Streda 12. marca 2014

P7_TA(2014)0230

Programy sledovania Národnej bezpečnostnej agentúry USA, orgány sledovania v jednotlivých členských štátoch a vplyv na základné práva občanov EÚ

Uznesenie Európskeho parlamentu z 12. marca 2014 o programe sledovania Národnej bezpečnostnej agentúry Spojených štátov amerických, orgánoch sledovania v jednotlivých členských štátoch a ich vplyve na základné práva občanov EÚ a na transatlantickú spoluprácu v oblasti spravodlivosti a vnútorných vecí (2013/2188(INI))

(2017/C 378/14)

Európsky parlament,

— so zreteľom na Zmluvu o Európskej únii (ZEÚ), a najmä na jej články 2, 3, 4, 5, 6, 7, 10, 11 a 21,

— so zreteľom na Zmluvu o fungovaní Európskej únie (ZFEÚ), a najmä na jej články 15, 16 a 218 a hlavu V,

— so zreteľom na Protokol č. 36 o prechodných ustanoveniach, na jeho článok 10 a na vyhlásenie č. 50 týkajúce sa tohto protokolu,

— so zreteľom na Chartu základných práv Európskej únie, a najmä na jej články 1, 3, 6, 7, 8, 10, 11, 20, 21, 42, 47, 48 a 52,

— so zreteľom na Európsky dohovor o ľudských právach, a najmä na jeho články 6, 8, 9, 10 a 13 a jeho protokoly,

— so zreteľom na Všeobecnú deklaráciu ľudských práv, a najmä na jej články 7, 8, 10, 11, 12 a 14 ([1]),

— so zreteľom na Medzinárodný pakt o občianskych a politických právach, a najmä na jeho články 14, 17, 18 a 19,

— so zreteľom na Dohovor Rady Európy o ochrane údajov (ETS č. 108) a na Dodatkový protokol z 8. novembra 2001 k Dohovoru o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov týkajúceho sa orgánov dozoru a cezhraničných tokov údajov (ETS č. 181),

— so zreteľom na Viedenský dohovor o diplomatických stykoch, a najmä na jeho články 24, 27 a 40,

— so zreteľom na Dohovor Rady Európy o počítačovej kriminalite (ETS č. 185),

— so zreteľom na správu osobitného spravodajcu Organizácie Spojených národov o podpore a ochrane ľudských práv a základných slobôd v boji proti terorizmu predloženú 17. mája 2010 ([2]),

— so zreteľom na oznámenie Komisie s názvom Politika a riadenie v oblasti internetu – Úloha Európy pri formovaní budúcnosti riadenia internetu (COM(2014)0072);

— so zreteľom na správu osobitného spravodajcu Organizácie Spojených národov o podpore a ochrane práva na slobodu presvedčenia a prejavu predloženú 17. apríla 2013 ([3]),

— so zreteľom na usmernenia k ľudským právam a boju proti terorizmu prijaté Výborom ministrov Rady Európy 11. júla 2002,

([1]) http://www.un.org/en/documents/udhr/.
([2]) http://daccess-dds-ny.un.org/doc/UNDOC/LTD/G12/134/10/PDF/G1214710.pdf?OpenElement.
([3]) http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

— so zreteľom na Bruselské vyhlásenie zo 6. konferencie parlamentných výborov pre dohľad nad spravodajskými a bezpečnostnými službami členských štátov Európskej únie z 1. októbra 2010,

— so zreteľom na uznesenie Parlamentného zhromaždenia Rady Európy č. 1954 (2013) o národnej bezpečnosti a prístupe k informáciám,

— so zreteľom na správu o demokratickom dohľade nad bezpečnostnými službami prijatú Benátskou komisiou 11. júna 2007 ([1]) a s veľkým očakávaním jej aktualizácie naplánovanej na jar roku 2014,

— so zreteľom na výpovede zástupcov výborov pre dohľad nad spravodajskými službami Belgicka, Holandska, Dánska a Nórska,

— so zreteľom na veci podané na francúzske ([2]), poľské a britské súdy ([3]), ako aj na Európsky súd pre ľudské práva ([4]) v súvislosti so systémami hromadného dohľadu,

— so zreteľom na Európsky dohovor ustanovený Radou v súlade s článkom 34 Zmluvy o Európskej únii o vzájomnej pomoci v trestných veciach medzi členskými štátmi Európskej únie ([5]), a najmä na jeho hlavu III,

— so zreteľom na rozhodnutie Komisie 2000/520/ES z 26. júla 2000 o primeranosti ochrany poskytovanej zásadami bezpečného prístavu a súvisiacimi často kladenými otázkami vydanými Ministerstvom obchodu Spojených štátov amerických,

— so zreteľom na hodnotiace správy Komisie o vykonávaní zásad bezpečného prístavu z 13. februára 2002 (SEC(2002)0196) a z 20. októbra 2004 (SEC(2004)1323),

— so zreteľom na oznámenie Komisie z 27. novembra 2013 o fungovaní bezpečného prístavu z pohľadu občanov EÚ a spoločností so sídlom v EÚ (COM(2013)0847) a na oznámenie Komisie z 27. novembra 2013 o obnovení dôvery v dátové toky medzi EÚ a USA (COM(2013)0846),

— so zreteľom na svoje uznesenie z 5. júla 2000 o návrhu rozhodnutia Komisie o primeranosti ochrany poskytovanej zásadami bezpečného prístavu a súvisiacimi často kladenými otázkami vydanými Ministerstvom obchodu Spojených štátov amerických ([6]), ktorý zaujal stanovisko, že primeranosť systému nebolo možné potvrdiť, a na stanoviská pracovnej skupiny zriadenej podľa článku 29, konkrétne na stanovisko 4/2000 zo 16. mája 2000 ([7]),

— so zreteľom na dohody medzi Spojenými štátmi americkými a Európskou úniou o využívaní a postupovaní osobných záznamov o cestujúcich (dohoda o PNR) z rokov 2004, 2007 ([8]) a 2012 ([9]),

— so zreteľom na spoločné preskúmanie vykonávania dohody medzi EÚ a Spojenými štátmi o využívaní osobných záznamov o cestujúcich a ich postupovaní Ministerstvu vnútornej bezpečnosti Spojených štátov amerických ([10]), ktoré je priložené k správe Komisie Európskemu parlamentu a Rade o spoločnom preskúmaní (COM(2013)0844),

---

([1]) http://www.venice.coe.int/webforms/documents/CDL-AD(2007)016.aspx.
([2]) La Fédération Internationale des Ligues des Droits de l'Homme a La Ligue française pour la défense des droits de l'Homme et du Citoyen proti X; Súd prvého stupňa v Paríži..
([3]) Veci predložené organizáciou Privacy International a organizáciou Liberty vyšetrujúcemu orgánu (Investigatory Powers Tribunal).
([4]) Spoločné uplatňovanie na základe článku 34 Big Brother Watch, Open Rights Group, English PEN a Dr Constanze Kurz (žalobcovia) proti Spojenému kráľovstvu (odporca).
([5]) Ú. v. ES C 197, 12.7.2000, s. 1.
([6]) Ú. v. ES C 121, 24.4.2001, s. 152.
([7]) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp32en.pdf.
([8]) Ú. v. EÚ L 204, 4.8.2007, s. 18.
([9]) Ú. v. EÚ L 215, 11.8.2012, s. 5.
([10]) SEC(2013)0630, 27.11.2013.

Streda 12. marca 2014

— so zreteľom na stanovisko generálneho advokáta Cruza Villalóna so záverom, že smernica 2006/24/ES o uchovávaní údajov vytvorených alebo spracovaných v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb alebo verejných komunikačných sietí je ako celok v rozpore s článkom 52 ods. 1 Charty základných práv Európskej únie a že jej článok 6 je v rozpore s článkom 7 a článkom 52 ods. 1 charty ([1]),

— so zreteľom na rozhodnutie Rady 2010/412/EÚ z 13. júla 2010 o uzavretí Dohody medzi Európskou úniou a Spojenými štátmi americkými o spracovaní a zasielaní údajov obsiahnutých vo finančných správach z Európskej únie do Spojených štátov amerických na účely Programu na sledovanie financovania terorizmu (TFTP) ([2]) a na sprievodné vyhlásenia Komisie a Rady,

— so zreteľom na Dohodu o vzájomnej právnej pomoci medzi Európskou úniou a Spojenými štátmi americkými ([3]),

— so zreteľom na prebiehajúce rokovania o rámcovej dohode medzi EÚ a Spojenými štátmi americkými o ochrane osobných údajov pri ich prenose a spracúvaní na účely predchádzania trestným činom vrátane terorizmu a ich vyšetrovania, odhaľovania alebo stíhania v rámci policajnej a justičnej spolupráce v trestných veciach (tzv. zastrešujúca dohoda),

— so zreteľom na nariadenie Rady (ES) č. 2271/96 z 22. novembra 1996 o ochrane pred účinkami uplatňovania právnych predpisov prijatých treťou krajinou mimo jej územia a pred účinkami opatrení na nich založených alebo z nich vyplývajúcich ([4]),

— so zreteľom na vyhlásenie prezidenta Brazílskej federatívnej republiky na otvorení 68. zasadnutia Valného zhromaždenia OSN, ktoré sa konalo 24. septembra 2013, a na prácu, ktorý vykonal Parlamentný výbor na vyšetrovanie špionáže zriadený federálnym senátom Brazílie,

— so zreteľom na vlastenecký zákon Spojených štátov, ktorý prezident George W. Bush podpísal 26. októbra 2001,

— so zreteľom na zákon o dohľade a zahraničnom poskytovaní informácií (FISA) z roku 1978 a na pozmeňujúci zákon FISA z roku 2008,

— so zreteľom na vykonávacie nariadenie č. 12333, ktoré prezident Spojených štátov amerických vydal v roku 1981 a ktoré bolo zmenené v roku 2008,

— so zreteľom na politickú smernicu prezidenta (PPD-28) o signálnom spravodajstve, ktorú vydal prezident Barack Obama 17. januára 2014,

— so zreteľom na legislatívne návrhy, ktoré v súčasnosti skúma Kongres Spojených štátov vrátane návrhu zákona Spojených štátov o slobode, návrhu zákona o dohľade nad spravodajskými službami a reforme sledovania a ďalších,

— so zreteľom na preskúmania vykonané Radou pre dohľad nad ochranou súkromia a občianskymi slobodami, Národnou bezpečnostnou radou Spojených štátov a prezidentskou skupinou skúmajúcou spravodajské a komunikačné technológie, najmä na správu tejto prezidentskej skupiny z 12. decembra 2013 s názvom Sloboda a bezpečnosť v meniacom sa svete,

— so zreteľom na rozsudok okresného súdu Spojených štátov amerických pre federálny dištrikt Kolumbia vo veci Klayman a iní proti Obamovi a iným, civilné konanie č. 13-0851 zo 16. decembra 2013, a na rozsudok okresného súdu Spojených štátov amerických pre okres New York-juh vo veci ACLU a iní proti Jamesovi R. Clapperovi a iným, civilné konanie č. 13-3994 z 11. júna 2013,

— so zreteľom na správu o zisteniach spolupredsedov EÚ pracovnej skupiny ad hoc EÚ – Spojené štáty pre ochranu údajov z 27. novembra 2013 ([5]),

([1]) Stanovisko generálneho advokáta Cruza Villalóna z 12. decembra 2013 vo veci C-293/12.
([2]) Ú. v. EÚ L 195, 27.7.2010, s. 3.
([3]) Ú. v. EÚ L 181, 19.7.2003, s. 34.
([4]) Ú. v. ES L 309, 29.11.1996, s. 1.
([5]) Dokument Rady 16987/2013.

