet az Európai Bíróság közelmúltbeli ítéletére, amely kimondja, hogy „jóllehet a tagállamok feladata a saját belső és külső biztonságuk biztosítását szolgáló intézkedések meghozatala, nem eredményezheti az uniós jog alkalmazhatatlanságát pusztán az, hogy valamely határozat a nemzetbiztonságot érinti" ([1]); továbbá emlékeztet arra, hogy ez esetben valamennyi uniós polgár magánéletének védelme, valamint az összes uniós kommunikációs hálózat biztonsága és megbízhatósága forog kockán; ezért úgy véli, hogy az uniós szintű vita és fellépés nemcsak jogos, hanem egyenesen az Unió autonómiáját érintő kérdés;

17. elismeréssel adózik az e vizsgálathoz hozzájáruló intézmények és szakértők előtt; kifogásolja annak tényét, hogy több tagállam hatósága visszautasította az Európai Parlament által a polgárok nevében végzett vizsgálat keretében való együttműködést; üdvözli számos kongresszusi és nemzeti parlamenti képviselő nyitottságát;

18. tudatában van annak, hogy a rendelkezésre álló korlátozott időben 2013 júliusa óta csupán arra nyílt lehetőség, hogy elvégezzék a szóban forgó valamennyi kérdés előzetes vizsgálatát; elismeri a közölt információk horderejét és feltárásuk folytatólagos jellegét; ezért egy jövőbe tekintő megközelítést fogad el, amely egyedi javaslatokat foglal magában, valamint egy mechanizmust a következő parlamenti ciklusban végzett nyomon követés érdekében, ezáltal folyamatosan biztosítva a megállapítások kiemelt helyét az Unió politikai napirendjén;

19. szándékában áll, hogy határozott politikai kötelezettségvállalásokat kérjen a 2014. májusi választásokat követően megválasztandó új Európai Bizottságtól e vizsgálat javaslatainak és ajánlásainak végrehajtására vonatkozóan;

Ajánlások

20. felhívja az Egyesült Államok hatóságait és az uniós tagállamokat, hogy – ha ez még nem történt meg – tiltsák be az átfogó tömeges megfigyelési tevékenységeket;

21. felszólítja az uniós tagállamokat, és különösen az úgynevezett „Kilenc szem" (9-eyes) és „Tizennégy szem" (14-eyes) programokban ([2]) részt vevő országokat, hogy átfogóan értékeljék és adott esetben vizsgálják felül a hírszerző szolgálatok tevékenységeire irányadó nemzeti jogszabályaikat és gyakorlataikat annak biztosítása érdekében, hogy azok parlamenti és bírósági felügyelet, valamint a nyilvánosság felügyelete alatt álljanak, hogy tiszteletben tartsák a törvényesség, a szükségesség, az arányosság, a tisztességes eljárás, a felhasználó értesítése és az átláthatóság elvét, többek közt utalva az ENSZ bevált gyakorlatokat ismertető gyűjteményére és a Velencei Bizottság ajánlásaira, valamint hogy legyenek összhangban az Emberi Jogok Európai Egyezményében foglalt normákkal és feleljenek meg a tagállamok alapvető jogokkal kapcsolatos kötelezettségeinek, különösen az adatvédelem, a magánélet védelme és az ártatlanság vélelme tekintetében;

([1]) A C-300/11. sz. ZZ kontra Secretary of State for the Home Department ügyben hozott, 2013. június 4-i ítélet.

([2]) A „9 szem" program az Egyesült Államokat, az Egyesült Királyságot, Kanadát, Ausztráliát, Új-Zélandot, Dániát, Franciaországot, Norvégiát és Hollandiát foglalja magában; a „14 szem" program résztvevői az előbbi országok, továbbá Németország, Belgium, Olaszország, Spanyolország és Svédország.

2014. március 12., szerda

22. felhívja az uniós tagállamokat és – tekintettel 2013. július 4-i állásfoglalására és a vizsgálata során lefolytatott meghallgatásokra – különösen az Egyesült Királyságot, Franciaországot, Németországot, Svédországot, Hollandiát és Lengyelországot, hogy biztosítsák a hírszerző ügynökségeik tevékenységét szabályozó meglévő, illetve jövőbeli jogi keretrendszereik és felügyeleti mechanizmusaik összhangját az Emberi Jogok Európai Egyezményével és az uniós adatvédelmi joggal; felhívja ezeket a tagállamokat, hogy adjanak magyarázatot a tömeges megfigyelési tevékenységgel – többek közt a határokon átnyúló kommunikáció tömeges megfigyelésével, a kábelen továbbított kommunikáció nem célzott megfigyelésével, a hírszerző ügynökségek és a hírközlési vállalkozások között a személyes adatokhoz és a transzatlanti kábelekhez, az Egyesült Államok hírszerzési személyzetéhez és az Unió területén található berendezéseihez való, a megfigyelési tevékenység felügyelete nélküli hozzáférésre, illetve ezek cseréjére vonatkozó esetleges megállapodásokkal – kapcsolatos állításokra, illetve arra, hogy ezek az uniós joggal miként egyeztethetők össze; kéri ezen országok nemzeti parlamentjeit, hogy fokozzák a hírszerzési felügyeleti szerveik közötti európai szintű együttműködést;

23. kéri különösen az Egyesült Királyságot, hogy tekintettel a GCHQ hírszerző szolgálat általi tömeges megfigyelésről szóló kiterjedt médiabeszámolókra, vizsgálja felül a hatályos jogi keretet, amely három különálló jogszabály – az emberi jogokról szóló 1998. évi törvény, a hírszerző szolgálatokról szóló 1994. évi törvény és a vizsgálati hatáskörök szabályozásáról szóló 2000. évi törvény – „komplex kölcsönhatásából" tevődik össze;

24. tudomásul veszi a 2002. évi holland hírszerzési és biztonsági törvény felülvizsgálatát (a „Dessens Bizottság" 2013. december 2-i jelentése); támogatja a felülvizsgálati bizottság azon ajánlásait, amelyek célja a holland hírszerző szolgálatok átláthatóságának, valamint ellenőrzésének és felügyeletének megerősítése; felszólítja Hollandiát, hogy tartózkodjon a hírszerző szolgálatok jogköreinek olyan módon történő kibővítésétől, amelynek alapján az ártatlan polgárok kábel útján továbbított kommunikációját nem célirányos és nagyszabású megfigyelés alá lehetne vonni, különös tekintettel arra, hogy a világ egyik legnagyobb internetcsatlakozási pontja (AMS-IX.) Amszterdamban található; óvatosságra int a rádióelektronikai felderítésért felelős új számítógépes csoport (Joint Sigint Cyber Unit) megbízatásának és képességeinek meghatározásakor, valamint óvatosságra int az amerikai hírszerzési alkalmazottak holland területen való tartózkodásának és tevékenységének engedélyezése tekintetében;

25. felszólítja a tagállamokat, többek között az őket képviselő hírszerző ügynökségeket is, hogy tartózkodjanak a jogszerűtlenül gyűjtött, harmadik államtól érkező adatok fogadásától, valamint a területükön belül olyan, harmadik állam kormányzata vagy ügynökségei által végzett megfigyelési tevékenységek megengedésétől, amelyek a nemzeti törvények alapján jogellenesek vagy nem felelnek meg a nemzetközi vagy uniós okmányokban rögzített jogi biztosítékoknak, ideértve az emberi jogok védelmét is az EUSZ, az EJEE és az Európai Unió Alapjogi Chartája értelmében;

26. felszólítja valamennyi titkosszolgálatot, hogy hagyjanak fel a tömeges lehallgatással és a webkamerák felvételeinek feldolgozásával; felszólítja a tagállamokat annak teljes körű kivizsgálására, hogy a saját titkosszolgálatuk részt vett-e, hogyan és milyen mértékben vett részt a webkamerák felvételeinek összegyűjtésében és feldolgozásában, valamint felszólítja őket az összes tárolt, az ilyen tömeges megfigyelési programokon keresztül gyűjtött felvételek megsemmisítésére;

27. felszólítja a tagállamokat, hogy haladéktalanul tegyenek eleget az Emberi Jogok Európai Egyezménye alapján fennálló, arra irányuló pozitív kötelezettségüknek, hogy megvédik polgáraikat az egyezményben foglalt követelményekkel ellentétes, harmadik államok vagy saját hírszerző szolgálataik által végzett megfigyeléstől – ideértve azon eseteket is, amikor annak célja a nemzetbiztonság védelme –, és gondoskodjanak arról, hogy a jogállamiság ne gyengüljön egy harmadik ország jogának területen kívüli alkalmazása következtében;

28. felkéri az Európa Tanács főtitkárát, hogy indítsa el az 52. cikk szerinti eljárást, amelynek értelmében „az Európa Tanács Főtitkára által előterjesztett megkeresésre minden Magas Szerződő Fél tájékoztatást ad arról a módról, ahogy belső joga biztosítja a jelen Egyezmény rendelkezéseinek hatékony végrehajtását.";

29. felszólítja a tagállamokat, hogy haladéktalanul hozzanak megfelelő intézkedéseket – a bírósági eljárásokat is ideértve – szuverenitásuk megsértésével, ezáltal pedig az általános nemzetközi közjog megsértésével szemben, amelyeket a tömeges megfigyelésre irányuló programok alkalmazásával követnek el; továbbá felkéri a tagállamokat, hogy az uniós polgárok alapvető jogainak védelme érdekében vegyék igénybe az összes rendelkezésre álló nemzetközi eszközt, nevezetesen a Polgári és Politikai Jogok Nemzetközi Egyezségokmányának (ICCPR) 41. cikke szerinti, államok közötti panasztételi eljárás elindítása révén;

30. felszólítja a tagállamokat, hogy alakítsanak ki hatékony mechanizmusokat, amelyek segítségével a jogállamisággal és a polgárok alapvető jogaival ellentétes (tömeges) megfigyelési programokért felelős személyeket felelősségre lehet vonni a hatalommal való visszaélés miatt;

31. felszólítja az Egyesült Államokat, hogy haladéktalanul vizsgálja felül jogszabályait annak érdekében, hogy azokat összehangolja a nemzetközi joggal, továbbá ismerje el a magánélethez való jogot és az uniós polgárok egyéb jogait, biztosítson bírósági jogorvoslatot az uniós polgárok számára, az uniós polgárok jogait az Egyesült Államok polgárait megillető jogokkal tegye egyenlővé, és írja alá a fakultatív jegyzőkönyvet, amely az ICCPR alapján lehetővé teszi az egyéni panaszok előterjesztését;

32. e tekintetben üdvözli az Obama amerikai elnök által tett észrevételeket és a 2014. január 17-én kiadott elnöki rendeletet, amelyek előrelépést jelentenek a nemzetbiztonsági célú megfigyelés és adatfeldolgozás alkalmazása engedélyezésének korlátozása, valamint afelé, hogy az Egyesült Államok hírszerző közössége állampolgárságtól vagy lakóhelytől függetlenül minden egyén személyes adatait azonos módon kezelje; további konkrét lépéseket vár ugyanakkor az Unió és az Egyesült Államok közötti kapcsolatokkal összefüggésben, amelyek elsősorban megerősítik a transzatlanti adattovábbítás iránti bizalmat, és jogilag kötelező erejű garanciákat nyújtanak az uniós polgárok magánélethez való jogainak érvényesíthetősége tekintetében, az e jelentésben részletesen előírtak szerint;

33. hangsúlyozza, hogy komoly aggályai vannak az Európa Tanácsnak a számítástechnikai bűnözésről szóló 2001. november 23-i egyezmény (Budapesti Egyezmény) 32. cikkének értelmezésével foglalkozó bizottságában a tárolt számítógépes adatokhoz való, engedéllyel történő határokon átnyúló hozzáférés, illetve adott esetben az azokhoz való ilyen nyilvános hozzáférés tárgyában folytatott munkával kapcsolatban, és határozottan ellenzi olyan kiegészítő jegyzőkönyv vagy iránymutatás elfogadását, amely e rendelkezés hatályát az említett egyezmény által létrehozott hatályos rendszeren túlra is kiterjesztené, mivel ez utóbbi már jelenleg is a territorialitás elve alóli jelentős kivételt képez, és mivel ez a bűnüldöző hatóságok akadálytalan távoli hozzáférését eredményezheti más államok joghatósága alá tartozó területen elhelyezkedő szerverekhez és számítógépekhez, anélkül hogy igénybe kellene venniük a kölcsönös jogsegélyről szóló megállapodásokat vagy az igazságügyi együttműködés más, az egyének alapvető jogainak – köztük az adatok védelméhez és a megfelelő eljáráshoz való jog – garantálása céljából létrehozott eszközöket, különösen az Európa Tanács 108. egyezményét;

34. felszólítja a Bizottságot, hogy 2014 júliusa előtt végezze el annak vizsgálatát, hogy a 2271/96/EK rendelet alkalmazandó-e a személyes adatok továbbítására vonatkozó jogszabályok kollíziójának eseteiben;

35. felhívja az Alapjogi Ügynökséget, hogy végezzen részletes kutatást az alapvető jogok védelméről a megfigyeléssel összefüggésben, és különösen az uniós polgárok jelenlegi jogi helyzetéről az ilyen gyakorlatokkal kapcsolatban rendelkezésükre álló jogorvoslatok tekintetében;

Nemzetközi adattovábbítás

Az Egyesült Államok adatvédelmi keretrendszere és az Egyesült Államok védett adatkikötője

36. megjegyzi, hogy azon társaságok, amelyek a médiában feltárt információk szerint közreműködtek az uniós érintetteknek az egyesült államokbeli NSA részéről történő nagyszabású, tömeges megfigyelésében, önmaguk tanúsították a védett adatkikötőre vonatkozó elveknek való megfelelést, és megállapítja, hogy a védett adatkikötő képezi az uniós személyes adatok Egyesült Államokba való továbbításának jogi eszközét (például Google, Microsoft, Yahoo!, Facebook, Apple, LinkedIn); aggodalmát fejezi ki amiatt, hogy az említett szervezetek az adatközpontjaik közötti információfolyamot és kommunikációt nem titkosítják, ezáltal lehetővé téve a hírszerző szolgálatok számára az információk megszerzését; üdvözli a fentiek nyomán az egyes egyesült államokbeli vállalatok által tett kijelentéseket, amelyek szerint felgyorsítják a globális adatközpontjaik közötti adatáramlás titkosítására vonatkozó tervek megvalósítását;

37. úgy véli, hogy az egyesült államokbeli hírszerző szolgálatoknak a védett adatkikötő keretében feldolgozott uniós személyes adatokhoz való nagyszabású hozzáférése nem teljesíti a „nemzetbiztonság” által indokolt eltérés kritériumait;

2014. március 12., szerda

38. arra az álláspontra helyezkedik, hogy mivel a jelenlegi körülmények között a védett adatkikötőre vonatkozó elvek nem biztosítanak elegendő védelmet az uniós polgárok számára, az ilyen jellegű adattovábbításokat más eszközök révén, így például szerződési feltételek vagy kötelező erejű vállalati szabályok alapján kell megvalósítani, feltéve, hogy ezek az eszközök egyedi garanciákat és biztosítékokat állapítanak meg, és más jogi keretekkel nem kerülhetők meg;

39. arra az álláspontra helyezkedik, hogy a Bizottság nem orvosolta a védett adatkikötő jelenlegi végrehajtásában megfigyelhető, jól ismert hiányosságokat;

40. felszólítja a Bizottságot, hogy terjesszen elő intézkedéseket a 2000/520/EK bizottsági határozat azonnali hatállyal történő felfüggesztésére, amely megállapította az Egyesült Államok Kereskedelmi Minisztériuma által kiadott, védett adatkikötőre vonatkozó elvek és a kapcsolódó gyakran felvetődő kérdések megfelelőségét; felszólítja ezért az USA hatóságait, tegyenek javaslatot a személyes adatok Unióból az USA-ba történő továbbításáról szóló olyan új keretre, amely megfelel az uniós adatvédelmi jogban foglalt követelményeknek, és biztosítja az adatvédelem előírt szintjét;

41. felszólítja a tagállamok illetékes hatóságait, különösen az adatvédelmi hatóságokat, hogy fennálló hatáskörükkel élve haladéktalanul függesszék fel az adatáramlást mindazon szervezetekhez, amelyek önmaguk tanúsították az egyesül államokbeli védett adatkikötőre vonatkozó elveknek való megfelelést, és írják elő, hogy ilyen adatáramlás kizárólag más eszközök révén valósulhat meg, amennyiben azok rendelkeznek a szükséges garanciákkal és biztosítékokkal a magánélethez való jog, valamint az egyének alapvető jogainak és szabadságainak védelmét illetően;

42. felszólítja a Bizottságot, hogy 2014 decemberéig ismertesse a magánélet védelmére vonatkozó egyesült államokbeli keretrendszer átfogó értékelését, amely a kereskedelmi, a bűnüldözési és a hírszerzési tevékenységekre egyaránt kiterjed, és amely az egyesült államokbeli általános adatvédelmi törvény hiányára tekintettel konkrét ajánlásokat fogalmaz meg; bátorítja a Bizottságot, hogy vegye fel a kapcsolatot az USA adminisztrációjával annak érdekében, hogy kidolgozzanak egy olyan jogi keretet, amely magas szintű védelmet nyújt az egyének számára személyes adataiknak az USA-ba történő továbbítása tekintetében, valamint biztosítja a magánélet védelmére vonatkozó uniós és egyesült államokbeli keretrendszer közötti ekvivalenciát;

Egyéb harmadik országokba történő adattovábbítás a megfelelőségi határozat alapján

43. emlékeztet arra, hogy a 95/46/EK irányelv kimondja, hogy személyes adatok csak akkor továbbíthatók harmadik országba, ha – az ezen irányelv egyéb rendelkezései értelmében elfogadott nemzeti rendelkezéseknek való megfelelés sérelme nélkül – az adott harmadik ország megfelelő védelmi szintet tud biztosítani, e rendelkezés célja pedig az uniós adatvédelmi jog által biztosított védelem folytonosságának garantálása a személyes adatok Unión kívüli továbbításának esetében;

44. emlékeztet arra, hogy a 95/46/EK irányelv előírja, hogy a harmadik ország által nyújtott védelem szintjének megfelelőségét a továbbítási művelettel vagy műveletsorozattal kapcsolatos körülmények figyelembevételével kell értékelni; egyúttal emlékeztet arra, hogy a szóban forgó irányelv végrehajtási hatáskörökkel is felruházza a Bizottságot annak kinyilvánítására, hogy egy harmadik ország megfelelő szintű védelmet biztosít a 95/46/EK irányelvben foglalt kritériumok tükrében; emlékeztet arra, hogy a 95/46/EK irányelv egyben annak kinyilvánítására is felhatalmazza a Bizottságot, hogy egy harmadik ország nem biztosít megfelelő szintű védelmet;

45. emlékeztet arra, hogy ez utóbbi esetben a tagállamok kötelesek meghozni a szükséges intézkedéseket annak megakadályozására, hogy ugyanilyen típusú adatok továbbítására kerüljön sor a kérdéses harmadik ország részére, a Bizottságnak pedig tárgyalásokat kell kezdeményeznie a helyzet orvoslása érdekében;

46. felszólítja a Bizottságot és a tagállamokat annak haladéktalan kivizsgálására, hogy az új-zélandi adatvédelmi törvény és a személyes információk védelméről és az elektronikus dokumentumokról szóló kanadai törvény által biztosított megfelelő szintű védelmet – amelyet a 2013/65/EU és a 2002/2//EK bizottsági határozatok is kinyilvánítottak – befolyásolta-e ezen országok nemzetbiztonsági ügynökségeinek közreműködése az uniós polgárok tömeges megfigyelésében, és kéri, hogy adott esetben hozzanak megfelelő intézkedéseket a megfelelőségi határozat felfüggesztése vagy visszavonása érdekében; felszólítja továbbá a Bizottságot, hogy más olyan országok esetében is értékelje a helyzetet, amelyek megfelelőségi besorolást kaptak; elvárja, hogy a Bizottság legkésőbb 2014 decemberéig beszámoljon a Parlamentnek a fent említett országokkal kapcsolatos megállapításairól;