— so zreteľom na svoje uznesenia z 5. septembra 2001 ([1]) a 7. novembra 2002 ([2]) o existencii globálneho systému na odpočúvanie súkromnej a obchodnej komunikácie (odpočúvací systém ECHELON),

— so zreteľom na svoje uznesenie z 21. mája 2013 o charte EÚ: stanovenie noriem pre slobodu médií v EÚ ([3]),

— so zreteľom na svoje uznesenie zo 4. júla 2013 o programe sledovania Národnej bezpečnostnej agentúry Spojených štátov, orgánoch sledovania v rôznych členských štátoch a ich vplyve na občanov EÚ ([4]), v ktorom poveril svoj Výbor pre občianske slobody, spravodlivosť a vnútorné veci, aby uskutočnil dôkladné preskúmanie tejto záležitosti,

— so zreteľom na pracovný dokument č. 1 o programoch sledovania Spojených štátov a EÚ a ich vplyve na základné práva občanov EÚ,

— so zreteľom na pracovný dokument č. 3 o vzťahu medzi postupmi sledovania v EÚ a Spojených štátoch a ustanoveniami EÚ na ochranu údajov,

— so zreteľom na pracovný dokument č. 4 o činnostiach sledovania Spojených štátov, pokiaľ ide o údaje EÚ a ich možné právne dôsledky pre transatlantické dohody a spoluprácu,

— so zreteľom na pracovný dokument č. 5 o demokratickom dohľade nad spravodajskými službami členských štátov a spravodajskými orgánmi EÚ,

— so zreteľom na pracovný dokument Výboru pre zahraničné veci s názvom Aspekty zahraničnej politiky súvisiace s vyšetrovaním hromadného sledovania občanov EÚ elektronickými prostriedkami;

— so zreteľom na svoje uznesenie z 23. októbra 2013 o organizovanej trestnej činnosti, korupcii a praní špinavých peňazí: odporúčania týkajúce sa opatrení a iniciatív, ktoré sa majú vykonať ([5]),

— so zreteľom na svoje uznesenie z 23. októbra 2013 o pozastavení dohody TFTP v dôsledku sledovania Národnou bezpečnostnou agentúrou Spojených štátov ([6]),

— so zreteľom na svoje uznesenie z 10. decembra 2013 o uvoľnení potenciálu cloud computingu v Európe ([7]),

— so zreteľom na Medziinštitucionálnu dohodu medzi Európskym parlamentom a Radou o postupovaní utajovaných skutočností, ktorých držiteľom je Rada a ktoré sa týkajú záležitostí mimo oblasti spoločnej zahraničnej a bezpečnostnej politiky, Európskemu parlamentu a o zaobchádzaní s takýmito skutočnosťami Európskym parlamentom ([8]),

— so zreteľom na prílohu VIII rokovacieho poriadku,

— so zreteľom na článok 48 rokovacieho poriadku,

— so zreteľom na správu Výboru pre občianske slobody, spravodlivosť a vnútorné veci (A7-0139/2014),

Vplyv hromadného sledovania

A. keďže ochrana údajov a súkromia patria medzi základné práva; keďže bezpečnostné opatrenia vrátane protiteroristických sa musia uplatňovať v súlade so zásadami právneho štátu a musia podliehať záväzkom v oblasti základných práv vrátane práv týkajúcich sa ochrany súkromia a údajov;

([1]) Ú. v. EÚ C 72 E, 21.3.2002, s. 221.
([2]) Ú. v. EÚ C 16 E, 22.1.2004, s. 88.
([3]) Prijaté texty, P7_TA(2013)0203.
([4]) Prijaté texty, P7_TA(2013)0322.
([5]) Prijaté texty, P7_TA(2013)0444.
([6]) Prijaté texty, P7_TA(2013)0449.
([7]) Prijaté texty, P7_TA(2013)0535.
([8]) Ú. v. EÚ C 353 E, 3.12.2013, s. 156.

Streda 12. marca 2014

B. keďže informačné toky a údaje, ktoré dnes dominujú bežnému každodennému životu a ktoré sú súčasťou nedotknuteľnosti každého z nás, je potrebné chrániť proti neoprávnenému vniknutiu rovnako ako súkromné obydlia;

C. keďže väzby medzi Európou a Spojenými štátmi americkými sú založené na myšlienke a zásadách demokracie a právneho štátu, slobody, spravodlivosti a solidarity;

D. keďže spolupráca medzi Spojenými štátmi a Európskou úniou a jej členskými štátmi v oblasti boja proti terorizmu má aj naďalej kľúčový význam pre bezpečnosť a ochranu obidvoch partnerov;

E. keďže vzájomná dôvera a porozumenie sú kľúčovými faktormi transatlantického dialógu a partnerstva;

F. keďže po 11. septembri 2001 sa boj proti terorizmu stal jednou z najdôležitejších priorít väčšiny vlád; keďže z odhalení založených na uniknutých dokumentoch poskytnutých Edwardom Snowdenom, bývalým spolupracovníkom NSA, vyplýva pre politických predstaviteľov povinnosť riešiť problémy dohľadu a kontroly spravodajských agentúr, pokiaľ ide o činnosti sledovania, a vyhodnotiť vplyv ich činností na základné práva a zásady právneho štátu v demokratickej spoločnosti;

G. keďže odhalenia vyvolali v EÚ od júna 2013 veľa obáv, pokiaľ ide o:

— rozsah systémov sledovania odhalených v Spojených štátoch a v členských štátoch EÚ,

— porušenie právnych noriem EÚ, základných práv a noriem ochrany údajov,

— úroveň dôvery medzi EÚ a Spojenými štátmi ako transatlantickými partnermi,

— stupeň spolupráce a zapojenia určitých členských štátov EÚ, pokiaľ ide o programy sledovania Spojených štátov alebo rovnocenné programy na vnútroštátnej úrovni, ako odhalili médiá,

— nedostatok kontroly a účinného dohľadu politických orgánov Spojených štátov a niektorých členských štátov EÚ nad svojimi spravodajskými službami,

— možnosť, že tieto operácie hromadného dohľadu sa využívajú na iné účely, než sú národná bezpečnosť a striktný boj proti terorizmu, napríklad na hospodársku a priemyselnú špionáž alebo na vytváranie profilov z politických dôvodov,

— narušenie slobody tlače a komunikácie príslušníkov profesií s právom na zachovanie dôvernosti vrátane právnych zástupcov a lekárov;

— príslušné úlohy a stupeň zapojenia spravodajských agentúr a súkromných spoločností IT a telekomunikačných spoločností,

— čoraz nejasnejšie hranice medzi presadzovaním práva a spravodajskými činnosťami, čo vedie k tomu, že sa s každým občanom zaobchádza ako s podozrivou osobou, ktorú treba sledovať,

— hrozby pre súkromie v digitálnej ére a dôsledky hromadného sledovania na občanov a spoločnosti;

H. keďže neobvyklý rozsah odhalenej špionáže si vyžaduje, aby ju orgány Spojených štátov, európske inštitúcie, vlády, národné parlamenty a justičné orgány členských štátov dôkladne vyšetrili;

I. keďže orgány Spojených štátov popreli niektoré z odhalených informácií ale proti drvivej väčšine nenamietali; keďže v Spojených štátoch a v niektorých členských štátoch EÚ sa rozprúdila rozsiahla verejná diskusia; keďže vlády a parlamenty EÚ ostávajú príliš často ticho a nepristupujú k primeranému vyšetrovaniu;

J. keďže prezident Obama nedávno oznámil reformu NSA a jej programov sledovania;

K. keďže v porovnaní s krokmi, ktoré podnikli inštitúcie EÚ aj niektoré členské štáty EÚ, sa Európsky parlament s plnou vážnosťou ujal svojej povinnosti ozrejmiť nerozvážne praktiky hromadného sledovania občanov EÚ a prostredníctvom svojho uznesenia zo 4. júla 2013 o programe sledovania Národnej bezpečnostnej agentúry Spojených štátov amerických, orgánoch sledovania v jednotlivých členských štátoch a ich vplyve na základné práva občanov EÚ poveril svoj Výbor pre občianske slobody, spravodlivosť a vnútorné veci, aby vykonal dôkladné prešetrenie tejto záležitosti;

L. keďže je povinnosťou európskych inštitúcií zabezpečiť, aby sa právo EÚ plne vykonávalo v prospech európskych občanov a aby právnu silu zmlúv EÚ nenarušila akceptácia účinkov noriem alebo konaní tretích krajín mimo ich územia bez toho, žeby to vyvolalo akýkoľvek záujem;

Vývoj v Spojených štátoch v súvislosti s reformou spravodajských služieb

M. keďže okresný súd federálneho dištriktu Kolumbia vo svojom rozhodnutí zo 16. decembra 2013 rozhodol, že hromadné zhromažďovanie metaúdajov agentúrou NSA je v rozpore so štvrtým dodatkom k ústave Spojených štátov ([1]); keďže však okresný súd okresu New York-juh vo svojom rozhodnutí z 27. decembra 2013 rozhodol, že toto zhromažďovanie je zákonné;

N. keďže okresný súd pre východnú časť Michiganu rozhodol, že v štvrtom dodatku sa vyžaduje uvážlivosť vo všetkých vyšetrovaniach, predchádzajúce oprávnenia na všetky opodstatnené vyšetrovania, oprávnenia založené na vopred existujúcej príčine, ako aj špecifickosť, pokiaľ ide o osoby, miesta a veci, a sprostredkovanie neutrálneho sudcu medzi výkonnými úradníkmi orgánov na presadzovanie práva a občanmi ([2]);

O. keďže skupina vymenovaná prezidentom, ktorá skúma spravodajské a komunikačné technológie, vo svojej správe z 12. decembra 2013 navrhuje 46 odporúčaní pre prezidenta Spojených štátov; keďže v odporúčaniach sa zdôrazňuje potreba chrániť národnú bezpečnosť a zároveň osobné súkromie a občianske slobody; keďže v tejto súvislosti vyzýva vládu Spojených štátov: čo možno najskôr ukončiť hromadné zhromažďovanie telefónnych záznamov osôb Spojenými štátmi na základe oddielu 215 vlasteneckého zákona; vykonať dôkladné preskúmanie právneho rámca agentúry NSA a spravodajských služieb Spojených štátov s cieľom zabezpečiť dodržiavanie práva na súkromie; zastaviť snahy o rozvracanie alebo o vytvorenie zraniteľného komerčného softvéru (tzv. backdoor a malvér); zintenzívniť používanie šifrovania, najmä v prípade prenášaných údajov a nenarúšať snahy o vytvorenie šifrovacích noriem; vytvoriť funkciu advokáta pre verejný záujem, ktorý bude na súde pre sledovanie zahraničných spravodajských služieb obhajovať súkromie a občianske slobody; Rade pre dohľad nad súkromím a občianskymi slobodami udeliť právomoc na dohľad nad činnosťami spravodajských služieb na účely zahraničných spravodajských služieb, a to nielen na účely boja proti terorizmu; a prijímať sťažností informátorov, využívať zmluvy o vzájomnej právnej pomoci na získanie elektronických komunikácií a nevyužívať sledovanie na odcudzenie priemyselných alebo obchodných tajomstiev;

P. keďže podľa otvoreného vyhlásenia, ktoré predložili bývalí vedúci pracovníci NSA/skupina bývalých pracovníkov spravodajskej služby (VIPS) prezidentovi Obamovi 7. januára 2014 ([3]), hromadné zhromažďovanie údajov nezlepší schopnosť zabrániť budúcim teroristickým útokom; keďže autori zdôrazňujú, že hromadné sledovanie vykonávané agentúrou NSA viedlo k zabráneniu nulového počtu útokov a že sa investovali miliardy do programov, ktoré sú menej účinné a oveľa viac zasahujú do súkromia občanov než domáca technológia nazvaná THINTHREAD, ktorá bola vytvorená v roku 2001;

Q. keďže v súvislosti s činnosťami spravodajských služieb týkajúcimi sa osôb, ktoré nie sú štátnymi príslušníkmi Spojených štátov amerických, na základe oddielu 702 FISA sa v odporúčaniach pre prezidenta Spojených štátov uznáva základná zásada rešpektovania súkromia a ľudskej dôstojnosti ustanovená v článku 12 Všeobecnej deklarácie ľudských práv a v článku 17 Medzinárodného paktu o občianskych a politických právach; keďže sa v nich neodporúča udeliť osobám, ktoré nie sú štátnymi príslušníkmi Spojených štátov, rovnaké práva a ochranu ako štátnym príslušníkom Spojených štátov;

([1]) Klayman a iní proti Obamovi a iným, civilné konanie č. 13-0851, 16. decembra 2013.
([2]) ACLU proti NSA č. 06-CV-10204, 17. augusta 2006.
([3]) http://consortiumnews.com/2014/01/07/nsa-insiders-reveal-what-went-wrong.

Streda 12. marca 2014

R. keďže prezident Spojených štátov Barack Obama vo svojej prezidentskej politickej smernici o signálnom spravodajstve zo 17. januára 2014 a vo svojom následnom prejave vyhlásil, že hromadné sledovanie elektronickými prostriedkami je nevyhnutné pre Spojené štáty na ochranu ich národnej bezpečnosti, občanov a občanov spojencov a partnerov Spojených štátov, ako aj na podporu ich záujmov v zahraničnej politike; keďže táto politická smernica prezidenta obsahuje určité zásady týkajúce sa zhromažďovania, využívania a poskytovania spravodajských údajov a rozširuje niektoré záruky na osoby, ktoré nie sú štátnymi príslušníkmi USA, pričom sčasti budú podliehať rovnakému zaobchádzaniu ako občania Spojených štátov, a to vrátane záruk, pokiaľ ide o osobné údaje všetkých jednotlivcov bez ohľadu na ich štátnu príslušnosť alebo bydlisko; keďže však prezident Obama si nevyžiadal žiadne konkrétne návrhy, najmä pokiaľ ide o legislatívny zákaz činností hromadného sledovania a zavedenia administratívnej a súdnej nápravy pre osoby, ktoré nie sú štátnymi príslušníkmi Spojených štátov;

Právny rámec

Základné práva

S. keďže v správe o zisteniach spolupredsedov EÚ pracovnej skupiny ad hoc EÚ – Spojené štáty pre ochranu údajov sa uvádza prehľad právnej situácie v Spojených štátoch, nezistili sa však skutočnosti o programoch sledovania Spojených štátov; keďže o tzv. pracovnej skupine druhej cesty", v rámci ktorej členské štáty dvojstranne diskutujú s orgánmi Spojených štátov o záležitostiach týkajúcich sa národnej bezpečnosti, neboli zverejnené žiadne informácie;

T. keďže základné práva, najmä sloboda prejavu, sloboda tlače, sloboda myslenia, sloboda svedomia, sloboda náboženského vyznania a združovania, súkromný život, ochrana údajov, ako aj právo na účinný prostriedok nápravy, prezumpcia neviny a právo na spravodlivý proces a nediskrimináciu ustanovené v Charte základných práv Európskej únie a v Európskom dohovore o ľudských právach (EDĽP), sú základnými kameňmi demokracie; keďže hromadné sledovanie ľudí je v rozpore s týmito základnými kameňmi;