Szerződési feltételeken és egyéb eszközökön alapuló adattovábbítás

47. emlékeztet arra, hogy a nemzeti adatvédelmi hatóságok korábban már jelezték, hogy az általános szerződési feltételeket és a kötelező erejű vállalati szabályokat nem a személyes adatokhoz tömeges megfigyelés céljából való hozzáféréssel jellemzett helyzetekre figyelemmel alkották meg, az ilyen jellegű hozzáférés pedig nem állna összhangban a szerződési feltételek vagy a kötelező erejű vállalati szabályok eltérési záradékaival, amelyek jogos érdekből, szükséges esetben és arányos mértékben alkalmazott rendkívüli eltérésekre hivatkoznak egy demokratikus társadalomban;

48. felszólítja a tagállamokat, hogy tiltsák be vagy függesszék fel a harmadik országokba irányuló, az illetékes nemzeti hatóságok által engedélyezett általános szerződési feltételeken, szerződési feltételeken vagy kötelező erejű vállalati szabályokon alapuló adatáramlást, amennyiben várható, hogy az adatok felhasználójára irányadó jog olyan követelményeket támaszt vele szemben, amelyek túllépik a demokratikus társadalomban szigorúan szükséges, megfelelő és arányos korlátozásokat, és amennyiben ezek a követelmények vélhetően hátrányos hatással lesznek az alkalmazandó adatvédelmi jog és az általános szerződési feltételek által nyújtott garanciákra, vagy ha az adattovábbítás folytatása súlyosan veszélyeztetné az érintetteket;

49. felszólítja a 29. cikk szerinti munkacsoportot, hogy tegyen közzé iránymutatásokat és ajánlásokat azon garanciákra és biztosítékokra vonatkozóan, amelyeket az uniós személyes adatok nemzetközi továbbítására vonatkozó szerződéses jogi eszközöknek tartalmazniuk kell annak érdekében, hogy biztosítsák az egyének magánéletének, valamint alapvető jogainak és szabadságainak védelmét, figyelembe véve különösen a harmadik országok hírszerzési és nemzetbiztonsági vonatkozású jogszabályait, valamint az adatokat egy harmadik országban fogadó társaságok közreműködését a harmadik ország hírszerző ügynökségei által végzett megfigyelési tevékenységekben;

50. felszólítja a Bizottságot, hogy haladéktalanul vizsgálja meg az általa kidolgozott általános szerződési feltételeket annak megállapítása érdekében, hogy azok biztosítják-e a szükséges védelmet az ilyen feltételek alapján hírszerzés céljából továbbított személyes adatokhoz való hozzáférés terén, és adott esetben vizsgálják felül azokat;

Adattovábbítás a kölcsönös jogsegélyről szóló megállapodás alapján

51. felszólítja a Bizottságot, hogy még 2014 vége előtt végezze el a kölcsönös jogsegélyről szóló hatályos megállapodás mélyreható vizsgálatát – annak 17. cikke értelmében –, gyakorlati végrehajtásának ellenőrzése és különösen annak megállapítása céljából, hogy az Egyesült Államok ténylegesen alkalmazta-e azt információk és bizonyítékok megszerzésére az Unióban, valamint hogy megvalósult-e a megállapodás kijátszása az információknak közvetlenül az Unióban történő megszerzése érdekében, továbbá annak megállapítása céljából, hogy a megállapodás miként befolyásolta az egyének alapvető jogait; a vizsgálat nem hagyatkozhat pusztán az Egyesült Államok hivatalos nyilatkozataira az elemzés elégséges alapjaként, hanem célzott uniós értékelésekre kell épülnie; e mélyreható felülvizsgálatnak azzal is foglalkoznia kell, hogy milyen következményekkel jár az Unió alkotmányos szerkezetének alkalmazása a szóban forgó eszközre vonatkozóan annak érdekében, hogy az összhangba kerüljön az uniós joggal, figyelembe véve mindenekelőtt a 36. jegyzőkönyvet és annak 10. cikkét, valamint az e jegyzőkönyvről szóló 50. sz. nyilatkozatot; felszólítja továbbá a Tanácsot és a Bizottságot, hogy vizsgálják meg a tagállamok és az Egyesült Államok közötti kétoldalú megállapodásokat annak biztosítása céljából, hogy e kétoldalú megállapodások összhangban legyenek az EU és az Egyesült Államok között létesült vagy a jövőben létesítendő megállapodásokkal;

Kölcsönös bűnügyi jogsegély az Unióban

52. felkéri a Tanácsot és a Bizottságot, hogy tájékoztassák a Parlamentet a tagállamok közötti kölcsönös bűnügyi jogsegélyről szóló egyezmény tagállamok általi tényleges alkalmazásáról, különös tekintettel a távközlés lehallgatásáról szóló III. címre; felszólítja a Bizottságot, hogy az előzetes felkérésnek eleget téve és az 50. sz. nyilatkozatnak megfelelően 2014 vége előtt terjesszen elő javaslatot a 36. jegyzőkönyvre vonatkozóan, annak a Lisszaboni Szerződés keretéhez való hozzáigazítása érdekében;

A TFTP- és a PNR-megállapodásokon alapuló adattovábbítás

53. arra az álláspontra helyezkedik, hogy az Európai Bizottság és az Egyesült Államok Pénzügyminisztériuma által biztosított információ nem tisztázza, hogy a SWIFT-hálózatok vagy bankok operációs rendszereinek vagy kommunikációs hálózatainak megfigyelése révén az egyesült államokbeli hírszerző ügynökségek hozzáféréssel rendelkeznek-e a SWIFT fizetési üzeneteihez az Unióban, egyedül vagy uniós nemzeti hírszerző ügynökségekkel együttműködve, valamint a kölcsönös jogsegély és az igazságügyi együttműködés kétoldalú csatornáinak igénybevétele nélkül;

2014. március 12., szerda

54. emlékeztet 2013. október 23-i állásfoglalására, és kéri a Bizottságot a TFTP-megállapodás felfüggesztésére;

55. felszólítja a Bizottságot, hogy reagáljon az arra vonatkozó aggodalmakra, hogy a légitársaságok által világszerte alkalmazott legfontosabb számítógépes foglalási rendszerek közül három székhelye az Egyesült Államokban található, és az utas-nyilvántartási adatokat az Egyesült Államok területén felhőalapú rendszerekben tárolják az Egyesült Államok joga szerint, amely nem biztosít megfelelő szintű adatvédelmet;

Adatvédelmi keretmegállapodás a rendőrségi és igazságügyi együttműködés terén („átfogó megállapodás")

56. úgy véli, hogy az átfogó megállapodás keretében elérendő kielégítő megoldás előfeltétele annak, hogy teljes mértékben helyreállhasson a transzatlanti partnerek közötti bizalom;

57. kéri, hogy haladéktalanul kezdődjenek újra a tárgyalások az USA-val az átfogó megállapodásról, amelynek egyenlő jogokat kell biztosítania az uniós és az egyesült államokbeli polgárok számára; hangsúlyozza továbbá, hogy a megállapodásnak az USA-ban megkülönböztetés nélkül minden uniós polgár számára hatékony és végrehajtható közigazgatási és bírósági jogorvoslatot kell biztosítania;

58. felkéri a Bizottságot és a Tanácsot, hogy ne kezdeményezzenek az Egyesült Államokkal kötendő új ágazati megállapodásokat vagy megegyezéseket a személyes adatok bűnüldözés céljából történő továbbítására vonatkozóan mindaddig, amíg hatályba nem lép az átfogó megállapodás;

59. sürgeti a Bizottságot, hogy 2014 áprilisáig részletesen számoljon be a tárgyalási meghatalmazás különféle pontjairól és a helyzet legfrissebb állásáról;

Adatvédelmi reform

60. felszólítja a Tanács elnökségét és a tagállamokat, hogy gyorsítsák fel a teljes adatvédelmi csomagot érintő munkájukat, lehetővé téve ennek 2014. évi elfogadását annak érdekében, hogy az uniós polgárok már a közeljövőben magas szintű védelmet élvezhessenek; hangsúlyozza, hogy a harmadik országok felé irányuló hitelességnek és magabiztosságnak szükségszerű előfeltétele a Tanács részéről megnyilvánuló határozott elkötelezettség és teljes körű támogatás;

61. hangsúlyozza, hogy az adatvédelmi rendeletre és az adatvédelmi irányelvre egyaránt szükség van az egyének alapvető jogainak védelméhez, ezért e kettőt egyetlen csomag részeként kell kezelni és egy időben kell elfogadni annak garantálása érdekében, hogy valamennyi uniós adatfeldolgozó tevékenység magas szintű védelmet biztosítson minden körülmények között; hangsúlyozza, hogy csupán akkor fogad el további, bűnüldözési együttműködésre vonatkozó intézkedéseket, miután a Tanács tárgyalást kezdett a Parlamenttel és a Bizottsággal az adatvédelmi csomagról;

62. emlékeztet arra, hogy a „beépített adatvédelem" és az „alapértelmezett adatvédelem" fogalma az adatvédelem megerősítését célozza, és iránymutatásként kell szolgálnia minden interneten kínált termék, szolgáltatás és rendszer vonatkozásában;

63. úgy véli, hogy az online kommunikációra és a távközlésre vonatkozó magasabb szintű átláthatósági és biztonsági előírások szükségszerű tényezők egy jobb adatvédelmi rendszer megvalósításában; ezért arra kéri a Bizottságot, hogy terjesszen elő jogalkotási javaslatot az online kommunikációra és a távközlésre vonatkozó egységesített általános feltételekről, továbbá bízzon meg egy felügyeleti szervet az általános feltételek betartásának ellenőrzésével;

Számításifelhő-szolgáltatások

64. megjegyzi, hogy az egyesült államokbeli számításifelhő-szolgáltatásokba és -szolgáltatókba vetett bizalmat kedvezőtlenül befolyásolták a fent említett gyakorlatok; ezért hangsúlyozza, hogy az európai számítási felhők és informatikai megoldások kialakítása elengedhetetlen alkotóeleme a növekedésnek és a munkahelyteremtésnek, valamint a számításifelhő-szolgáltatásokba és -szolgáltatókba vetett bizalomnak, illetve a személyes adatok magas szintű védelme biztosításának;

65. felszólítja az összes uniós közigazgatási szervet, hogy ne használjanak számításifelhő-szolgáltatásokat, amennyiben fennáll annak az esélye, hogy ott nem az uniós jogot alkalmazzák;

66. ismételten hangot ad mélységes aggodalmának a felhőalapú szolgáltatásokra vonatkozó megállapodások alapján, harmadik ország jogszabályai szerint működő vagy harmadik országban telepített tárolószervereket működtető számításifelhő-szolgáltatók által a feldolgozott uniós személyes adatok és információk harmadik állam hatóságainak való kötelező és közvetlen kiszolgáltatása miatt, valamint a harmadik országok bűnüldöző hatóságai és hírszerző szolgálatai által feldolgozott személyes adatokhoz és információkhoz való közvetlen távoli hozzáférés miatt;

67. helyteleníti, hogy ez a hozzáférés általában a harmadik országbeli hatóságok részéről saját jogi normáik közvetlen alkalmazása révén valósul meg, a jogi együttműködés érdekében kidolgozott nemzetközi okmányok, például a kölcsönös jogsegélyre vagy az igazságügyi együttműködés más formáira vonatkozó megállapodások igénybevétele nélkül;

68. felhívja a Bizottságot és a tagállamokat, hogy gyorsítsák fel az Európai Számítási Felhő Partnerség kialakítására irányuló munkát, és ebbe teljes körűen vonják be a civil társadalmat és a műszaki szakmai közösséget, így például az Internet Engineering Task Force (IETF) szervezetet, és ennek során vegyék figyelembe az adatvédelmi szempontokat;

69. sürgeti a Bizottságot, hogy a személyes adatok feldolgozását is érintő nemzetközi megállapodások tárgyalásakor fordítson külön figyelmet azokra a kockázatokra és veszélyekre, amelyeket a felhőalapú számítástechnika jelent az alapvető jogok és különösen – bár nem kizárólagosan – a magánélethez és a személyes adatok védelméhez fűződő jog tekintetében, amelyeket az Európai Unió Alapjogi Chartájának 7. és 8. cikke rögzít; ezenkívül sürgeti a Bizottságot, hogy szenteljen figyelmet a tárgyalópartner felhőalapú számítástechnikai szolgáltatások révén feldolgozott személyes adatokhoz való hozzáférésre vonatkozó hazai szabályozásának, különösen annak a követelménynek, hogy ilyen hozzáférést csak a megfelelő jogi eljárás maradéktalan betartásával és egyértelmű jogalapra építve biztosítsanak, továbbá annak a követelménynek, hogy meg kell határozni a hozzáférés pontos feltételeit, a hozzáférés engedélyezésének célját, az adatok átadása során érvényesülő biztonsági intézkedéseket, a személyek jogait, valamint a felügyeletre és a hatékony jogorvoslatra vonatkozó szabályokat;

70. emlékeztet arra, hogy az Unióban szolgáltatásokat nyújtó minden társaságnak kivétel nélkül tiszteletben kell tartania az uniós jogot, és felelősséget kell vállalnia az esetleges jogsértésekért, valamint hangsúlyozza annak fontosságát, hogy hatékony, arányos és visszatartó erejű közigazgatási szankciók álljanak rendelkezésre, amelyek kiszabhatók azon számításifelhő-szolgáltatókra, amelyek nem tesznek eleget az uniós adatvédelmi normáknak;

71. felkéri a Bizottságot és a tagállamok illetékes hatóságait annak felmérésére, hogy az uniós jogi személyek titkosszolgálatokkal folytatott együttműködése során, illetve az uniós adatvédelmi jogszabályokba ütköző módon az uniós polgárok személyes adatait megkérő harmadik országbeli hatóságok bírósági végzéseinek elfogadásával milyen mértékben sértették meg a magánélet védelmére és az adatvédelemre vonatkozó uniós szabályokat;

72. felszólítja az óriási méretű adathalmazok és az új alkalmazások, így például a tárgyak internetének használatával új szolgáltatásokat nyújtó vállalkozásokat, hogy már a fejlesztési szakaszban építsenek be adatvédelmi intézkedéseket annak érdekében, hogy a polgárok körében fenntartsák a nagyfokú bizalmat;

Transzatlanti kereskedelmi és beruházási partnerség (TTIP)

73. elismeri, hogy az Európai Unió és az Egyesült Államok tárgyalásokra törekednek egy transzatlanti kereskedelmi és beruházási partnerség érdekében, amely komoly stratégiai jelentőséggel bír a további gazdasági növekedés elérése szempontjából;

74. erőteljesen hangsúlyozza, hogy tekintettel a digitális gazdaságnak az Unió és az Egyesült Államok közötti kapcsolatban és e két fél közötti bizalom újjáépítésében betöltött fontos szerepére, az Európai Parlament végleges TTIP-megállapodáshoz való hozzájárulását veszélyezteti, ha nem vetnek maradéktalanul véget a mindenre kiterjedő tömeges megfigyelési tevékenységeknek és az uniós intézmények és diplomáciai képviseletek lehallgatásának, valamint nem találnak megfelelő megoldást az uniós polgárok adatvédelmi jogaira, ideértve a közigazgatási és bírósági jogorvoslatot is;

hangsúlyozza, hogy a Parlament csupán abban az esetben járul hozzá a végleges TTIP-megállapodáshoz, ha e megállapodás maradéktalanul tiszteletben tartja többek között az Unió Alapjogi Chartájában elismert alapvető jogokat, és ha az egyének magánélethez való jogának védelmét pedig a személyes adatok feldolgozásának és terjesztésének összefüggésében továbbra is a GATS-egyezmény XIV. cikke szabályozza; hangsúlyozza, hogy a GATS-egyezmény XIV. cikkének alkalmazása során az uniós adatvédelmi jogszabályok nem tekinthetők „önkényes és megalapozatlan diszkriminációnak";

A hírszerző szolgálatok demokratikus felügyelete

75. hangsúlyozza, hogy jóllehet a hírszerző szolgálatok tevékenységének felügyeletét egyrészről a demokratikus legitimitásra (szilárd 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;

76. 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;

77. felszólít egy olyan európai parlamenti képviselőkből és szakértőkből álló munkacsoport felállítására, amely átlátható módon és a nemzeti parlamentekkel való együttműködés mellett megvizsgálná a demokratikus felügyelet – beleértve a hírszerző szolgálatok parlamenti felügyeletét és az Unión belüli fokozott felügyeleti együttműködést is – megerősítésére tett ajánlásokat; úgy véli, hogy a munkacsoportnak különösen az európai minimumszabályok vagy iránymutatások kidolgozásának lehetőségét kell megvizsgálnia a hírszerző szolgálatok (előzetes és utólagos) felügyeletére vonatkozóan, a meglévő bevált gyakorlatok és a nemzetközi szervek (ENSZ, 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; meg kell még vizsgálnia az átláthatóság növelésére vonatkozó kritériumokat, az információkhoz való hozzáférés általános elvére és az úgynevezett „Tshwane elvekre" ([1]) építve, valamint a megfigyelés időtartamára és hatókörére vonatkozó alapelveket, biztosítva, hogy azok arányosak legyenek, és a megfigyelés céljára korlátozódjanak;

78. felszólítja a munkacsoportot, hogy 2015 elejére készítsen jelentést egy, a Parlamentben a – parlamenti vagy független – nemzeti felügyeleti testületek közreműködésével megrendezendő konferencia számára, és segédkezzen annak megrendezésében is;

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

80. felszólítja a tagállamokat, hogy alakítsanak ki együttműködést a felügyeleti szervek között, különösen a nemzeti hírszerzési felügyeletek európai hálózatának (ENNIR) keretében;

81. sürgeti a főképviselőt/alelnököt, hogy a Parlament illetékes testületeinek rendszeresen számoljon be az Európai Unió Helyzetelemző Központja (IntCen) – amely az Európai Külügyi Szolgálat része – által végzett tevékenységekről, ideértve az emberi jogok és az alkalmazandó uniós adatvédelmi szabályok IntCen általi teljes körű tiszteletben tartását is, amelynek segítségével a Parlament hatékonyabban felügyelheti az uniós politikák külső dimenzióját; sürgeti a főképviselőt/alelnököt, hogy terjesszen elő javaslatot az IntCen által végzett tevékenységek jogalapjára arra az esetre, ha a hírszerzési és az adatgyűjtési képességek terén saját műveleteket és jövőbeli hatásköröket alakítanának ki, ami hatással lehet az Unió belbiztonsági stratégiájára;

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

82. felszólítja a Bizottságot, hogy 2014 decemberéig terjesszen elő javaslatot egy minden uniós tisztségviselőre vonatkozó uniós biztonsági ellenőrzési eljárásra, 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 munkatársaikkal való eltérő bánásmódhoz vezet;

83. 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, amelyeket fel kell használni az uniós szintű felügyelet javítása érdekében;

Uniós ügynökségek

84. felhívja az Europol közös ellenőrző hatóságát, hogy a nemzeti adatvédelmi hatóságokkal együtt 2014 vége előtt folytasson le közös vizsgálatot annak ellenőrzése érdekében, hogy a nemzeti hatóságok jogszerűen szerezték-e meg az Europollal megosztott információkat és személyes adatokat, különösen ha az információkat vagy adatokat eredetileg uniós vagy harmadik országbeli hírszerző szolgálatok igényelték, és hogy megfelelő intézkedéseket vezettek-e be az ilyen információk és adatok felhasználásának és további terjesztésének megelőzése céljából; úgy véli, hogy az Europol nem dolgozhat fel olyan információkat vagy adatokat, amelyeket az Alapjogi Charta alapján védelmet élvező emberi jogok megsértésével szereztek meg;

85. felszólítja az Europolt, hogy teljes körűen használja fel megbízatását és kérje a tagállamok illetékes hatóságait, hogy indítsanak bűnügyi nyomozást az esetlegesen határokon átnyúló következményekkel járó jelentős kibertámadások és informatikai jogsértések tekintetében; úgy véli, hogy az Europol megbízatását ki kell terjeszteni annak érdekében, hogy saját nyomozást is indíthasson, ha két vagy több tagállam vagy az uniós testületek hálózati és információs rendszerei elleni rosszindulatú támadás gyanúja felmerül ([1]); felkéri a Bizottságot, hogy vizsgálja felül a Számítástechnikai Bűnözés Elleni Európai Központ (EC3) tevékenységét, és szükség esetén terjesszen elő javaslatot a hatásköreinek megerősítésére szolgáló átfogó keretre;

A véleménynyilvánítás szabadsága

86. mélységes aggodalmának ad hangot a sajtószabadságra leselkedő egyre nagyobb veszélyek és a hatósági megfélemlítés újságírókra gyakorolt bénító hatása miatt, különösen az újságírói források titkosságának védelmét illetően; megismétli „Az EU Alapjogi Chartájáról: a tömegtájékoztatás szabadságára vonatkozó irányadó szabályozás az EU-ban” című, 2013. május 21-i állásfoglalásában megfogalmazott felhívását;