U. keďže všetky členské štáty disponujú právnymi predpismi, ktoré chránia dôverné informácie medzi právnym zástupcom a klientom pred odhalením, čo je zásada, ktorú uznáva Súdny dvor EÚ ([1]);

V. keďže vo svojom uznesení z 23. októbra 2013 o organizovanej trestnej činnosti, korupcii a praní špinavých peňazí vyzýva Komisiu, aby predložila legislatívny návrh a vytvorení účinného a komplexného európskeho programu na ochranu informátorov s cieľom chrániť finančné záujmy EÚ a aby okrem toho uskutočnila prieskum, či takého právne predpisy by mali pokrývať aj iné oblasti právomoci Únie;

Právomoci Únie v oblasti bezpečnosti

W. keďže podľa článku 67 ods. 3 ZFEÚ sa EÚ „usiluje o zabezpečenie vysokej úrovne bezpečnosti"; keďže z ustanovení zmluvy (najmä článku 4 ods. 2 ZEÚ, článku 72 ZFEÚ a článku 73 ZFEÚ) vyplýva, že EÚ má určité právomoci vo veciach týkajúcich sa kolektívnej bezpečnosti Únie; keďže EÚ má právomoc vo veciach vnútornej bezpečnosti (článok 4 písm. j) ZFEÚ) a využíva ju pri rozhodovaní o viacerých legislatívnych nástrojoch a uzatváraní medzinárodných dohôd (PNR, TFTP) zameraných na boj proti závažnej trestnej činnosti a terorizmu a pri vypracúvaní stratégie vnútornej bezpečnosti a zriaďovaní agentúr, ktoré v tejto oblasti pracujú;

X. keďže v Zmluve o fungovaní Európskej únie sa uvádza, že „členské štáty môžu spoločne a vo svojej vlastnej zodpovednosti slobodne organizovať formy spolupráce a koordináciu podľa vlastného uváženia medzi príslušnými útvarmi zodpovednými za ochranu národnej bezpečnosti" (článok 73 ZFEÚ);

Y. keďže v článku 276 ZFEÚ sa uvádza, že „pri výkone svojich právomocí týkajúcich sa ustanovení kapitol 4 a 5 hlavy V tretej časti, ktoré sa vzťahujú na priestor slobody, bezpečnosti a spravodlivosti, Súdny dvor Európskej únie nemá právomoc preskúmavať platnosť alebo primeranosť operácií vykonaných políciou alebo inými orgánmi členského štátu presadzujúcimi výkon práva, ani rozhodovať o výkone právomocí členských štátov v oblasti udržiavania verejného poriadku a zabezpečovania vnútornej bezpečnosti";

([1]) Rozsudok z 18. mája 1982 vo veci C-155/79, AM & S Europe Limited proti Komisii Európskych spoločenstiev.

Z. keďže koncepcie „národnej bezpečnosti“, „vnútornej bezpečnosti“, „vnútornej bezpečnosti EÚ“ a „medzinárodnej bezpečnosti“ sa prelínajú; keďže Viedenský dohovor o zmluvnom práve, zásada lojálnej spolupráce medzi členskými štátmi EÚ a zásada práva v oblasti ľudských práv, že akékoľvek výnimky sa interpretujú obmedzene, poukazujú na reštriktívnu interpretáciu pojmu „národnej bezpečnosti“ a vyžadujú, aby členské štáty nezasahovali do právomocí EÚ;

AA. keďže podľa európskych zmlúv je Európska komisia „strážkyňou zmlúv“, a z tohto dôvodu má Komisia zákonnú úlohu vyšetriť každé možné porušenie práva EÚ;

AB. keďže agentúry členských štátov a aj súkromné strany pôsobiace v oblasti národnej bezpečnosti musia v súlade s článkom 6 ZEÚ, ktorý sa týka Charty základných práv EÚ a EDĽP, takisto dodržiavať práva ustanovené v tomto dohovore bez ohľadu na to, či sú ich občanmi, alebo občanmi iných štátov;

Exteritorialita

AC. keďže uplatňovanie zákonov, nariadení a iných legislatívnych alebo vykonávacích nástrojov tretej krajiny mimo ich území v situáciách, ktoré patria do jurisdikcie EÚ alebo jej členských štátov, môže ovplyvniť zavedený právny poriadok a zásady právneho štátu alebo dokonca aj porušiť medzinárodné právo alebo právo EÚ vrátane práv fyzických a právnických osôb, pričom sa musí zohľadniť rozsah a deklarovaný alebo skutočný zámer tohto uplatňovania; keďže za takýchto okolností je potrebné prijať opatrenia na úrovni Únie na zabezpečenie toho, aby sa v EÚ dodržiavali hodnoty EÚ zakotvené v článku 2 ZEÚ, v Charte základných práv, v EDĽP, ktoré sa týkajú základných práv, demokracie, právneho štátu a práv fyzických a právnických osôb, ako sú zakotvené v sekundárnom práve uplatňujúcom tieto základné zásady, napr. odstránením, neutralizovaním, zablokovaním účinkov príslušných zahraničných právnych predpisov alebo iným spôsobom na bránenie sa týmto účinkom;

Medzinárodné prenosy údajov

AD. keďže prenos osobných údajov inštitúciami, orgánmi, úradmi a agentúrami EÚ alebo členskými štátmi Spojeným štátom americkým na účely presadzovania práva, keď neexistujú primerané záruky a ochrany, pokiaľ ide o dodržiavanie základných práv občanov EÚ, najmä práv na súkromie a ochranu osobných údajov, znamená, že táto inštitúcia, orgán, úrad a agentúra EÚ alebo tento členský štát sú na základe článku 340 ZFEÚ alebo na základe zavedenej judikatúry Súdneho dvora EÚ ([1]) zodpovedné za porušenie práva EÚ – čo zahŕňa akékoľvek porušenie základných práv ustanovených v Charte EÚ;

AE. keďže prenos údajov nie je zo zemepisného hľadiska a najmä z hľadiska rastúcej globalizácie a celosvetovej komunikácie obmedzený, zákonodarcovia v EÚ musia čeliť novým výzvam, pokiaľ ide o ochranu osobných údajov a komunikácie; keďže je preto nevyhnutné posilniť právne rámce v oblasti spoločných noriem;

AF. keďže hromadné zhromažďovanie osobných údajov na komerčné účely a v boji proti terorizmu a závažnej nadnárodnej trestnej činnosti predstavuje riziko pre ochranu osobných údajov a právo na súkromie občanov EÚ;

Prenosy do Spojených štátov na základe zásady bezpečného prístavu Spojených štátov

AG. keďže právny rámec Spojených štátov na ochranu údajov nezabezpečuje pre občanov EÚ dostatočnú úroveň ochrany;

AH. keďže na to, aby mohli prevádzkovatelia EÚ prenášať osobné údaje subjektu v Spojených štátoch, Komisia vo svojom rozhodnutí 2000/520/ES vyhlásila primeranosť ochrany poskytovanej zásadami bezpečného prístavu a súvisiacimi často kladenými otázkami vydanými Ministerstvom obchodu Spojených štátov pre osobné údaje prenášané z Únie organizáciám so sídlom v Spojených štátoch, ktoré pristúpili k dohode o bezpečnom prístave;

([1]) Pozri najmä spojené veci C-6/90 a C-9/90, Francovich a iní proti Taliansku, rozsudok z 19. novembra 1991.

Streda 12. marca 2014

AI. keďže Európsky parlament vo svojom uznesení z 5. júla 2000 vyjadril pochybnosti a obavy, pokiaľ ide o primeranosť bezpečného prístavu a vyzval Komisiu, aby včas preskúmala rozhodnutie s ohľadom na skúsenosti a prípadný legislatívny vývoj;

AJ. keďže spravodajcovia v pracovnom dokumente Európskeho parlamentu č. 4 z 12. decembra 2013 o činnostiach sledovania Spojených štátov, pokiaľ ide o údaje EÚ a ich možné právne dôsledky pre transatlantické dohody a spoluprácu, vyjadrili pochybnosti a obavy súvisiace s primeranosťou systému bezpečného prístavu a vyzvali Komisiu, aby zrušila rozhodnutie o primeranosti bezpečného prístavu a našla nové právne riešenia;

AK. keďže v rozhodnutí Komisie 2000/520/ES sa ustanovuje, že príslušné orgány v členských štátoch môžu vykonávať svoje existujúce právomoci a pozastaviť dátové toky organizácii, ktorá má vlastné osvedčenie o dodržiavaní zásad bezpečného prístavu, s cieľom chrániť jednotlivcov, pokiaľ ide o spracovanie osobných údajov v prípadoch, keď je veľmi pravdepodobné, že zásady bezpečného prístavu sa porušujú alebo že by pokračujúci prenos mohol vytvoriť bezprostredné riziko vážneho poškodenia dotknutých osôb;

AL. keďže v rozhodnutí Komisie 2000/520/ES sa tiež uvádza, že v prípade predloženia dôkazov, že akýkoľvek subjekt zodpovedný za zabezpečenie dodržiavania zásad v skutočnosti neplní svoju úlohu, musí Komisia informovať Ministerstvo hospodárstva Spojených štátov, a ak to je potrebné, predložiť opatrenia na odvolanie alebo pozastavenie uvedeného rozhodnutia alebo na obmedzenie rozsahu jeho účinnosti;

AM. keďže Komisia vo svojich prvých dvoch správach o vykonávaní bezpečného prístavu z roku 2002 a z roku 2004 zistila viacero nedostatkov, pokiaľ ide o riadne vykonávanie bezpečného prístavu, a vydala niekoľko odporúčaní pre orgány Spojených štátov s cieľom ich nápravy;

AN. keďže Komisia vo svojej tretej správe o vykonávaní z 27. novembra 2013, čo je deväť rokov po druhej správe, a bez toho, že by boli napravené akékoľvek nedostatky zistené v tejto správe, zistila ďalšie rozsiahle slabé stránky a nedostatky v bezpečnom prístave a dospela k záveru, že nie je možné pokračovať v súčasnom vykonávaní; keďže Komisia zdôrazňuje, že rozsiahly prístup spravodajských agentúr Spojených štátov k údajom prenášaným do Spojených štátov subjektmi s osvedčením bezpečného prístavu vzbudzuje ďalšie vážne otázky, pokiaľ ide o kontinuitu ochrany údajov dotknutých osôb EÚ; keďže Komisia adresovala orgánom Spojených štátov 13 odporúčaní a zaviazala sa spoločne s orgánmi Spojených štátov do leta roku 2014 stanoviť nápravné opatrenia, ktoré treba čo možno najskôr uplatniť, čo tvorí základ na úplné preskúmanie fungovania zásad bezpečného prístavu;

AO. keďže delegácia Výboru Európskeho parlamentu pre občianske slobody, spravodlivosť a vnútorné veci (výbor LIBE) sa vo Washingtone D. C. od 28. do 31. októbra 2013 stretla s Ministerstvom obchodu Spojených štátov a s Federálnou obchodnou komisiou Spojených štátov; keďže ministerstvo obchodu uznalo existenciu organizácií, ktoré majú vlastné osvedčenia o dodržiavaní zásad bezpečného prístavu, ktoré však jasne vykazujú „neaktuálny stav“, čo znamená, že spoločnosť nespĺňa požiadavky bezpečného prístavu, hoci naďalej prijíma osobné údaje z EÚ; keďže Federálna obchodná komisia pripustila, že bezpečný prístav by sa mal preskúmať s cieľom jeho zlepšenia, najmä pokiaľ ide o systém podávania sťažností a systém alternatívneho urovnávania sporov;

AP. keďže zásady bezpečného prístavu môžu byť obmedzené „v rozsahu potrebnom na splnenie požiadaviek národnej bezpečnosti, verejného záujmu alebo požiadaviek presadzovania práva“; keďže to predstavuje výnimku zo základného práva, takáto výnimka sa musí vždy interpretovať reštriktívne a musí byť obmedzená na to, čo je potrebné a primerané v demokratickej spoločnosti, a v zákone musia byť jasne ustanovené podmienky a záruky na to, aby bolo toto obmedzenie opodstatnené; keďže rozsah uplatnenia tejto výnimky by mali objasniť Spojené štáty a EÚ, a to najmä Komisia, aby sa zabránilo akejkoľvek interpretácii alebo vykonávaniu, ktoré v podstate ruší okrem iných práv aj základné právo na súkromie a ochranu osobných údajov; keďže takáto výnimka by sa preto nemala používať tak, aby sa narušila alebo zrušila ochrana, ktorú poskytujú Charta základných práv, EDĽP, právne predpisy EÚ o ochrane údajov a zásady bezpečného prístavu; trvá na tom, že ak sa v prípade národnej bezpečnosti uplatní výnimka, musí sa špecifikovať vnútroštátne právo, na základe ktorého sa táto výnimka uplatní;

AQ. keďže rozsiahly prístup spravodajských agentúr Spojených štátov vážne narušil transatlantickú dôveru a negatívne ovplyvnil dôveru v organizácie Spojených štátov, ktoré pôsobia v EÚ; keďže sa to ešte prehĺbilo nedostatkom súdnych a správnych opravných prostriedkov pre občanov EÚ v rámci právnych predpisov Spojených štátov, najmä v prípadoch sledovania na spravodajské účely;

Prenosy tretím krajinám s rozhodnutím o primeranosti

AR. keďže podľa zverejnených informácií a zistení vyšetrovania, ktoré vykonal výbor LIBE, národné bezpečnostné agentúry Nového Zélandu, Kanady a Austrálie sa zúčastňovali na rozsiahlom hromadnom sledovaní elektronickej komunikácie a aktívne spolupracovali so Spojenými štátmi v rámci takzvaného programu päť očí (Five eyes) a mohli si vzájomne vymieňať osobné údaje občanov EÚ prenesené z EÚ;

AS. keďže v rozhodnutiach Komisie 2013/65/EÚ ([1]) a 2002/2/ES ([2]) bola úroveň ochrany, ktorú zabezpečuje Nový Zéland zákonom o súkromí a kanadský zákon o ochrane osobných údajov a elektronických dokumentov, vyhlásená za primeranú; keďže uvedené odhalenia tiež vážne ovplyvňujú dôveru v právne systémy týchto krajín, pokiaľ ide o kontinuitu ochrany poskytovanú občanom EÚ; keďže Komisia nepreskúmala tento aspekt;

Prenosy na základe zmluvných doložiek a iných nástrojov

AT. keďže v smernici 95/46/ES sa stanovuje, že medzinárodné prenosy do tretej krajiny môžu prebiehať aj prostredníctvom osobitných nástrojov, ak prevádzkovateľ uvedie primerané záruky na ochranu súkromia a základných práv a slobôd jednotlivcov a na uplatňovanie príslušných práv;

AU. keďže takéto záruky môžu vyplývať najmä z príslušných zmluvných doložiek;

AV. keďže smernica 95/46/ES splnomocňuje Komisiu, aby rozhodla, či osobitné štandardné zmluvné doložky poskytujú dostatočné záruky podľa požiadaviek smernice, a keďže na tomto základe Komisia prijala tri modely štandardných zmluvných doložiek pre transfery prevádzkovateľom a spracovateľom (a čiastkovým spracovateľom) v tretích krajinách;

AW. keďže podľa rozhodnutí Komisie, ktorými sa ustanovujú štandardné zmluvné doložky, môžu príslušné orgány v členských štátoch uplatniť svoje súčasné právomoci na pozastavenie tokov údajov, ak sa zistí, že právne predpisy vzťahujúce sa na dovozcu alebo čiastkového spracovateľa mu ukladajú povinnosť odchýliť sa od platných právnych predpisov v oblasti ochrany údajov, ktoré presahujú rámec obmedzení nevyhnutných v demokratickej spoločnosti, ako je stanovené v článku 13 smernice 95/46/ES, v prípade, že tieto požiadavky by mohli mať podstatný nepriaznivý vplyv na záruky poskytované platnými právnymi predpismi v oblasti ochrany údajov a štandardnými zmluvnými doložkami, alebo v prípadoch, v ktorých je vysoko pravdepodobné, že štandardné zmluvné doložky uvedené v prílohe sa nedodržiavajú alebo sa nebudú dodržiavať a pokračovanie v prenose by predstavovalo bezprostredné riziko vážneho poškodenia dotknutých osôb;

AX. keďže vnútroštátne orgány na ochranu údajov vypracovali záväzné firemné pravidlá, aby zjednodušili medzinárodné prenosy v rámci nadnárodnej spoločnosti s primeranými zárukami s ohľadom na ochranu súkromia a základných práv a slobôd jednotlivcov, a pokiaľ ide o uplatnenie príslušných práv; keďže záväzné firemné pravidlá musia pred ich uplatňovaním schváliť príslušné orgány členských štátov po tom, ako posúdili ich súlad s právnymi predpismi Únie v oblasti ochrany údajov; keďže v správe výboru LIBE o všeobecnom nariadení o ochrane údajov sa záväzné firemné pravidlá pre spracovateľov údajov zamietli, pretože by ponechali prevádzkovateľa údajov a dotknutú osobu bez kontroly jurisdikciou, v rámci ktorej sa údaje spracúvajú;

([1]) Ú. v. EÚ L 28, 30.1.2013, s. 12.
([2]) Ú. v. ES L 2, 4.1.2002, s. 13.

Streda 12. marca 2014

AY. keďže vzhľadom na svoju právomoc ustanovenú článkom 218 ZFEÚ je Európsky parlament zodpovedný za nepretržité monitorovanie hodnoty medzinárodných dohôd, ktorým udelil svoj súhlas;

Prenosy na základe dohody o TFTP a dohody o PNR

AZ. keďže Európsky parlament vo svojom uznesení z 23. októbra 2013 vyjadril vážne obavy v súvislosti s odhaleniami týkajúcimi sa činností NSA, pokiaľ ide o priamy prístup k správam o finančných platbách a súvisiacim údajom, ktoré by predstavovali jednoznačné porušenie dohody o TFTP, najmä jej článku 1;

BA. keďže sledovanie financovania terorizmu je základným prostriedkom v boji proti financovaniu terorizmu a závažnej trestnej činnosti, pričom umožňuje vyšetrovateľom v boji proti terorizmu nájsť prepojenia medzi cieľmi vyšetrovania a inými osobami, ktoré sú v spojení so širšími sieťami teroristov a sú podozrivé z ich financovania;

BB. keďže Európsky parlament požiadal Komisiu, aby pozastavila platnosť dohody a aby mu boli okamžite sprístupnené všetky príslušné informácie a dokumenty na účely ich prediskutovania v Parlamente; keďže Komisia na to nereagovala;

BC. keďže na základe obvinení uverejnených v médiách Komisia rozhodla o začatí konzultácií so Spojenými štátmi v súlade s článkom 19 dohody o TFTP; keďže 27. novembra 2013 komisárka Malmströmová informovala výbor LIBE, že po stretnutí s orgánmi Spojených štátov a vzhľadom na ich odpovede v listoch a počas stretnutí sa Komisia rozhodla nepokračovať v konzultáciách, keďže nebol dôvod domnievať sa, že vláda Spojených štátov konala v rozpore s ustanoveniami dohody, a keďže Spojené štáty poskytli písomné ubezpečenie, že nedošlo k žiadnemu priamemu zberu údajov, ktorý by bol v rozpore s ustanoveniami dohody o TFTP; keďže nie je jasné, či orgány Spojených štátov obišli dohodu tým, že získali prístup k takýmto údajom pomocou iných prostriedkov, ako naznačuje list orgánov Spojených štátov z 18. septembra 2013 ([1]);

BD. keďže počas návštevy delegácie výboru LIBE vo Washingtone 28. – 31. októbra 2013 sa delegácia stretla s Ministerstvom financií Spojených štátov; keďže Ministerstvo financií Spojených štátov uviedlo, že odkedy dohoda o TFTP nadobudla platnosť, nemalo prístup k údajom zo systému SWIFT v EÚ, iba v rámci TFTP; keďže Ministerstvo financií Spojených štátov sa odmietlo vyjadriť k otázke, či k údajom zo systému SWIFT mal mimo TFTP prístup akýkoľvek iný vládny orgán alebo ministerstvo Spojených štátov alebo či si administratíva Spojených štátov bola vedomá činností hromadného sledovania agentúry NSA; keďže 18. decembra 2013 pán Glenn Greenwald pred vyšetrovacím výborom LIBE uviedol, že NSA a GCHQ sa zamerali na siete SWIFT;

BE. keďže belgické a holandské orgány na ochranu údajov sa 13. novembra 2013 rozhodli, že povedú spoločné vyšetrovanie bezpečnosti platobných sietí SWIFT, aby sa uistili, či tretie strany mohli získať neoprávnený alebo nezákonný prístup k bankovým údajom európskych občanov ([2]);

BF. keďže podľa spoločného preskúmania dohody o PNR medzi EÚ a Spojenými štátmi Ministerstvo vnútornej bezpečnosti Spojených štátov 23-krát poskytlo údaje PNR jednotlivých prípadov agentúre NSA na podporu prípadov boja proti terorizmu v súlade s osobitnými podmienkami dohody;

BG. keďže v spoločnom preskúmaní sa neuvádza skutočnosť, že v prípade spracovania osobných údajov na spravodajské účely podľa práva USA nemajú osoby, ktoré nie sú americkými občanmi, súdny ani správny prostriedok na ochranu svojich práv a ústavná ochrana sa poskytuje iba občanom Spojených štátov; keďže táto neexistencia súdnych alebo správnych práv ruší ochranu pre občanov EÚ ustanovenú v súčasnej dohode o PNR;

([1]) V liste sa uvádza, že „vláda Spojených štátov vyhľadáva a získava informácie o financiách … ‚[ktoré] sa zhromažďujú prostredníctvom regulačných, diplomatických a spravodajských kanálov a presadzovaním práva, ako aj výmenou so zahraničnými partnermi“, a že „vláda Spojených štátov využíva TFTP, aby získala údaje zo systému SWIFT, ktoré nezískava z iných zdrojov“.

([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.

Streda 12. marca 2014

Prenosy na základe Dohody medzi EÚ a Spojenými štátmi americkými o vzájomnej právnej pomoci v trestných veciach

BH. keďže Dohoda medzi Európskou úniou a Spojenými štátmi americkými o vzájomnej právnej pomoci v trestných veciach zo 6. júna 2003 ([1]) nadobudla platnosť 1. februára 2010 a jej cieľom bolo uľahčiť spoluprácu medzi EÚ a Spojenými štátmi v účinnejšom boji proti zločinu pri náležitom rešpektovaní práv jednotlivcov a zásad právneho štátu;

Rámcová dohoda o ochrane údajov v oblasti policajnej a justičnej spolupráce („zastrešujúca dohoda")

BI. keďže účelom tejto všeobecnej dohody je ustanoviť právny rámec pre všetky prenosy osobných údajov medzi EÚ a Spojenými štátmi výhradne na účely predchádzania trestným činom vrátane terorizmu a ich vyšetrovania, odhaľovania alebo stíhania v rámci policajnej a justičnej spolupráce v trestných veciach; keďže Rada 2. decembra 2010 schválila rokovania; keďže táto dohoda je mimoriadne dôležitá a predstavovala by základ na zjednodušenie prenosu dát v súvislosti s policajnou a justičnou spoluprácou v trestných veciach;

BJ. keďže touto dohodou by sa mali stanoviť jednoznačné a presné právne záväzné zásady spracovania údajov a malo by sa predovšetkým uznať právo občanov EÚ na justičný prístup, opravu a vymazanie ich osobných údajov v Spojených štátoch, ako aj právo na efektívny správny a justičný mechanizmus nápravy pre občanov EÚ v Spojených štátoch a nezávislý dohľad nad činnosťami týkajúcimi sa spracovania údajov;

BK. keďže Komisia vo svojom oznámení z 27. novembra 2013 naznačila, že „zastrešujúca dohoda" by mala priniesť vysokú úroveň ochrany pre občanov na oboch stranách Atlantického oceánu a mala by posilniť dôveru Európanov vo výmeny údajov medzi EÚ a Spojenými štátmi, čím by poskytla základ na ďalší rozvoj spolupráce v oblasti bezpečnosti a partnerstva medzi EÚ a Spojenými štátmi;

BL. keďže rokovania o dohode nepokročili vzhľadom na pretrvávajúcu odmietavú pozíciu vlády Spojených štátov, pokiaľ ide o uznanie efektívnych práv na správnu a justičnú nápravu občanom EÚ, a vzhľadom na zámer poskytnúť rozsiahle odchýlky od zásad ochrany údajov uvedených v dohode, ako je napríklad obmedzenie účelu, uchovávanie údajov alebo budúce prenosy doma alebo v zahraničí;

Reforma ochrany údajov

BM. keďže právny rámec ochrany údajov EÚ je v súčasnosti predmetom skúmania s cieľom vytvoriť komplexný, konzistentný, moderný a robustný systém pre všetky činnosti týkajúce sa spracovania údajov v Únii; keďže v januári 2012 Komisia predložila balík legislatívnych návrhov: všeobecné nariadenie o ochrane údajov ([2]), ktoré nahradí smernicu 95/46/ES a ktorým sa ustanovia jednotné právne predpisy v rámci celej EÚ, a smernicu ([3]), ktorou sa ustanoví harmonizovaný rámec pre všetky činnosti spojené so spracovaním údajov orgánmi presadzovania práva na účely presadzovania práva a ktorou sa zmenšia súčasné rozdiely medzi vnútroštátnymi právnymi predpismi;

BN. keďže 21. októbra 2013 výbor LIBE prijal legislatívne správy o týchto dvoch návrhoch a rozhodnutie o otvorení rokovaní s Radou s cieľom prijať právne nástroje v priebehu tohto legislatívneho obdobia;

BO. keďže napriek tomu, že Európska rada 24.–25. októbra 2013 vyzvala k včasnému prijatiu silného všeobecného rámca EÚ v oblasti ochrany údajov s cieľom zvýšiť dôveru občanov a podnikov v digitálnu ekonomiku, Rada po dvoch rokoch diskusií nebola stále schopná dohodnúť sa na všeobecnom prístupe k všeobecnému nariadeniu o ochrane údajov a k smernici ([4]);

([1]) Ú. v. EÚ L 181, 19.7.2003, s. 25.
([2]) COM(2012)0011 final, 25.1.2012.
([3]) COM(2012)0010 final, 25.1.2012.
([4]) http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf.