87. tudomásul veszi David Mirandának az Egyesült Királyság hatóságai általi őrizetbe vételét és a birtokában lévő anyagok lefoglalását a 2000. évi terrorizmusellenes törvény 7. melléklete alapján (továbbá a The Guardian című laphoz intézett, az anyagok megsemmisítésére vagy átadására irányuló kérést), és aggodalmának ad hangot, amiért mindez esetlegesen súlyosan sérti a véleménynyilvánítás és a tömegtájékoztatás szabadságát, amelyet az EJEE 10. cikke és az EU Alapjogi Chartájának 11. cikke is elismer, továbbá amiért a terrorizmus elleni harcot célul kitűző jogszabályok visszaélésekre adnak lehetőséget az ilyen helyzetekben;

88. felhívja a figyelmet a visszaélést jelentő személyek és támogatóik, többek között az újságírók nehéz helyzetére azt követően, hogy nyilvánosságra hozzák megállapításaikat; felszólítja a Bizottságot annak vizsgálatára, hogy a visszaélést jelentő személyekre irányuló, hatékony és átfogó európai védelmi program létrehozásáról szóló jövőbeni jogalkotási javaslat, amelyet a Parlament 2013. október 23-i állásfoglalásában már kért, kiterjedjen-e az uniós hatáskör más területeire is, különös tekintettel a hírszerzés területét érintő visszaélések jelentésének összetett voltára; felszólítja a tagállamokat, hogy alaposan vizsgálják meg annak lehetőségét, hogy a visszaélést jelentő személyeknek nemzetközi védelmet nyújtsanak a büntetőeljárásokkal szemben;

([1]) Az Európai Parlament 2014. február 25-i jogalkotási állásfoglalása a Bűnüldözési Együttműködés és Képzés Európai Ügynökségéről (Europol) szóló európai parlamenti és tanácsi rendeletre irányuló javaslatról (Elfogadott szövegek, P7_TA(2014)0121).

2014. március 12., szerda

89. felszólítja a tagállamokat, gondoskodjanak arról, hogy jogszabályaik, különösen a nemzetbiztonság területén, az elhallgatással szemben biztonságos alternatívát nyújtsanak a jogsértések, többek között a korrupció, a bűncselekmények, a jogi kötelezettségek megszegése, a bírói tévedések és a hatalommal való visszaélés eseteinek nyilvánosságra hozatalához vagy jelentéséhez, ami összhangban van a különböző korrupció elleni nemzetközi (ENSZ és Európa Tanács) eszközökkel, az Európa Tanács Parlamenti Közgyűlésének 1729 (2010). sz. állásfoglalásában foglalt elvekkel, a Tshwane elvekkel stb.;

Uniós informatikai biztonság

90. rámutat, hogy közelmúltbeli események egyértelműen igazolják az EU – és különösen az uniós intézmények, a nemzeti kormányok és parlamentek, a jelentősebb európai vállalatok, az európai informatikai infrastruktúrák és hálózatok – akut sebezhetőségét az összetett szoftverekkel és a rosszindulatú számítógépes programokkal végrehajtott, kifinomult támadásokkal szemben; megjegyzi, hogy ezek a támadások olyan mennyiségű pénzügyi és humánerőforrást igényelnek, hogy ennek alapján valószínűsíthető, hogy külföldi kormányok képviseletében eljáró állami szervektől származnak; ezzel összefüggésben a Belgacom távközlési vállalatot érintő feltörés vagy lehallgatás az Unió informatikai kapacitásai elleni támadás aggasztó példája; hangsúlyozza, hogy az Unió informatikai kapacitásának és biztonságának fokozása csökkenti az EU sebezhetőségét a nagy bűnszervezetek vagy terrorista csoportok által végrehajtott kibertámadásokkal szemben;

91. álláspontja szerint a tömeges megfigyelés válságot kiváltó napvilágra kerülését Európa lehetőségként használhatná arra, hogy elsőszámú stratégiai prioritású intézkedésként kezdeményezze egy autonóm informatikai kulcserőforrás mielőbbi kiépítését; hangsúlyozza, hogy a bizalom újbóli elnyerése érdekében egy ilyen európai informatikai kapacitásnak, amennyire lehetséges, nyílt szabványokon, valamint nyílt forráskódú szoftvereken és – lehetőség szerint – hardvereken kell alapulnia, ami a processzor kialakításától az alkalmazási szintig áttekinthetővé és felülvizsgálhatóvá teszi az egész ellátási láncot; rámutat arra, hogy az informatikai szolgáltatások stratégiai ágazatában a versenyképesség helyreállítása érdekében egy új digitális modellre van szükség, amelyhez az uniós intézmények, a tagállamok, a kutatóintézetek, az iparág és a civil társadalom részéről közös és nagyléptékű erőfeszítések társulnak; felhívja a Bizottságot és a tagállamokat, hogy vegyék igénybe a közbeszerzést ezen uniós erőforrás-kapacitások mozgósítására olyan módon, hogy az uniós biztonsági és adatvédelmi előírásokat az informatikai javak és szolgáltatások közbeszerzésében kiemelt követelménnyé teszik; ezért sürgeti a Bizottságot, hogy az adatfeldolgozás vonatkozásában vizsgálja felül a jelenlegi közbeszerzési gyakorlatokat annak érdekében, hogy megfontolja a tendereljárások tanúsítással rendelkező társaságokra és esetleg uniós társaságokra való korlátozását, amennyiben a biztonság és más létfontosságú érdekek is érintettek;

92. határozottan elítéli, hogy a hírszerző szolgálatok az informatikai biztonsági normák gyengítésére és az informatikai rendszerek széles körében ún. hátsó ajtók (backdoor) beépítésére törekedtek; kéri a Bizottságot, hogy terjesszen elő jogszabálytervezetet a „hátsó ajtók" bűnüldöző szervek által történő használatának tilalmára vonatkozóan; következésképpen azt ajánlja, hogy nyílt forráskódú szoftvereket használjanak minden olyan környezetben, ahol az informatikai biztonság aggodalomra ad okot;

93. felhívja a tagállamokat, a Bizottságot, a Tanácsot és az Európai Tanácsot, hogy a legnagyobb mértékben támogassa a kutatás és fejlesztés terén nyújtott finanszírozás révén is az európai innovatív és technológiai kapacitás kiépítését az informatikai eszközök, vállalatok és szolgáltatók (hardver, szoftver, szolgáltatások és hálózat) tekintetében, többek között a kiberbiztonsági, titkosítási és kriptográfiai kapacitások kiépítése céljából is; felszólítja az összes felelős uniós intézményt és a tagállamokat, hogy fektessenek be az uniós helyi és független technológiákba, azokat erőteljesen fejlesszék, és növeljék a felderítési képességeket;

94. felhívja a Bizottságot, a szabványosítási testületeket és az ENISA-t, hogy 2014 decemberéig alakítsák ki a biztonsági és adatvédelmi minimumszabványokat és iránymutatásokat az informatikai rendszerek, hálózatok és szolgáltatások tekintetében – beleértve a számítási felhő szolgáltatásokat is – az uniós polgárok személyes adatainak és valamennyi informatikai rendszer integritásának megfelelőbb védelme érdekében; meggyőződése, hogy e szabványok az új globális szabványok viszonyítási alapjaként szolgálhatnak, és nyílt és demokratikus – nem egyetlen ország, szervezet vagy multinacionális vállalat által vezérelt – folyamatban kell meghatározni őket; álláspontja az, hogy miközben a terrorizmus elleni küzdelem támogatására figyelembe kell venni a legitim bűnüldözési és hírszerzési megfontolásokat, ezek nem eredményezhetik az összes informatikai rendszer megbízhatósága általános csorbítását; támogatását fejezi ki az Internet Engineering Task Force (IETF) szervezet arra vonatkozóan hozott legutóbbi határozatai iránt, hogy a kormányokat be kell vonni az internetes biztonságot érintő fenyegetések modelljébe;

95. rámutat, hogy az uniós és nemzeti távközlési szabályozók, valamint bizonyos esetekben a távközlési vállalatok is egyértelműen figyelmen kívül hagyták felhasználóik és az ügyfelek informatikai biztonságát; felhívja a Bizottságot, hogy teljes mértékben hasznosítsa az elektronikus hírközlési adatvédelmi keretirányelv alapján meglévő hatásköreit a kommunikáció titkossága védelmének erősítése érdekében az annak biztosítását szolgáló intézkedések elfogadása révén, hogy a végberendezések kompatibilisek legyenek a felhasználók azon jogával, hogy ellenőrizhetik és védhetik személyes adataikat, továbbá annak érdekében, hogy gondoskodjon a távközlési rendszerek és szolgáltatások magas szintű biztonságáról, például a kommunikáció korszerű, végpontok közötti titkosításának előírása révén;

96. támogatja az uniós kiberstratégiát, de megítélése szerint az nem foglalja magában az összes lehetséges fenyegetést, és ki kell terjeszteni a rosszindulatú állami tevékenységekre is; hangsúlyozza, hogy fokozott informatikai biztonságra és ellenállóbb informatikai rendszerekre van szükség;

97. felhívja a Bizottságot, hogy legkésőbb 2015 januárjáig terjesszen elő egy intézkedési tervet az informatikai ágazatban az EU függetlenségének erősítésére, ideértve az európai informatikai technológiai kapacitások (azaz az informatikai rendszerek, berendezések, szolgáltatások, felhőszámítás, titkosítás és anonimizálás) erősítésének és a kritikus informatikai infrastruktúra (tulajdonjogok és sebezhetőség tekintetében történő) védelmének következetesebb felfogását;

98. felszólítja a Bizottságot, hogy a Horizont 2020 program következő munkaprogramjának keretében több forrást fordítson az informatikai technológiák terén az európai kutatásra, fejlesztésre, innovációra és képzésre, különös tekintettel az adatvédelmet erősítő technológiákra és infrastruktúrákra, a kriptológiára, a számítástechnikai biztonságra, a lehető legjobb biztonsági megoldásokra, köztük a nyílt forráskódú biztonsági megoldásokra és az információs társadalom más szolgáltatásaira, továbbá hogy mozdítsa elő az európai szoftverek és hardverek, a titkosított kommunikációs eszközök és a kommunikációs infrastruktúrák belső piacát azáltal is, hogy a számítástechnikai ágazat számára átfogó európai ipari stratégiát dolgoz ki; úgy véli, hogy a kis- és középvállalkozások lényeges szerepet játszanak a kutatásban; hangsúlyozza, hogy nem szabad uniós pénzeszközöket fordítani pusztán arra a célra, hogy informatikai rendszerekhez való jogosulatlan hozzáféréshez szükséges eszközöket fejlesszenek ki;

99. kéri a Bizottságot, hogy térképezze fel az aktuális feladatokat és legkésőbb 2014 decemberéig vizsgálja felül, hogy szükséges-e az ENISA, az Europol Számítástechnikai Bűnözés Elleni Központja és a speciális szakértelemmel rendelkező egyéb uniós központok, a CERT-EU és az európai adatvédelmi biztos esetében a tágabb felhatalmazás, a jobb koordináció és/vagy további erőforrások és technikai kapacitások biztosítása annak érdekében, hogy képesek legyenek az európai kommunikációs rendszerek biztonságát szolgáló kulcsszerep betöltésére, a jelentős uniós informatikai jogsértések megelőzésére és kivizsgálására, valamint a jelentős uniós informatikai jogsértések eredményesebb helyszíni műszaki vizsgálatának elvégzésére (vagy a tagállamok és uniós szervek ebben való támogatására); különösen felszólítja a Bizottságot arra, hogy fontolja meg az ENISA szerepének erősítését az uniós intézményeken belüli belső rendszerek védelme tekintetében, valamint az ENISA-n belül az EU és a tagállamok számára hozzon létre egy számítógépes vészhelyzeteket elhárító csoportot (CERT);

100. kéri a Bizottságot, hogy vizsgálja meg, szükséges-e egy olyan uniós informatikai akadémia, amely összefogja a kapcsolódó területek legjobb független európai és nemzetközi szakembereit, és feladata az összes érintett uniós intézmény és szerv számára az informatikai technológiákra vonatkozó tudományos tanácsadás, ideértve a biztonsági vonatkozású stratégiákat;

101. felhívja az Európai Parlament titkárságának illetékes szolgálatait, hogy az Európai Parlament elnökének felügyelete mellett legkésőbb 2015 júniusáig – egy időközi jelentéssel 2014 decemberéig – végezzék el az Európai Parlament informatikai biztonsági megbízhatóságának alapos felülvizsgálatát és felmérését az alábbiakra összpontosítva: a költségvetési eszközök, személyzeti erőforrások, technikai kapacitások, belső szervezet és valamennyi lényeges elem, a Parlament informatikai rendszerei magas biztonsági szintjének megvalósítása érdekében; meggyőződése, hogy egy ilyen felmérésnek legalább tájékoztatást, elemzést és ajánlásokat kell adnia az alábbiakról:

— a rendszeres, szigorú, független biztonsági ellenőrzések és behatolási vizsgálatok szükségessége külső biztonsági szakértők kiválasztásával, biztosítva az átláthatóságot, valamint a harmadik országokkal vagy bármely érdekcsoporttal szembeni legitimitásuk garanciáit;

— az új informatikai rendszerek tendereljárásaiba bevált gyakorlatokon alapuló, konkrét informatikai biztonsági/adatvédelmi követelmények beépítése, ideértve azt a lehetőséget, hogy a vásárlás feltételeként nyílt forráskódú szoftvert írnak elő, vagy azon követelménynek a lehetőségét, hogy az érzékeny, biztonsággal kapcsolatos területeket érintő tenderekben megbízható európai társaságok vegyenek részt;

2014. március 12., szerda

— az Európai Parlamenttel informatikai és távközlési területen szerződésben álló vállalatok listája, figyelembe véve bármely napvilágra jutott információt arról, hogy hírszerző ügynökségekkel állnak kapcsolatban (pl. az NSA-szerződésekről napvilágra került információkat olyan vállalatok tekintetében, mint az RSA, amelynek termékeit az Európai Parlament elvileg arra használja, hogy védje az adatainak a képviselők és a személyzet részéről történő távoli elérését), ideértve ugyanazon szolgáltatások lehetőleg európai társaságok által történő biztosításának megvalósíthatóságát is;

— az uniós intézmények által informatikai rendszereikben alkalmazott szoftverek, különösen a készen kapható kereskedelmi szoftvereknek az uniós vagy harmadik országbeli bűnüldözési és hírszerzési hatóságok általi behatolással vagy feltöréssel szembeni megbízhatósága és ellenállósága, figyelembe véve a vonatkozó nemzetközi szabványokat, a legjobb gyakorlatoknak megfelelő biztonsági kockázatkezelési elveket, valamint a biztonság megsértésére vonatkozó európai hálózat- és információbiztonsági szabványok követését;

— több nyílt forráskódú rendszer használata;

— a mobileszközök (például a munkahelyi vagy magáncélú okostelefonok, táblagépek stb.) megnövekedett használatának, és annak a rendszer informatikai biztonságára gyakorolt hatásának kezelése érdekében meghozandó lépések és intézkedések;

— a Parlament különböző munkahelyszínei közötti kommunikáció, és a Parlamentben használt informatikai rendszerek biztonsága;

— a Parlament informatikai rendszerei számára a szerverek és informatikai központok használata és azok helye, és a rendszerek biztonságára és integritására gyakorolt hatások;

— a biztonsági visszaélésekre vonatkozó hatályos szabályok gyakorlati végrehajtása, és a nyilvánosan elérhető távközlési hálózatok szolgáltatói részéről az illetékes hatóságok haladéktalan értesítése;

— a számításifelhő- és felhőtárhely-szolgáltatások Parlament általi használata, ideértve a felhőben tárolt adatok jellegét, hogy milyen védelem érvényesül a tartalomra és annak elérésére, és hogy hol vannak a felhőszerverek, pontosítva az adatvédelemre és a hírszerzésre alkalmazandó jogi keretet, és megvizsgálva azt a lehetőséget, hogy kizárólag uniós területen található felhőszervereket használnak;

— a kriptográfiai technológiák kiterjedtebb használatának lehetővé tételére vonatkozó terv, különösen az összes informatikai és kommunikációs szolgáltatásban – így a számításifelhő-szolgáltatások, elektronikus levelezés, azonnali üzenetküldés és telefónia – a végpont-hitelesített titkosítás;

— az elektronikus aláírás elektronikus levelekben történő használata;

— alapértelmezett elektronikus levelezési titkosítási szabvány, például a GNU Privacy Guard használatára vonatkozó terv, amely egyúttal lehetővé tenné a digitális aláírások használatát;

— a Parlamenten belül a biztonságos belső kommunikációt lehetővé tevő azonnali üzenetküldési szolgáltatás bevezetésének lehetősége, amelyben a szerver csak titkosított tartalmat látna;

102. felhívja az összes uniós intézményt és ügynökséget – különösen az Európai Tanácsot, a Tanácsot, az Európai Külügyi Szolgálatot (az uniós küldöttségeket is beleértve), a Bizottságot, a Bíróságot és az Európai Központi Bankot –, hogy legkésőbb 2015 júniusáig (egy időközi jelentéssel 2014 decemberéig) az ENISA-val, az Europollal és a CERT-ekkel együttműködve végezzenek el egy hasonló munkát; felkéri a tagállamokat hasonló értékelések elvégzésére;

103. hangsúlyozza, hogy az Unió külső fellépéseit illetően késedelem nélkül el kellene végezni a költségvetési szükségletek felmérését és meg kellene hozni az első intézkedéseket az Európai Külügyi Szolgálat (EKSZ) vonatkozásában, és ehhez megfelelő pénzeszközöket kell a 2015. évi költségvetési tervezetben hozzárendelni;

104. álláspontja szerint a szabadságon, biztonságon és a jog érvényesülésén alapuló térség tekintetében használt nagyléptékű informatikai rendszerek – mint a Schengeni Információs Rendszer második generációja, a Vízuminformációs Rendszer, az Eurodac és olyan lehetséges jövőbeni rendszerek, mint az EU-ESTA – fejlesztését és üzemeltetését olyan módon kell végezni, hogy biztosított legyen, hogy a harmadik országbeli hatóságok kérései nyomán az adatok ne sérüljenek; felkéri az eu-LISA-t (a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség nagyméretű IT-rendszereinek üzemeltetési igazgatását végző ügynökséget), hogy 2014 végéig számoljon be a Parlamentnek a működő rendszerek megbízhatóságáról;

105. felhívja a Bizottságot és az EKSZ-t, hogy lépjen fel nemzetközi szinten – különösen az ENSZ-szel közösen –, és az érdekelt partnerekkel együttműködésben hajtsa végre az internet demokratikus irányítására vonatkozó uniós stratégiát az ICANN és az IANA tevékenységei felett magánszemélyek, vállalatok vagy országok illetéktelen befolyásának megelőzése érdekében, e szervezetekben valamennyi érdekelt fél megfelelő képviseletének biztosításával, mindeközben elkerülve az állami ellenőrzés vagy cenzúra, illetve az internet „balkanizálódásának" és széttöredezésének elősegítését;

106. felszólítja az EU-t, hogy töltsön be vezető szerepet az internet felépítésének és irányításának átalakításában, amelynek célja az adatáramlással és -tárolással kapcsolatos kockázatok kezelése, a nagyobb adatminimalizálásra és átláthatóságra, a nyers adatok centralizált tömeges tárolásának visszaszorítására, valamint az internetes forgalom átirányítására vagy az összes internetes forgalom teljes körű, végpontok közötti titkosítására való törekvés, annak érdekében, hogy el lehessen kerülni a jelenlegi kockázatokat, amelyek az adatforgalom olyan országokon keresztül történő irányításából adódnak, amelyek nem felelnek meg az alapjogok, adatvédelem és a magánélet védelme alapvető normáinak;

107. felszólít az alábbiak előmozdítására:

— uniós keresőmotorok és uniós közösségi hálózatok, fontos lépésként az EU informatikai függetlenségének megteremtése felé;

— európai informatikai szolgáltatók;

— a kommunikáció általános titkosítása, ideértve az elektronikus levelezést és az sms-közléseket is;