Streda 12. marca 2014

Bezpečnosť IT a cloud computing

BP. keďže v uvedenom uznesení Európskeho parlamentu z 10. decembra 2013 sa zdôrazňuje ekonomický potenciál „cloud computingu“ pre rast a zamestnanosť; keďže sa odhaduje, že celková hospodárska hodnota trhu s cloud computingom EÚ dosiahne do roku 2016 hodnotu 207 miliárd USD ročne, čo je dvojnásobok hodnoty v roku 2012;

BQ. keďže úroveň ochrany údajov v prostredí cloud computingu nesmie byť nižšia ako úroveň ochrany požadovaná v akomkoľvek inom kontexte spracovania údajov; keďže právne predpisy Únie v oblasti ochrany údajov vzhľadom na skutočnosť, že sú technologicky neutrálne, sa už v plnom rozsahu vzťahujú na služby cloud computingu, ktoré v EÚ fungujú;

BR. keďže činnosti hromadného sledovania poskytujú spravodajským agentúram prístup k osobným údajom, ktoré uchovávajú alebo inak spracúvajú jednotlivci v EÚ v rámci dohôd o službách cloudu s najväčšími americkými poskytovateľmi cloudu; keďže spravodajské orgány Spojených štátov získali prístup k osobným údajom uloženým na serveroch nachádzajúcich sa na pôde EÚ pripojením sa na vnútorné siete Yahoo a Google; keďže takéto činnosti znamenajú porušenie medzinárodných záväzkov a európskych noriem v oblasti základných práv vrátane práva na súkromný a rodinný život, dôvernosti komunikácie, prezumpcie neviny, slobody prejavu, slobody informácií, slobody zhromažďovania a združovania a slobody podnikania; keďže nie je vylúčené, že spravodajské orgány získali prístup aj k informáciám, ktoré v službách cloudu uložili verejné orgány členských štátov alebo podniky a inštitúcie;

BS. keďže spravodajské agentúry Spojených štátov uplatňujú politiku systematického narúšania šifrovacích protokolov a produktov s cieľom odpočúvať aj šifrovanú komunikáciu; keďže Národná bezpečnostná agentúra Spojených štátov zhromaždila obrovské množstvo takzvaných zneužití nultého dňa (zero-day exploit) – zraniteľných miest týkajúcich sa bezpečnosti informačných technológií, ktoré ešte verejnosť ani dodávatelia produktov nepoznajú; keďže tieto činnosti v hromadnej miere narúšajú celkové snahy na zlepšenie bezpečnosti informačných technológií;

BT. keďže skutočnosť, že spravodajské agentúry mali prístup k osobným údajom používateľov online služieb, vážne narušila dôveru občanov v tieto služby a z tohto dôvodu má negatívny vplyv na obchodné investície do rozvoja nových služieb využívajúcich veľké objemy údajov a nových aplikácií, ako napríklad internet vecí;

BU. keďže dodávatelia informačných technológií často dodávajú produkty, ktoré sa nepodrobili riadnej skúške bezpečnosti alebo ktorým dokonca účelne nainštalujú backdoor; keďže nedostatok pravidiel v oblasti zodpovednosti pre dodávateľov softvéru vedie k situácii, ktorú ihneď využijú spravodajské agentúry, ale súčasne vzniká aj riziko útokov zo strany iných subjektov;

BV. keďže je nevyhnutné, aby spoločnosti poskytujúce takéto nové služby a aplikácie dodržiavali pravidlá v oblasti ochrany údajov a súkromia dotknutých osôb, ktorých údaje sú zhromažďované, spracúvané a analyzované, a to s cieľom zachovať vysokú úroveň dôvery občanov;

Demokratický dohľad nad spravodajskými službami

BW. keďže spravodajské služby v demokratických spoločnostiach majú osobitné právomoci a spôsobilosť na ochranu základných práv, demokracie a zásad právneho štátu, práv občanov a štátu na ochranu pred závažnými vnútornými a vonkajšími hrozbami, pričom musia podliehať demokratickej zodpovednosti a súdnemu dohľadu; keďže výlučne na tento účel disponujú osobitnými právomocami a schopnosťami; keďže tieto právomoci by sa mali používať v rámci právnych obmedzení vyplývajúcich zo základných práv, demokracie a zásad právneho štátu a ich uplatňovanie by malo byť pod prísnym dohľadom, v opačnom prípade prídu o legitimitu a vzniká hrozba, že oslabia demokraciu;

BX. keďže spravodajským službám je priznaná určitá úroveň utajenia, aby sa zabránilo ohrozeniu prebiehajúcich operácií, odhaleniu spôsobu práce alebo ohrozeniu životov agentov, a toto utajenie nemôže obchádzať ani vylúčiť pravidlá demokratickej a súdnej kontroly a vyšetrovania ich činnosti a takisto ani pravidlá transparentnosti, a to najmä vzhľadom na základné práva a zásady právneho štátu, pretože všetky sú základným kameňom demokratickej spoločnosti;

BY. keďže väčšina súčasných vnútroštátnych mechanizmov a orgánov dohľadu bola zriadená alebo prepracovaná v 90. rokoch minulého storočia a nebola nevyhnutne prispôsobená rýchlemu politickému a technologickému vývoju v poslednom desaťročí čo viedlo k vyššej medzinárodnej spolupráci, ktorá zahŕňa aj výmenu osobných údajov, a často k prelínaniu hraníc činností v oblasti spravodajských služieb a v oblasti presadzovania práva;

BZ. keďže demokratický dohľad nad spravodajskými činnosťami sa stále vykonáva len na vnútroštátnej úrovni, a to napriek zvýšenej výmene informácií medzi členskými štátmi EÚ navzájom a medzi členskými štátmi a tretími krajinami; keďže medzi úrovňou medzinárodnej spolupráce na jednej strane a možnosťami dohľadu obmedzenými na vnútroštátnu úroveň na druhej strane je čoraz väčšia priepasť, čo má za následok nedostatočnú a neúčinnú demokratickú kontrolu;

CA. keďže vnútroštátne orgány dohľadu nemajú často úplný prístup k spravodajským informáciám zo zahraničných spravodajských agentúr, čo môže viesť k situáciám, keď sa medzinárodná výmena informácií uskutoční bez ich primeraného preverenia; keďže tento problém ešte zhoršuje takzvané pravidlo tretej strany alebo zásada „kontroly pôvodcu“, ktorá má umožniť pôvodcovi udržiavať kontrolu nad ďalším šírením citlivých informácií, ale často sa, žiaľ, interpretuje aj ako zásada uplatňovaná pri dohľade útvarov príjemcu;

CB. keďže iniciatívy týkajúce sa reformy transparentnosti v súkromnej a verejnej oblasti sú nevyhnutné na zabezpečenie dôvery verejnosti v činnosť spravodajských agentúr; keďže právne systémy by nemali brániť spoločnostiam zverejňovať informácie o tom, ako postupujú pri žiadostiach vlády a súdnych príkazoch na prístup k údajom o používateľoch, a mali by im umožniť zverejňovať súhrnné informácie o počte schválených a zamietnutých žiadostí a príkazov;

Hlavné zistenia

1. domnieva sa, že najnovšie zistenia v tlači podľa informátorov a novinárov spolu so znaleckým posudkom poskytnutým v rámci tohto vyšetrovania priniesli na základe priznaní orgánov a nepostačujúcej odpovede na tieto tvrdenia presvedčivé dôkazy o existencii rozsiahlych, komplexných a vysoko technologicky vyspelých systémov navrhnutých spravodajskými službami Spojených štátov a niektorých členských štátov na zber, ukladanie a analýzu komunikačných údajov vrátane údajov o obsahu, lokalizačných údajov a metaúdajov všetkých občanov na svete v nevídanom rozsahu, a to bez rozlišovania a spôsobom, ktorý nie je založený na podozreniach;

2. poukazuje konkrétne na spravodajské programy agentúry Spojených štátov NSA, ktoré umožňujú hromadné sledovanie občanov EÚ prostredníctvom priameho prístupu k ústredným serverom vedúcich amerických internetových spoločností (program PRISM), analýzy obsahu a metaúdajov (program Xkeyscore), obchádzania online šifrovania (BULLRUN), prístupu k počítačovým a telefonickým sieťam a prístupu k lokalizačným údajom, ako aj na systémy spravodajskej agentúry Spojeného kráľovstva GCHQ, ako je sledovanie odoslanej komunikácie (program Tempora) a program na dešifrovanie (Edgehill), cielené útoky na informačné systémy typu man-in-the-middle (programy Quantumtheory a Foxacid), zber a uchovávanie 200 miliónov textových správ SMS za deň (program Dishfire);

3. berie na vedomie obvinenia z „hackerstva“ alebo odpočúvania systémov Belgacom spravodajskou agentúrou Spojeného kráľovstva GCHQ; berie na vedomie tvrdenie spoločnosti Belgacom, a to, že nemôže potvrdiť ani poprieť, či sledovanie bolo zamerané na inštitúcie EÚ alebo sa ich dotklo, a že použitý malvér bol mimoriadne zložitý a jeho používanie a vývoj si vyžadujú rozsiahle finančné a personálne prostriedky, ktorými súkromné subjekty ani hackeri nedisponujú;

4. zdôrazňuje, že tieto skutočnosti prudko otriasli dôverou: dôverou medzi dvomi transatlantickými partnermi, dôverou medzi občanmi a ich vládami, dôverou vo fungovanie demokratických inštitúcií na obidvoch stranách Atlantického oceánu, dôverou v dodržiavanie zásad právneho štátu a dôverou v bezpečnosť služieb IT; je presvedčený, že v záujme obnovenia dôvery na všetkých týchto úrovniach je potrebný bezodkladný a komplexný plán reakcie obsahujúci rad opatrení, ktorý bude pod dohľadom verejnosti;

5. konštatuje, že viaceré vlády vyhlasujú, že tieto programy hromadného sledovania sú potrebné v boji proti terorizmu; dôrazne odsudzuje terorizmus, ale je pevne presvedčený, že boj proti terorizmu nikdy nemôže slúžiť ako odôvodnenie necielených, tajných a niekedy dokonca nezákonných programov hromadného sledovania; zastáva názor, že takéto programy nie sú v súlade so zásadami nevyhnutnosti a primeranosti v demokratickej spoločnosti;

Streda 12. marca 2014

6. pripomína pevné presvedčenie EÚ, že je potrebné vytvoriť rovnováhu medzi bezpečnostnými opatreniami a ochranou občianskych slobôd a základných práv pri zaručení maximálneho dodržiavania ochrany súkromia a osobných údajov;

7. domnieva sa, že jediným dôvodom na zber údajov v takom rozsahu nie je len boj proti terorizmu, keďže ide o zber všetkých možných údajov o všetkých občanoch; upozorňuje preto na možnú existenciu iných účelov vrátane politickej a hospodárskej špionáže, pričom tieto pochybnosti treba rozptýliť;

8. spochybňuje zlučiteľnosť činností hospodárskej špionáže niektorých členských štátov s vnútorným trhom EÚ a s právnymi predpismi o hospodárskej súťaži, ktoré sú zakotvené v hlave I a hlave VII Zmluvy o fungovaní Európskej únie; potvrdzuje zásadu lojálnej spolupráce zakotvenú v článku 4 ods. 3 Zmluvy o Európskej únii a zásadu, že členské štáty „neprijmú žiadne opatrenie, ktoré by mohlo ohroziť dosiahnutie cieľov Únie“;

9. konštatuje, že medzinárodné zmluvy a právne predpisy EÚ a Spojených štátov ani vnútroštátne mechanizmy dohľadu neboli schopné zabezpečiť potrebné kontroly a vyváženosť ani demokratickú zodpovednosť;

10. odsudzuje rozsiahly, systematický, plošný zber osobných údajov nevinných osôb, ktoré často obsahujú intímne osobné informácie; zdôrazňuje, že systémy hromadného, nerozlíšeného sledovania spravodajskými agentúrami predstavujú vážne porušenie základných práv občanov; zdôrazňuje, že právo na súkromie nie je luxusom, ale základným kameňom slobodnej a demokratickej spoločnosti; ďalej poukazuje na skutočnosť, že hromadné sledovanie môže mať potenciálne závažný vplyv na slobodu tlače, myslenia a prejavu a na slobodu zhromažďovania a združovania, a zároveň predstavuje významný potenciál na zneužitie zhromaždených informácií proti politickým oponentom; zdôrazňuje, že tieto činnosti hromadného sledovania zahŕňajú aj nezákonné činnosti spravodajských služieb a vyvolávajú otázky v súvislosti s exteritorialitou vnútroštátnych právnych predpisov;

11. domnieva sa, že je zásadné chrániť právo na dôvernosť informácií v prípade právnikov, novinárov, lekárov a iných regulovaných povolaní pred činnosťami hromadného sledovania; zdôrazňuje najmä, že akákoľvek neistota, pokiaľ ide o dôvernosť komunikácie medzi právnikmi a ich klientmi by mohla mať negatívny vplyv na právo občanov EÚ na prístup k právnemu poradenstvu a k spravodlivosti a na právo na spravodlivý súdny proces;

12. považuje programy sledovania za ďalší krok smerom k vytvoreniu plne rozvinutého preventívneho stavu, ktorý zmení zavedenú paradigmu trestného práva v demokratických spoločnostiach, kde oprávnenie na akékoľvek zasahovanie do základných práv podozrivých osôb musí udeliť sudca alebo prokurátor na základe odôvodneného podozrenia a musí byť upravované právom, namiesto nej podporí kombináciu presadzovania práva a spravodajských činností s neistými a oslabenými právnymi zárukami, často nie v súlade s demokratickými kontrolami, vyváženosťou a základnými právami, najmä s prezumpciou neviny; v tejto súvislosti pripomína rozhodnutie nemeckého Spolkového ústavného súdu ([1]) o zákaze používania preventívnych záťahov („präventive Rasterfahndung“), pokiaľ nie sú k dispozícii dôkazy o konkrétnom ohrození iných zákonom chránených práv s vysokou prioritou, pričom stav všeobecného ohrozenia alebo medzinárodné napätie nie sú dostatočným odôvodnením takýchto opatrení;

13. trvá na tom, že tajné predpisy a súdy predstavujú porušenie zásad právneho štátu; trvá na tom, že akýkoľvek rozsudok súdu alebo tribunálu a akékoľvek rozhodnutie správneho orgánu nečlenského štátu EÚ, ktorým sa priamo alebo nepriamo povoľuje prenos osobných údajov, nesmie byť žiadnym spôsobom uznané alebo vykonané bez platnej zmluvy o vzájomnej právnej pomoci alebo medzinárodnej zmluvy medzi žiadajúcou treťou krajinou a Úniou alebo členským štátom a tiež predchádzajúceho povolenia príslušného orgánu dozoru; zdôrazňuje, že akýkoľvek rozsudok tajného súdu alebo tribunálu a akékoľvek rozhodnutie správneho orgánu nečlenského štátu, ktorým sa tajne, priamo alebo nepriamo, povoľujú činnosti sledovania, nebudú uznané alebo vykonané;

([1]) Č. 1 BvR 518/02 zo 4. apríla 2006.