— az európai informatikai rendszer kulcsfontosságú elemei, például a kliensek, szerverek és operációs rendszerek közötti megoldások, nyílt forráskódú szabványok használata, a hálózatok összekapcsolását szolgáló európai komponensek, például routerek kifejlesztése;

108. felszólítja a Bizottságot, hogy terjesszen elő jogalkotási javaslatot egy, a hívásrészletezési adatok (CDR) uniós szintű feldolgozását is magában foglaló uniós útválasztási rendszerre, ami a meglévő internet egy alrendszere lenne, és nem terjedne ki az Unió határain túlra; megjegyzi, hogy minden útválasztási és hívásrészletezési adatot az uniós jogi keretekkel összhangban kell feldolgozni;

109. felhívja a tagállamokat, hogy az ENISA-val, az Europol Számítástechnikai Bűnözés Elleni Központjával, a CERT-ekkel és a nemzeti adatvédelmi hatóságokkal és a számítógépes bűnözéssel foglalkozó csoportokkal együttműködésben alakítson ki biztonsági kultúrát, és indítson oktatási és figyelemfelkeltő kampányokat annak érdekében, hogy a polgárok képesek legyenek a tájékozott döntésre a tekintetben, hogy mely személyes adatokat osztanak meg az interneten, és miként védjék azokat megfelelőbb módon, ideértve a titkosítás és a biztonságos számításifelhő-szolgáltatások révén való védelmet, teljes mértékben igénybe véve az egyetemes szolgáltatási irányelvben előírt közérdekű tájékoztatási platformot;

110. felhívja a Bizottságot, hogy 2014 decemberéig tegyen javaslatot olyan jogszabályokra, amelyek a szoftver- és hardvergyártókat arra ösztönzik, hogy termékeikbe kialakításuk és alapértelmezett tulajdonságok révén nagyobb fokú védelmet és adatvédelmet építsenek be többek között azáltal, hogy akadályozzák az indokolatlan és aránytalan tömeges adatgyűjtést, illetve bevezetik a gyártók kijavítatlan ismert biztonsági résekért, hibás vagy nem biztonságos termékekért vagy a jogellenes hozzáférést és adatfeldolgozást lehetővé tevő titkos „hátsó ajtók" beépítéséért való jogi felelősségét; e tekintetben arra kéri a Bizottságot, hogy mérlegelje a számítástechnikai hardverek tanúsítására vagy hitelesítésére szolgáló rendszer kialakításának lehetőségét, amely uniós szintű vizsgálati eljárásokat is magában foglal a termékek integritásának és biztonságának garantálása érdekében;

A bizalom helyreállítása

111. meggyőződése, hogy a vizsgálat – a jogszabály-módosítások szükségszerűségén túl – igazolta, hogy az USA-nak helyre kell állítania a bizalmat uniós partnereivel, mivel elsődlegesen egyesült államokbeli hírszerző ügynökségek tevékenységei kerültek célkeresztbe;

2014. március 12., szerda

112. rámutat, hogy a létrejött bizalmi válság kiterjed az alábbiakra:

— az Unión belüli együttműködés szellemisége, mivel egyes nemzeti hírszerző ügynökségek veszélyeztethetik az Unió célkitűzéseinek elérését;

— a polgárok, akik ráébredtek, hogy nemcsak harmadik országok és multinacionális vállalatok, de saját kormányaik is kémkedhetnek utánuk;

— a digitális társadalomban az alapvető jogok, a demokrácia és a jogállamiság tisztelete, valamint a demokratikus, igazságügyi és parlamentáris biztosítékok hitelessége és felügyelete;

Az Európai Unió és az Egyesült Államok viszonyában

113. emlékeztet az Unió tagállamai és az USA közötti fontos, a demokráciába, a jogállamiságba és az alapjogokba vetett hiten alapuló történelmi és stratégiai partnerségekre;

114. meggyőződése, hogy az USA részéről a polgárok tömeges megfigyelése és a politikai vezetők utáni kémkedés komoly károkat okozott az EU és az USA kapcsolataiban, és kedvezőtlen hatást gyakorolt az Unióban működő egyesült államokbeli szervezetekbe vetett bizalomra; ezt tovább súlyosítja az, hogy az uniós polgárokat az USA joga értelmében semmiféle bírósági és közigazgatási jogorvoslat nem illeti meg, különösen a hírszerzési célú megfigyelési tevékenységekkel kapcsolatos ügyekben;

115. elismeri – az Unió és az USA előtt álló globális kihívásokra figyelemmel –, hogy a transzatlanti partnerséget tovább kell erősíteni, és hogy létfontosságú a terrorizmusellenes transzatlanti együttműködés folytatódása a jogállamiság valódi közös tiszteletben tartásán és a válogatás nélküli tömeges megfigyelések elutasításán alapuló bizalom új alapjaira építve; ezért ragaszkodik ahhoz, hogy az USA-nak egyértelmű intézkedéseket kell hoznia a bizalom újbóli kiépítésére és a partnerség alapját képező közös alapértékek újbóli hangsúlyozására;

116. készen áll az egyesült államokbeli partnerekkel folytatott párbeszédre annak érdekében, hogy a megfigyelés reformjáról és a hírszerzési felügyelet felülvizsgálatáról folyó amerikai nyilvános és kongresszusi vita során garantálják az uniós polgárok és lakosok vagy az uniós jog védelme alatt álló más személyek magánélethez való jogait és más jogait, továbbá az USA bíróságain az azonos tájékoztatási jogot és adatvédelmet, ideértve a bírósági jogorvoslatot is, többek között az adatvédelmi törvény és az elektronikus távközlési adatvédelmi törvény felülvizsgálatán, valamint a Polgári és Politikai Jogok Nemzetközi Egyezségokmánya (ICCPR) első fakultatív jegyzőkönyvének ratifikálásán keresztül annak érdekében, hogy véget vessenek a jelenlegi megkülönböztetésnek;

117. ragaszkodik a szükséges reformok elvégzéséhez és az európaiak számára tényleges garanciák nyújtásához annak biztosítására, hogy a külföldi hírszerzési célokat szolgáló megfigyelés és adatfeldolgozás arányos legyen, egyértelműen meghatározott feltételekre korlátozódjon, és a terrorista tevékenységek megalapozott gyanújához és gyanúokhoz kapcsolódjon; hangsúlyozza, hogy ezt a célt átlátható bírósági felügyeletnek kell alávetni;

118. megítélése szerint egyértelmű politikai jelzésekre van szükség amerikai partnereink részéről annak demonstrálására, hogy az USA különbséget tesz szövetséges és ellenség között;

119. szorgalmazza, hogy a Bizottság és az USA kormányzata a bűnüldözési célú adattovábbításról szóló EU–USA keretmegállapodásról folyó tárgyalásokkal összefüggésben rendezze az uniós polgárok tájékoztatáshoz és bírósági jogorvoslathoz való jogát, és e tárgyalásokat – az EU–USA igazságügyi és belügyminiszterek 2013. november 18-i miniszteri találkozóján tett kötelezettségvállalással összhangban – 2014 nyara előtt fejezze be;

120. szorgalmazza, hogy az USA csatlakozzon az Európa Tanács személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezményéhez (108. egyezmény), ahogy csatlakozott a számítógépes bűnözésről szóló 2001. évi egyezményhez, ezzel erősítve a transzatlanti szövetségesek közötti közös jogalapot;

121. felhívja az uniós intézményeket, hogy tárják fel az USA-val egy olyan magatartási kódex létrehozásának lehetőségét, amely garantálná, hogy uniós intézmények és létesítmények ellen ne folyjon egyesült államokbeli kémtevékenység;

Az Európai Unión belül

122. egyben meggyőződése, hogy az uniós tagállamok részvétele és tevékenységei bizalomvesztéshez vezettek egyebek mellett a tagállamok között, valamint a polgárok és saját nemzeti hatóságaik között; véleménye szerint csak a megfigyelés célját és eszközeit illető teljes átláthatósággal, nyilvános vitával és végső soron a jogszabályok felülvizsgálatával – amelynek része a tömeges megfigyelési tevékenységek felszámolása, valamint a bírósági és parlamenti felügyelet megerősítése –, lesz lehetséges az elveszett bizalom helyreállítása; újra felhívja a figyelmet az átfogó uniós biztonsági politikák kidolgozásának nehézségeire, miközben tömeges megfigyelési tevékenységek zajlanak, és hangsúlyozza, hogy a lojális együttműködés uniós elve megköveteli azt, hogy a tagállamok tartózkodjanak a többi tagállam területén végzett hírszerzési tevékenységektől;

123. megjegyzi, hogy egyes tagállamok kétoldalú kommunikációt folytatnak az USA hatóságaival a kémkedéssel kapcsolatos állításokról, és hogy némelyikük megkötött (az Egyesült Királyság) vagy megkötni tervez (Németország, Franciaország) ún. kémkedésellenes megállapodásokat; hangsúlyozza, hogy ezeknek a tagállamoknak teljes mértékben tiszteletben kell tartaniuk az Unió egészének érdekeit; véleménye szerint az ilyen kétoldalú megállapodások kontraproduktívak és nem játszanak fontos szerepet, mivel ez a probléma európai szintű megközelítést tesz szükségessé; kéri a Tanácsot, hogy tájékoztassa a Parlamentet azokról a fejleményekről, amelyeket a tagállamok az uniós szintű, kölcsönös kémkedésellenes megállapodás tekintetében elértek;

124. megítélése szerint ezek a megállapodások nem ütközhetnek az uniós szerződésekbe, különösen a(z EUSZ 4. cikkének (3) bekezdése szerinti) lojális együttműködés elvébe, illetve nem gyengíthetik az uniós politikákat általánosságban, illetve konkrétan a belső piacot, a tisztességes versenyt, valamint a gazdasági, ipari és társadalmi fejlődést; úgy határoz, hogy minden ilyen megállapodás esetében megvizsgálja annak az európai joggal való összeegyeztethetőségét, valamint fenntartja a jogot a Szerződés szerinti eljárások igénybevételére, amennyiben ezek a megállapodások az uniós kohézióba vagy az Unió alapját képező alapvető elvekbe ütköznek;