14. domnieva sa, že uvedené obavy sa zvyšujú v dôsledku rýchleho technologického a spoločenského rozvoja, pretože internet a mobilné zariadenia sa v modernom každodennom živote vyskytujú všade („všadeprítomná výpočtová technika“) a obchodný model väčšiny internetových spoločností je založený na spracovaní osobných údajov; domnieva sa, že rozsah tohto problému je bezprecedentný; domnieva sa, že to môže vyvolať situáciu, keď infraštruktúra pre hromadné zbieranie spracovanie údajov by mohla byť zneužitá v prípade zmeny politického režimu;

15. poznamenáva, že neexistuje žiadna záruka, či už pre verejné inštitúcie EÚ, alebo pre občanov, že bezpečnosť IT alebo súkromie možno chrániť pred vniknutím dobre vybavených narušiteľov („žiadna 100 % bezpečnosť IT“); konštatuje, že na dosiahnutie maximálnej bezpečnosti IT musia byť Európania ochotní venovať dostatočné prostriedky, a to personálne, ako aj finančné, aby sa zachovala európska nezávislosť a sebestačnosť v oblasti IT;

16. dôrazne odmieta názor, že všetky otázky týkajúce sa programov hromadného sledovania sú čisto záležitosťou národnej bezpečnosti, a teda vo výhradnej právomoci členských štátov; pripomína, že členské štáty musia pri zabezpečovaní svojej národnej bezpečnosti v plnej miere dodržiavať právo EÚ a EDĽP; pripomína nedávny rozsudok Súdneho dvora, podľa ktorého „hoci je vecou členských štátov, aby prijali opatrenia na zaistenie svojej vnútornej a vonkajšej bezpečnosti, samotná skutočnosť, že rozhodnutie sa týka bezpečnosti štátu, nemôže viesť k tomu, že sa neuplatní právo Únie“ ([1]); pripomína, že v stávke je ochrana súkromia všetkých občanov EÚ, takisto ako bezpečnosť a spoľahlivosť všetkých komunikačných sietí EÚ; domnieva sa preto, že diskusia a konanie na úrovni EÚ sú nielen oprávnené, ale zároveň ide o otázku autonómie EÚ;

17. oceňuje inštitúcie a odborníkov, ktorí prispeli k tomuto vyšetrovaniu; vyjadruje poľutovanie nad skutočnosťou, že orgány niektorých členských štátov odmietli spolupracovať na vyšetrovaní, ktoré Európsky parlament viedol v mene občanov; víta otvorenosť viacerých členov Kongresu a národných parlamentov;

18. je si vedomý, že v takomto obmedzenom časovom rámci bolo od júla 2013 možné viesť iba predbežné vyšetrovanie všetkých uvedených otázok; uznáva tak rozsah dotknutých odhalení, ako aj ich pretrvávajúci charakter; prijíma preto prístup plánovania vopred, ktorý pozostáva zo súboru konkrétnych návrhov a mechanizmu nadväzujúcich opatrení v ďalšom volebnom období, ktorým sa zabezpečí, že zistenia ostanú jednou z priorít politického programu EÚ;

19. má v úmysle žiadať pevné politické záväzky od novej Komisie, ktorá bude vymenovaná po voľbách v máji 2014, aby uplatnila návrhy a odporúčania tohto vyšetrovania;

Odporúčania

20. vyzýva orgány Spojených štátov a členských štátov EÚ, ktoré to ešte neurobili, aby zakázali činnosti súvisiace s plošným hromadným sledovaním;

21. vyzýva členské štáty EÚ, najmä tie, ktoré sa podieľajú na takzvaných programoch „9 očí“ a „14 očí“ ([2]), aby podľa potreby komplexne zhodnotili a zrevidovali svoje vnútroštátne právne predpisy a postupy, ktorými sa riadia činnosti spravodajských služieb, s cieľom zabezpečenia, aby boli pod dohľadom parlamentu a súdnictva a pod verejnou kontrolou, aby dodržiavali zásady zákonnosti, potrebnosti, proporcionality, riadneho spracovania, upozornenia používateľa, transparentnosti pomocou kompilácie správnej praxe OSN a odporúčaní Benátskej komisie, a aby boli v súlade s normami Európskeho dohovoru o ľudských právach a plnili si svoje záväzky v oblasti základných práv, najmä čo sa týka ochrany údajov, súkromia a prezumpcie neviny;

([1]) Rozsudok vo veci C-300/11, ZZ proti Secretary of State for the Home Department , 4. júna 2013.

([2]) Do programu „9 očí“ sú zapojené USA, Veľká Británia, Kanada, Austrália, Nový Zéland, Dánsko, Francúzsko, Nórsko a Holandsko; na programe „14 očí“ sa podieľajú uvedené krajiny, ako aj Nemecko, Belgicko, Taliansko, Španielsko a Švédsko.

Streda 12. marca 2014

22. vyzýva všetky členské krajiny a v súvislosti s uznesením zo 4. júla 2013 a informačnými vypočutiami predovšetkým Spojené kráľovstvo, Francúzsko, Nemecko, Švédsko, Holandsko a Poľsko, aby ich súčasné či budúce legislatívne rámce a kontrolné mechanizmy upravujúce činnosti spravodajských agentúr boli v súlade s normami Európskeho dohovoru o ľudských právach a právnymi predpismi Európskej únie na ochranu údajov; vyzýva tieto členské štáty, aby vysvetlili informácie o činnostiach hromadného sledovania vrátane hromadného sledovania cezhraničných telekomunikácií, necieleného sledovania káblových komunikácií, možných dohodách medzi spravodajskými službami a telekomunikačnými spoločnosťami, čo sa týka prístupu k osobným údajom a výmeny týchto údajov a prístupu k transatlantickým káblom, zamestnancov a zariadenia spravodajských služieb USA na území EÚ bez dohľadu nad monitorovacími operáciami, a ich zlučiteľnosti s právnymi predpismi EÚ; vyzýva národné parlamenty týchto krajín, aby zintenzívnili spoluprácu orgánov dohľadu nad spravodajskými službami na európskej úrovni;

23. vyzýva Spojené kráľovstvo, aby najmä vzhľadom na rozsiahle mediálne správy o hromadnom sledovaní spravodajskou službou GCHQ revidovala svoj súčasný právny rámec, ktorý tvorí „zložitá interakcia“ medzi tromi samostatnými právnymi predpismi – zákonom o ľudských právach z roku 1998, zákonom o spravodajských službách z roku 1994 a zákonom o regulácii vyšetrovacích právomocí z roku 2000;

24. berie na vedomie revíziu holandského zákona o spravodajských a bezpečnostných službách z roku 2002 (správa Dessensovej komisie z 2. decembra 2013); podporuje tie odporúčania revíznej komisie, ktoré sú zamerané na posilnenie transparentnosti, kontroly a dohľadu nad holandskými spravodajskými službami; vyzýva Holandsko, aby sa zdržalo rozširovania právomocí spravodajských služieb takým spôsobom, ktorým by sa umožňovalo aj vykonávanie necieleného a rozsiahleho monitorovania káblových komunikácií nevinných občanov, najmä vzhľadom na skutočnosť, že jedno z najväčších internetových prepojovacích centier na svete sa nachádza v Amsterdame (AMS-IX); požaduje obozretnosť pri vymedzovaní mandátu a kapacít nového útvaru Joint Sigint Cyber Unit, ako aj obozretnosť v súvislosti s prítomnosťou a operáciami pracovníkov spravodajskej služby USA na území Holandska;

25. vyzýva členské štáty vrátane ich vlastných spravodajských agentúr, aby neprijímali údaje z tretích štátov, ktoré sa zozbierali nezákonne, a neumožňovali na svojom území sledovanie vládami alebo agentúrami tretích štátov, ktoré je podľa vnútroštátneho práva nezákonné alebo neposkytuje právne záruky zakotvené v medzinárodných nástrojoch alebo nástrojoch EÚ vrátane ochrany ľudských práv podľa ZEÚ, EDĽP a Charty základných práv Európskej únie;

26. žiada ukončenie hromadného zachytávania a spracovania snímok z webových kamier akoukoľvek tajnou službou; vyzýva členské štáty, aby naplno vyšetrovali či, ako a do akej miery sa ich príslušné tajné služby podieľali na získavaní a spracovaní snímok z webových kamier a aby vymazali všetky uložené snímky získané prostredníctvom takýchto programov hromadného sledovania;

27. vyzýva členské štáty, aby si bezodkladne splnili svoj záväzok podľa Európskeho dohovoru o ľudských právach na ochranu svojich občanov pred sledovaním tretími štátmi alebo ich vlastnými spravodajskými službami navzdory požiadavkám dohovoru, a to aj v prípadoch, keď je jeho cieľom chrániť národnú bezpečnosť, a zabezpečiť, aby sa zásady právneho štátu neoslabili v dôsledku uplatňovania právnych predpisov tretích krajín mimo ich územia;

28. vyzýva generálneho tajomníka Rady Európy, aby začal postup podľa článku 52, podľa ktorého „každá vysoká zmluvná strana poskytne na žiadosť generálneho tajomníka Rady Európy vysvetlenie o spôsobe, akým jej vnútroštátne právo zabezpečuje účinné vykonávanie všetkých ustanovení tohto dohovoru“;

29. vyzýva členské štáty, aby bezodkladne prijali primerané opatrenia vrátane súdneho konania proti narušeniu zvrchovanosti, a teda porušeniu všeobecného medzinárodného verejného práva, ku ktorému došlo prostredníctvom programov hromadného sledovania; ďalej vyzýva členské štáty EÚ, aby využili všetky dostupné medzinárodné opatrenia na obranu základných práv občanov EÚ, a to najmä začatím medzištátneho konania žaloby v súlade s článkom 41 Medzinárodného paktu o občianskych a politických právach;

30. vyzýva členské štáty, aby zriadil účinné mechanizmy, na základe ktorých sa budú osoby zodpovedné za programy (hromadného) sledovania, ktoré sú v rozpore so zásadami právneho štátu a základnými právami občanov, zodpovedať za zneužitie právomoci;

31. vyzýva Spojené štáty, aby bezodkladne zrevidovali svoje právne predpisy v záujme ich zladenia s medzinárodným právom, uznali právo na súkromie a ďalšie práva občanov EÚ, zabezpečili súdnu nápravu pre občanov EÚ, zrovnoprávnili práva občanov EÚ s právami občanov USA a podpísali opčný protokol, ktorý v rámci Medzinárodného paktu o občianskych a politických právach umožňuje jednotlivcom podávať sťažnosti;

32. v tejto súvislosti víta pripomienky a politickú smernicu, ktorú vydal prezident USA Obama 17. januára 2014, ako krok smerom k obmedzovaniu povolenia na využívanie sledovania a spracúvania údajov na účely národnej bezpečnosti a ako krok smerom k rovnakému zaobchádzaniu so všetkými osobnými informáciami jednotlivcov bez ohľadu na ich štátnu príslušnosť alebo bydlisko zo strany spravodajských služieb USA; v kontexte vzťahov medzi EÚ a USA však očakáva ďalšie konkrétne kroky, ktoré, a čo je najdôležitejšie, posilnia dôveru v transatlantický prenos údajov a poskytnú záväzné záruky v oblasti vymáhateľných práv na súkromie občanov EÚ, ako sa podrobne uvádza v tejto správe;