125. felszólítja a tagállamokat, hogy tegyenek meg minden erőfeszítést a jobb együttműködés biztosításáért, szem előtt tartva a kémtevékenységekkel szembeni biztosítékok nyújtását a megfelelő uniós testületekkel és ügynökségekkel együttműködve az uniós polgárok és intézmények, az európai vállalatok, az uniós ipar, valamint informatikai infrastruktúrák és hálózatok, továbbá az európai kutatás érdekében; úgy véli, hogy a hatékony információcserének alapfeltétele az uniós érdekelt felek tevékeny részvétele; rámutat, hogy a biztonsági fenyegetések nemzetközi jellege erősödött, még szétszórtabbá és összetettebbé váltak, így fokozott európai együttműködést tesznek szükségessé; úgy véli, hogy Szerződéseknek jobban tükrözniük kellene a kialakult helyzetet, és ezért a Szerződések felülvizsgálatát kéri a tagállamok és az Unió közötti lojális együttműködés fogalmának erősítése érdekében, tekintettel a biztonság térsége megteremtésére irányuló célra, valamint az Unión belül a tagállamok közötti kölcsönös kémtevékenységek megelőzése érdekében;

126. feltétlenül szükségesnek tartja, hogy minden fontos uniós intézmény és uniós küldöttség lehallgatásbiztos kommunikációs rendszerekkel (elektronikus levelezés és távközlés, ideértve a vezetékes és mobiltelefonokat is), valamint lehallgatásbiztos tárgyalókkal rendelkezzen; ezért egy titkosított belső uniós elektronikus levelezőrendszer kialakítását szorgalmazza;

127. felszólítja a Tanácsot és a Bizottságot, hogy további késedelem nélkül hagyják jóvá 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, az Európai Parlament Parlament által 2012. május 23-án elfogadott rendeletjavaslatot, amelynek benyújtására az EUMSZ 226. cikke alapján került sor; a Szerződés felülvizsgálatát kéri annak érdekében, hogy az ilyen vizsgálati hatásköröket korlátozások és kivételek nélkül terjesszék ki az uniós hatáskör vagy fellépés minden területére, továbbá hogy a Szerződés tartalmazza az eskü alatti kihallgatás lehetőségét;

Nemzetközi szinten

128. felszólítja a Bizottságot, hogy legkésőbb 2015 januárjáig terjesszen be uniós stratégiát az internet demokratikus irányításáról;

2014. március 12., szerda

129. felhívja a tagállamokat, hogy kövessék az adatvédelmi és a magánélet védelmével foglalkozó biztosok 35. nemzetközi konferenciájának felhívását, hogy „támogassák az ENSZ Polgári és Politikai Jogok Nemzetközi Egyezségokmányának 17. cikkéhez kiegészítő jegyzőkönyv elfogadását, amelynek a nemzetközi konferencia által kialakított és jóváhagyott normákon és az Emberi Jogi Bizottság által az Egyezségokmányhoz fűzött 16. sz. általános megjegyzésen kell alapulniuk annak érdekében, hogy a jogállamisággal összhangban létrejöjjenek az adatvédelem és a magánélet védelme globálisan irányadó normái"; felszólítja a tagállamokat, hogy ennek keretében egyúttal szorgalmazzák egy olyan nemzetközi ENSZ-ügynökség létrehozását, amelynek feladata különösen a megjelenő megfigyelési eszközök nyomon követése, valamint használatuk szabályozása és kivizsgálása; felkéri a főképviselőt/a Bizottság alelnökét és az Európai Külügyi Szolgálatot kezdeményező hozzáállás tanúsítására;

130. felhívja a tagállamokat, hogy az ENSZ-en belül következetes és erőteljes stratégiát dolgozzanak ki, támogatva különösen a Brazília és Németország által kezdeményezett, a „Magánélethez való jog a digitális érában" című, az ENSZ Közgyűlés harmadik bizottsága (Emberi Jogi Bizottság) által 2013. november 27-én elfogadott határozatot, valamint további intézkedéseket hozva a magánélethez és az adatvédelemhez való alapvető jogok nemzetközi szintű védelmére, egyúttal elkerülve az állami ellenőrzést, vagy cenzúrát, vagy az internet széttöredezését, ideértve a tömeges megfigyelési tevékenységeket tiltó nemzetközi szerződés és az annak felügyeletét ellátó ügynökség kezdeményezését;

Prioritási terv: Európai digitális habeas corpus – az alapvető jogok védelme a digitális korban

131. úgy határoz, hogy a következő jogalkotási ciklusra szóló prioritási tervként benyújtja az uniós polgároknak, intézményeknek és tagállamoknak a fent említett ajánlásokat; az EUMSZ 265. cikkével összhangban felszólítja a Bizottságot és az ezen állásfoglalásban említett többi uniós intézményt, szervet, hivatalt és ügynökséget, hogy tegyenek eleget az ezen állásfoglalásban kifejtett ajánlásoknak és felhívásoknak;

132. úgy határoz, hogy az alábbi 8 fellépéssel elindítja az „Európai digitális habeas corpus – az alapvető jogok védelme a digitális korban" című kezdeményezést, amelynek végrehajtását felügyeli:

— 1. fellépés: Az adatvédelmi intézkedéscsomag elfogadása 2014-ben;

— 2. fellépés: A polgároknak a magánélet védelméhez és az adatvédelemhez való alapvető jogát garantáló, valamint az uniós polgárok számára többek között az EU-ból az USA-ba bűnüldözési célokból történő adattovábbítás esetére megfelelő jogorvoslati mechanizmust biztosító EU–USA keretmegállapodás megkötése;

— 3. fellépés: A teljes felülvizsgálat elvégzéséig és a jelenlegi joghézagok megszüntetéséig a „védett adatkikötő" felfüggesztése, biztosítva, hogy a személyes adatok Unióból az USA-ba történő kereskedelmi célú továbbítása a legmagasabb szintű uniós normáknak megfelelően történjen;

— 4. fellépés: A TFTP-megállapodás felfüggesztése (i) a keretmegállapodásra vonatkozó tárgyalások befejezéséig; (ii) az uniós elemzés alapján lefolytatott alapos vizsgálat elvégzéséig és a Parlament 2013. október 23-i állásfoglalásában felvetett összes aggály megnyugtató rendezéséig;

— 5. fellépés: A személyes adatokat érintő bármiféle megállapodás, mechanizmus vagy harmadik országokkal folytatott információcsere értékelése annak biztosítása érdekében, hogy a megfigyelési tevékenységek révén ne sértsék meg a magánélethez és a személyes adatok védelméhez való jogot, továbbá a szükséges nyomonkövetési intézkedések meghozatala;

— 6. fellépés: A jogállamiság és az uniós polgárok alapvető jogainak védelme (többek között a sajtószabadságra irányuló fenyegetésektől), a nyilvánosság pártatlan tájékoztatáshoz való jogának és a szakmai titoktartás védelme (ideértve az ügyvédi titoktartást), valamint a visszaélést jelentő személyek fokozott védelme;

— 7. fellépés: Az európai informatikai függetlenségi stratégia kidolgozása („új digitális megállapodás", ideértve a megfelelő források elkülönítését nemzeti és uniós szinten) annak érdekében, hogy fellendüljön a számítástechnikai ágazat és az európai vállalatok kihasználhassák az uniós adatvédelemből adódó versenyelőnyt;

— 8. fellépés: Annak biztosítása, hogy az Unió úttörő szerepet játsszon az internet demokratikus és semleges igazgatásának előmozdítása terén;

133. felszólítja az uniós intézményeket és a tagállamokat az „Európai digitális habeas corpus – az alapvető jogok védelme a digitális korban” című kezdeményezés támogatására; vállalja, hogy az uniós polgárok jogainak hirdetőjeként jár el, a végrehajtás nyomon követésének alábbi menetrendjét követve:

— 2014. április – 2015. május: A LIBE vizsgálócsoport mintájára ellenőrző csoport felállítása, amely a vizsgálati felhatalmazással kapcsolatos, újonnan napvilágot látott fejlemények nyomon követéséért és ezen állásfoglalás végrehajtásának ellenőrzéséért felelős;

— 2014. júliustól: Állandó adattovábbítás- és jogorvoslat-felügyeleti mechanizmus létrehozása az illetékes bizottságon belül.

— 2014 tavasza: Az Európai Tanács hivatalos felszólítása arra, hogy az „Európai digitális habeas corpus – az alapvető jogok védelme a digitális korban” című kezdeményezést foglalják bele az EUMSZ 68. cikke értelmében elfogadandó iránymutatásokba.

— 2014 ősze: Arra irányuló kötelezettségvállalás, hogy az „Európai digitális habeas corpus – az alapvető jogok védelme a digitális korban” című kezdeményezés és a kapcsolódó ajánlások kulcskritériumot képeznek a következő Bizottság jóváhagyása tekintetében;

— 2014: Az informatikai ágazathoz kapcsolódó különféle területek (ideértve a matematikát, a kriptográfiát és az adatvédelmet fokozó technológiákat) magas szintű európai szakértőit egy asztalhoz ültető konferencia, amely elősegíti a következő jogalkotási ciklusra szóló uniós informatikai stratégia kidolgozását;

— 2014-2015: Rendszeresen ülésező bizalmi, adatvédelmi és polgárjogi csoport létrehozása az Európai Parlament és az Egyesült Államok Kongresszusa, valamint más elkötelezett harmadik országok (például Brazília) parlamentjei között;

— 2014-2015: Konferencia az európai nemzeti parlamentek hírszerzést felügyelő testületeivel;

o

o o

134. utasítja elnökét, hogy továbbítsa ezt az állásfoglalást az Európai Tanácsnak, a Tanácsnak, a Bizottságnak, a tagállamok parlamentjeinek és kormányainak, a nemzeti adatvédelmi hatóságoknak, az európai adatvédelmi biztosnak, az eu-LISA-nak, az ENISA-nak, az Alapjogi Ügynökségnek, a 29. cikk szerinti munkacsoportnak, az Európa Tanácsnak, az Amerikai Egyesült Államok Kongresszusának, az USA kormányának, a Brazil Szövetségi Köztársaság elnökének, kormányának és parlamentjének, és az Egyesült Nemzetek főtitkárának.

135. utasítja Állampolgári Jogi, Bel- és Igazságügyi Bizottságát, hogy ezen állásfoglalás elfogadása után egy évvel a Parlament plenáris ülésén foglalkozzon ezzel az üggyel; alapvető fontosságúnak tartja megvizsgálni, hogy a Parlament által elfogadott ajánlásokat milyen mértékben valósították meg, illetve elemezni azokat az eseteket, amikor nem követték ezeket az ajánlásokat;