33. zdôrazňuje svoje znepokojenie v súvislosti s prácou výboru Dohovoru o počítačovej kriminalite Rady Európy pri výklade článku 32 Dohovoru o počítačovej kriminalite z 23. novembra 2001 (Budapeštiansky dohovor), ktorý sa týka cezhraničného prístupu k uloženým počítačovým údajom na základe súhlasu, alebo ak sú verejne dostupné, a nesúhlasí so záverom dodatkového protokolu alebo pokynov, ktorých zámerom je rozšíriť rozsah tohto ustanovenia nad súčasný režim zriadený týmto dohovorom, čo predstavuje veľkú výnimku k zásade teritoriality, lebo by mohol viesť k neobmedzenému diaľkovému prístupu orgánov presadzovania práva k serverom a počítačom, ktoré sa nachádzajú v iných jurisdikciách bez toho, aby sa odvolával na dohody o vzájomnej právnej pomoci a iné nástroje súdnej spolupráce, ktoré majú zaručiť základné práva pre jednotlivcov vrátane ochrany údajov a ich riadneho spracovania, a to najmä dohovoru Rady Európy č. 108;

34. vyzýva Komisiu, aby do júla 2014 vyhodnotila uplatniteľnosť nariadenia (ES) č. 2271/96 na prípady kolízie právnych predpisov týkajúcich sa prenosov osobných údajov;

35. vyzýva Agentúru pre základné práva, aby začala dôkladný výskum ochrany základných práv v súvislosti so sledovaním, a najmä súčasnej zákonnej situácie občanov EÚ, čo sa týka justičných nápravných prostriedkov, ktoré majú k dispozícii v súvislosti s týmito praktikami;

Medzinárodné prenosy údajov

Právny rámec USA na ochranu údajov a bezpečný prístav USA

36. konštatuje, že spoločnosti, ktoré boli podľa odhalení médií zapojené do rozsiahleho hromadného sledovania príslušných občanov EÚ agentúrou Spojených štátov NSA, sú spoločnosti, ktoré majú vlastné osvedčenie o dodržiavaní zásad bezpečného prístavu, a že bezpečný prístav je právny nástroj používaný na prenos osobných údajov z EÚ do USA (napríklad Google, Microsoft, Yahoo!, Facebook, Apple a LinkedIn); vyjadruje obavy z toho, že tieto organizácie nešifrovali informácie a komunikácie, ktoré prúdia medzi ich dátovými centrami, čím umožňujú spravodajským službám zachytiť tieto informácie; víta neskoršie vyhlásenia niektorých spoločností USA, že urýchlia plány na šifrovanie tokov údajov medzi svojimi globálnymi dátovými centrami;

37. domnieva sa, že rozsiahly prístup spravodajských agentúr USA k osobným údajom EÚ spracúvaným v rámci mechanizmu bezpečného prístavu nespĺňa kritériá na odchýlku v rámci „národnej bezpečnosti“;

Streda 12. marca 2014

38. zastáva názor, že za súčasných okolností zásady bezpečného prístavu neposkytujú primeranú ochranu pre občanov EÚ, a preto by sa tieto prenosy mali vykonávať v rámci iných nástrojov, ako sú zmluvné doložky alebo záväzné firemné pravidlá, za predpokladu, že tieto nástroje stanovujú konkrétne záruky a ochranu a neobchádzajú ich iné zákonné rámce;

39. zastáva názor, že Komisia nevykonala nápravu známych nedostatkov týkajúcich sa súčasnej realizácie bezpečného prístavu;

40. vyzýva Komisiu, aby predložila opatrenia, ktorými zabezpečí okamžité pozastavenie platnosti rozhodnutia Komisie č. 2000/520/ES, kde sa deklarovala primeranosť zásad ochrany súkromia v rámci mechanizmu bezpečného prístavu a súvisiacich často kladených otázok (FAQ) vydaných Ministerstvom obchodu USA; preto vyzýva orgány USA, aby predložili návrh na nový rámec na prenos osobných údajov z EÚ do USA, ktorý spĺňa zákonné požiadavky Únie na ochranu údajov a zabezpečuje požadovanú primeranú úroveň ochrany;

41. vyzýva príslušné orgány členských štátov, najmä orgány na ochranu údajov, aby využili existujúce právomoci a bezodkladne pozastavili toky údajov do každej organizácie, ktorá má vlastné osvedčenie o dodržiavaní zásad bezpečného prístavu USA, a požadovali, aby sa tieto toky údajov vykonávali iba v rámci iných nástrojov a za predpokladu, že obsahujú potrebné záruky a ochranu, čo sa týka ochrany súkromia a základných práv a slobôd jednotlivcov;

42. vyzýva Komisiu, aby do decembra 2014 predložila komplexné hodnotenie rámca USA na ochranu súkromia, ktorý sa vzťahuje na obchodné činnosti, činnosti presadzovania práva a spravodajské činnosti, a konkrétne odporúčania vyplývajúce z neexistencie všeobecného zákona o ochrane údajov v USA; vyzýva Komisiu, aby sa spojila s vládou USA v záujme vytvorenia právneho rámca, ktorý by poskytoval vysokú úroveň ochrany jednotlivcov, čo sa týka ochrany ich osobných údajov pri prenose do USA, a zabezpečoval rovnocennosť rámcov EÚ a USE na ochranu súkromia;

Prenosy do iných tretích krajín na základe rozhodnutia o primeranosti

43. pripomína, že v smernici 95/46/ES sa stanovuje, že prenosy osobných údajov do tretej krajiny sa môžu vykonávať iba vtedy, keď bez toho, aby bolo dotknuté dodržiavanie vnútroštátnych ustanovení prijatých na základe ostatných ustanovení smernice, príslušná tretia krajina poskytne primeranú úroveň ochrany, pričom účelom tohto ustanovenia je zabezpečenie súvislej ochrany, ktorú poskytujú právne predpisy EÚ o ochrane údajov pri prenose osobných údajov mimo EÚ;

44. pripomína, že v smernici 95/46/ES sa takisto stanovuje, že primeranosť úrovne ochrany poskytovanej treťou stranou sa má hodnotiť na základe všetkých okolností súvisiacich s operáciou prenosu údajov či súborom týchto operácií; rovnako pripomína, že uvedenou smernicou sa poskytujú Komisii vykonávacie právomoci na vydanie vyhlásenia, že tretia krajina zaručuje primeranú úroveň ochrany na základe kritérií stanovených v smernici 95/46/ES; pripomína, že na základe smernice 95/46/ES sa Komisia splnomocňuje aj na vydanie vyhlásenia, že tretia krajina nezaručuje primeranú úroveň ochrany;

45. pripomína, že v druhom prípade členské štáty musia prijať nevyhnutné opatrenia, aby zabránili každému prenosu údajov rovnakého druhu do príslušnej tretej krajiny, a že Komisia by mala začať rokovania s cieľom nápravy tejto situácie;

46. vyzýva Komisiu a členské štáty, aby bezodkladne zhodnotili, či na primeranú úroveň ochrany osobných údajov novozélandského zákona o ochrane súkromia a kanadského zákona o ochrane osobných údajov a elektronických dokumentov, ktorá bola deklarovaná v rozhodnutiach Komisie 2013/65/EÚ a 2002/2/ES, malo vplyv zapojenie národných spravodajských agentúr týchto krajín do hromadného sledovania občanov EÚ, a aby v prípade potreby prijali primerané opatrenia na pozastavenie alebo zrušenie platnosti rozhodnutí o primeranosti; vyzýva Komisiu, aby vyhodnotila situáciu v iných krajinách, ktoré získali rating primeranosti; očakáva, že Komisia predloží Parlamentu správu o svojich zisteniach týkajúcich sa uvedených krajín najneskôr do decembra 2014;

Prenosy na základe zmluvných doložiek a iných nástrojov

47. pripomína, že vnútroštátne orgány na ochranu údajov naznačili, že pri vypracúvaní štandardných zmluvných doložiek a záväzných firemných pravidiel sa nebrali do úvahy situácie súvisiace s prístupom k osobným údajom na účely hromadného sledovania a že tento prístup by nebol v súlade s ustanoveniami zmluvných doložiek či záväzných firemných pravidiel o odchýlkach, ktoré sa týkajú výnimočných a prípadne nevyhnutných a primeraných odchýlok v oprávnenom záujme v demokratickej spoločnosti;

48. vyzýva členské štáty, aby zakázali alebo pozastavili toky údajov do tretích krajín na základe štandardných zmluvných doložiek, zmluvných doložiek alebo záväzných firemných pravidiel schválených príslušnými vnútroštátnymi orgánmi, ak možno predpokladať, že právne predpisy vzťahujúce sa na príjemcov údajov im ukladajú povinnosti, ktoré presahujú rámec obmedzení nevyhnutných v demokratickej spoločnosti a ktoré by mohli mať nepriaznivý vplyv na záruky poskytované platnými právnymi predpismi v oblasti ochrany údajov a štandardnými zmluvnými doložkami alebo preto, že pokračujúci prenos by predstavoval riziko vážneho poškodenia príslušných osôb;

49. vyzýva pracovnú skupinu zriadenú podľa článku 29, aby vydala usmernenia a odporúčania týkajúce sa záruk a ochrany, ktoré by zmluvné nástroje pre medzinárodné prenosy osobných údajov EÚ mali obsahovať v záujme zabezpečenia ochrany súkromia, základných práv a slobôd jednotlivcov, najmä vzhľadom na predpisy tretích krajín týkajúce sa spravodajských činností a národnej bezpečnosti a zapojenie spoločností, ktoré prijímajú údaje v tretej krajine, do hromadného sledovania spravodajskými agentúrami tretích krajín;

50. vyzýva Komisiu, aby bezodkladne preskúmala štandardné zmluvné doložky, ktoré ustanovila, s cieľom posúdiť, či poskytujú potrebnú ochranu, pokiaľ ide o prístup k osobným údajom prenášaným v rámci doložiek na spravodajské účely, a podľa potreby ich zrevidovala;

Prenosy na základe Dohody o vzájomnej právnej pomoci

51. vyzýva Komisiu, aby do konca roka 2014 vykonala dôkladné posúdenie súčasnej Dohody o vzájomnej právnej pomoci v súlade s jej článkom 17 s cieľom overiť jej vykonávanie v praxi a najmä, či ju USA účinne využívajú na získavanie informácií alebo dôkazov v EÚ a či sa táto dohoda neobchádza so zámerom získať informácie priamo v EÚ, a posúdiť vplyv na základné práva jednotlivcov; toto posúdenie by sa nemalo týkať len oficiálnych vyhlásení USA ako postačujúceho východiska pre analýzu, ale malo by vychádzať aj z konkrétnych hodnotení EÚ; toto dôkladné preskúmanie by sa malo zamerať aj na dôsledky uplatňovania ústavnej štruktúry Únie na tento nástroj s cieľom uviesť ho do súladu s právom Únie, najmä vzhľadom na jeho protokol 36 a článok 10 a na vyhlásenie 50 týkajúce sa tohto protokolu; zároveň vyzýva Komisiu, aby posúdila bilaterálne dohody uzatvorené medzi členskými štátmi a USA s cieľom zabezpečiť súlad medzi týmito bilaterálnymi dohodami a dohodami, ktoré EÚ uzatvára alebo plánuje uzatvoriť s USA;

Vzájomná pomoc v trestných veciach v EÚ

52. vyzýva Radu a Komisiu, aby informovali Parlament o tom, ako členské štáty skutočne aplikujú Dohovor o vzájomnej pomoci v trestných veciach medzi členskými štátmi, najmä jeho hlavu III o zachytávaní telekomunikácií; vyzýva Komisiu, aby do konca roka 2014 predložila návrh v súlade s vyhlásením 50 týkajúci sa protokolu 36, ako sa požadovalo, s cieľom prispôsobiť ho rámcu Lisabonskej zmluvy;

Prenosy na základe dohody o TFTP a dohody o PNR

53. zastáva názor, že informácie, ktoré poskytuje Európska komisia a Ministerstvo financií Spojených štátov, neobjasňujú, či spravodajské agentúry USA zachytávajú komunikácie zo sietí SWIFT, operačných systémov bánk alebo komunikačných sietí a majú tak prístup k finančným správam systému SWIFT v EÚ samostatne alebo v spolupráci s národnými spravodajskými agentúrami EÚ a bez použitia existujúcich bilaterálnych kanálov vzájomnej právnej pomoci a justičnej spolupráce;

Streda 12. marca 2014

54. pripomína svoje uznesenie z 23. októbra 2013 a žiada Komisiu o pozastavenie platnosti dohody o TFTP;

55. vyzýva Komisiu, aby reagovala na obavy, že tri hlavné počítačové rezervačné systémy, ktoré používajú letecké spoločnosti na celom svete, sídlia v USA a údaje PNR sú uložené v systémoch cloudu, ktoré fungujú na americkej pôde podľa právnych predpisov USA, kde ochrana údajov nie je dostatočná;

Rámcová dohoda o ochrane údajov v oblasti policajnej a justičnej spolupráce („zastrešujúca dohoda")

56. domnieva sa, že uspokojujúce riešenie v rámci „zastrešujúcej dohody" je podmienkou na úplné obnovenie dôvery medzi transatlantickými partnermi;

57. žiada o okamžité obnovenie rokovaní so USA o „zastrešujúcej dohode", ktorá by mala stanoviť jasné práva pre občanov EÚ na rovnakom právnom základe ako sú práva občanov USA; navyše zdôrazňuje, že v tejto dohode by sa mali stanoviť účinné a vymožiteľné správne a justičné prostriedky pre všetkých občanov EÚ v USA bez diskriminácie;

58. žiada Komisiu a Radu, aby neiniciovali so USA nijaké nové odvetvové dohody ani dojednania o prenose osobných údajov na účely presadzovania práva, kým nenadobudne platnosť „zastrešujúca dohoda";

59. vyzýva Komisiu, aby do apríla 2014 podrobne informovala o jednotlivých bodoch rokovacieho poverenia a o súčasnom stave;

Reforma ochrany údajov

60. vyzýva predsedníctvo Rady a členské štáty, aby urýchlili prácu na celom balíku ochrany údajov s cieľom umožniť jeho prijatie v roku 2014 tak, že občania EÚ sa budú môcť v blízkej budúcnosti tešiť z vysokej úrovne ochrany údajov; zdôrazňuje, že rozhodné konanie a plná podpora zo strany Rady sú nevyhnutnou podmienkou na preukázanie dôveryhodnosti a asertivity voči tretím krajinám;

61. zdôrazňuje, že nariadenie o ochrane údajov aj smernica o ochrane údajov sú nevyhnutné na ochranu základných práv jednotlivcov, a preto treba obe smernice vnímať ako balík opatrení, ktoré treba prijať súčasne s cieľom zabezpečiť, aby všetky činnosti spracúvania údajov v EÚ poskytovali vysokú úroveň ochrany za všetkých okolností; zdôrazňuje, že ďalšie opatrenia v oblasti spolupráce pri presadzovaní práva prijme len vtedy, keď Rada začne rokovať s Parlamentom a Komisiou o balíku ochrany údajov;

62. pripomína, že koncepcie špecifickej ochrany súkromných informácií a automatickej ochrany osobných údajov predstavujú posilnenie ochrany údajov a mali by mať štatút usmernení pre všetky produkty, služby a systémy poskytované cez internet;

63. považuje väčšiu transparentnosť a prísnejšie bezpečnostné normy pre internet a telekomunikácie za nevyhnutnú zásadu smerujúcu k lepšiemu systému ochrany údajov; preto vyzýva Komisiu, aby predložila právny návrh na štandardizované všeobecné zmluvné podmienky pre internet a telekomunikácie a aby poverila orgán dohľadu, aby monitoroval dodržiavanie všeobecných zmluvných podmienok;

Cloud computing

64. konštatuje, že uvedená prax negatívne ovplyvnila dôveru v cloud computing v USA a k poskytovateľom cloudu; preto zdôrazňuje, že vývoj európskeho cloudu a IT riešení je základným prvkom pre rast a zamestnanosť, dôveru v služby cloud computingu a k poskytovateľom cloud computingu, ako aj na zabezpečenie vysokej úrovne ochrany osobných údajov;

65. žiada všetky verejné orgány v Únii, aby nevyužívali služby cloudu v prípadoch, keď sa môže uplatňovať aj iné právo než právo EÚ;

66. opakuje svoje vážne obavy v súvislosti s tým, že poskytovatelia cloudu, ktorí podliehajú zákonom tretej krajiny alebo používajú na ukladanie údajov servery umiestnené v tretích krajinách, sú povinní priamo poskytovať osobné údaje a informácie EÚ spracúvané podľa dohôd o službách cloudu, ako aj poskytovať priamy diaľkový prístup k týmto osobným údajom a informáciám orgánom na presadzovanie práva a spravodajským službám tretej krajiny;

67. odsudzuje skutočnosť, že tento prístup sa zvyčajne poskytuje prostredníctvom priameho presadzovania právnych predpisov orgánmi tretích krajín bez toho, aby sa využívali medzinárodné nástroje zriadené na právnu spoluprácu, ako sú dohody o vzájomnej právnej pomoci alebo iné formy justičnej spolupráce;

68. vyzýva Komisiu a členské štáty, aby urýchlili zriadenie Európskeho partnerstva pre cloud, pričom by v plnej miere zapojili občiansku spoločnosť a technickú komunitu, napríklad osobitnú skupinu pre internetovú techniku (IETF), a aby zohľadnili aspekty ochrany údajov;

69. naliehavo vyzýva Komisiu, aby pri rokovaniach o medzinárodných dohodách, ktoré sa týkajú spracovania osobných údajov, venovala osobitnú pozornosť rizikám a problémom spojeným s cloud computingom, ktoré môžu ohroziť základné práva, a ako aj najmä právo na súkromie a na ochranu osobných údajov, ktoré sú zakotvené v článku 7 a 8 Charty základných práv Európskej únie; okrem toho naliehavo vyzýva Komisiu, aby venovala pozornosť vnútroštátnym predpisom rokovacieho partnera, ktorými sa riadu prístup orgánov presadzovania práva a spravodajských agentúr k osobným údajom spracovávaným prostredníctvom služieb cloud computingu, najmä tým, že bude žiadať, aby sa prístup povolil iba na základe dodržania riadneho právneho postupu a existencie jednoznačného právneho základu, ako aj požiadavke, aby sa vymedzili presné podmienky prístupu, účel získania tohto prístupu, bezpečnostné opatrenia zavedené pri poskytovaní údajov, práva jednotlivcov, ako aj pravidlá dohľadu a účinný mechanizmus odškodnenia;

70. pripomína, že všetky spoločnosti poskytujúce služby v EÚ musia bez výnimky dodržiavať zákony EÚ a nesú zodpovednosť za všetky ich porušenia, a zdôrazňuje význam využívania efektívnych, primeraných a odrádzajúcich správnych postihov, ktoré sa môžu uplatniť na poskytovateľov služieb cloud computingu, ktorí nedodržiavajú normy EÚ na ochranu údajov;

71. žiada Komisiu a príslušné orgány členských štátov, aby vyhodnotili, v akom rozsahu došlo k porušeniu predpisov EÚ v oblasti ochrany súkromia a údajov v dôsledku spolupráce právnych subjektov EÚ so spravodajskými službami alebo v dôsledku prijatia súdnych príkazov orgánov tretích krajín, ktoré požadovali osobné údaje o občanoch EÚ v rozpore s právnymi predpismi EÚ v oblasti ochrany údajov;

72. vyzýva podniky poskytujúce nové služby prostredníctvom technológií „big data“ a nových aplikácií, napríklad „internet vecí“, aby v záujme zachovania vysokej úrovne dôvery občanov zapracovali opatrenia na ochranu údajov už vo vývojovej fáze;

Dohoda o transatlantickom obchodnom a investičnom partnerstve (TTIP)

73. uznáva, že EÚ a USA štáty pokračujú v rokovaniach o transatlantickom obchodnom a investičnom partnerstve, ktoré má veľký strategický význam pre ďalší hospodársky rast;

74. dôrazne poukazuje na skutočnosť, že vzhľadom na význam digitálnej ekonomiky v tomto vzťahu a v záujme obnovy dôvery medzi EÚ a USA môže byť súhlas Európskeho parlamentu s konečnou dohodou o TTIP ohrozený, ak sa úplne nezastavia plošné hromadné sledovanie a hromadné spracovanie osobných údajov, ako aj odpočúvanie komunikácie v inštitúciách EÚ a v diplomatických zastupiteľstvách a ak sa nenájde vhodné riešenie týkajúce sa práv občanov EÚ na súkromie údajov vrátane administratívnych a súdnych opravných prostriedkov; zdôrazňuje, že Parlament môže súhlasiť

s konečnou dohodou o TTIP iba vtedy, keď bude dohoda plne rešpektovať okrem iného základné práva uznané v charte EÚ, a že ochrana súkromia jednotlivcov v súvislosti so spracovaním a zverejňovaním osobných údajov sa naďalej riadi článkom XIV dohody GATS; zdôrazňuje, že právne predpisy EÚ v oblasti ochrany údajov nemožno považovať za svojvoľnú ani neoprávnenú diskrimináciu pri uplatňovaní článku XIV dohody GATS;

Demokratický dohľad nad spravodajskými službami

75. zdôrazňuje, že napriek skutočnosti, že dohľad nad činnosťou spravodajských služieb by mal byť založený na demokratickej legitímnosti (pevný právny rámec, oprávnenia ex ante a overenia ex post) aj na primeranej technickej spôsobilosti a odbornosti, väčšine súčasných orgánov dohľadu EÚ a USA veľmi chýbajú obe, najmä technické spôsobilosti;

76. ako v prípade systému Echelon vyzýva všetky národné parlamenty, ktoré doposiaľ nezaviedli zmysluplný dohľad nad činnosťami spravodajských služieb vykonávaný parlamentnými alebo odbornými orgánmi so zákonnými vyšetrovacími právomocami, aby tak urobili; vyzýva národné parlamenty, aby zabezpečili, aby výbory/orgány vykonávajúce tento dohľad mali dostatočné zdroje, technické odborné znalosti a právne prostriedky vrátane práva na vykonávanie návštev na mieste, aby mohli účinne kontrolovať spravodajské služby;

77. požaduje vytvorenie skupiny poslancov a expertov, ktorá by transparentne a v spolupráci s národnými parlamentmi navrhovala odporúčania, ktoré treba prijať na posilnenie demokratickej kontroly vrátane parlamentnej kontroly nad spravodajskými službami a na posilnenie spolupráce v oblasti dohľadu v EÚ, najmä čo sa týka jej cezhraničného rozmeru; domnieva sa, že skupina by mala najmä preskúmať možnosť stanoviť minimálne európske normy alebo usmernenia v oblasti dohľadu nad spravodajskými službami (vykonávaného ex ante a ex post), ktoré by vychádzali z existujúcich osvedčených postupov a odporúčaní medzinárodných organizácií (OSN, Rada Európy) týkajúcich sa kontroly a zodpovednosti spravodajských služieb zo zahraničia, vrátane toho, že orgány dohľadu sú podľa „pravidla tretej strany" považované za tretiu stranu, alebo vrátane zásady „kontroly pôvodcom", možnosť vytvoriť kritériá pre zvýšenú transparentnosť na základe všeobecnej zásady prístupu k informáciám a tzv. zásad z Tshwane ([1]), ako aj možnosť vytvoriť zásady týkajúce sa obmedzenia, pokiaľ ide o trvanie a rozsah prípadného sledovania, pričom je potrebné zabezpečiť, aby toto sledovanie bolo primerané a obmedzené so zreteľom na daný účel;

78. vyzýva túto skupinu, aby vypracovala správu slúžiacu na prípravu konferencie, ktorú má Parlament v úmysle usporiadať do konca roka 2015 a do ktorej by sa zapojili národné orgány dohľadu, či už parlamentné alebo nezávislé;

79. vyzýva členské štáty, aby využili osvedčené postupy s cieľom zlepšiť prístup svojich orgánov dohľadu k informáciám o činnostiach spravodajských služieb (vrátane tajných informácií a informácií od iných služieb) a určili právomoc na vykonávanie kontrol na mieste, rozsiahly súbor vyšetrovacích právomocí, primerané zdroje a technické odborné znalosti, striktnú nezávislosť od vlády a povinnosť podávať správy svojim parlamentom;

80. vyzýva členské štáty, aby vyvinuli spoluprácu medzi orgánmi dohľadu, najmä v rámci Európskej siete vnútroštátnych orgánov dohľadu nad spravodajskými službami (ENNIR);

81. naliehavo vyzýva PK/VP, aby zodpovedné orgány Parlamentu pravidelne informovala o činnosti Centra EÚ pre analýzu spravodajských informácií (IntCen), ktoré je súčasťou Európskej služby pre vonkajšiu činnosť, vrátane riadneho dodržiavania základných ľudských práv a platných predpisov EÚ v oblasti súkromia údajov a aby tak Parlamentu umožnila lepšie dohliadať na vonkajšie aspekty politík EÚ; naliehavo žiada Komisiu a PK/VP, aby predložili návrh právneho základu pre činnosti strediska IntCen, ak sa plánujú pre toto stredisko akékoľvek vlastné operácie alebo budúce právomoci v oblasti štruktúry pre zhromažďovanie spravodajských informácií alebo údajov, ktoré by mohli mať vplyv na stratégiu vnútornej bezpečnosti EÚ;

([1]) Globálne zásady národnej bezpečnosti a právo na informácie, jún 2013.

82. vyzýva Komisiu, aby do decembra 2014 predložila návrh na európsky postup bezpečnostnej previerky vzťahujúci sa na všetkých úradníkov EÚ, pretože v súčasnom systéme, v rámci ktorého členské štáty vykonávajú bezpečnostnú previerku štátnej príslušnosti, sa stanovujú rozličné požiadavky a dĺžky trvania postupov v rámci vnútroštátnych systémov, čoho výsledkom je odlišné zaobchádzanie s poslancami Parlamentu a ich pracovníkmi v závislosti od štátnej príslušnosti;

83. pripomína ustanovenia medziinštitucionálnej dohody medzi Európskym parlamentom a Radou o postupovaní utajovaných informácií, ktorých držiteľom je Rada a ktoré sa netýkajú vecí v oblasti spoločnej zahraničnej a bezpečnostnej politiky, a o a spracúvaní týchto informácií Parlamentom, ktoré by sa mali použiť na zlepšenie dohľadu na úrovni EÚ;

Agentúry EÚ

84. vyzýva spoločný dozorný orgán Europolu, aby spolu s vnútroštátnymi orgánmi na ochranu údajov vykonali do konca roka 2014 spoločnú inšpekciu na zistenie, či vnútroštátne orgány zákonne získali informácie a osobné údaje, ktoré si vymieňajú s Europolom, najmä ak tieto informácie alebo údaje získali pôvodne spravodajské služby v EÚ alebo tretej krajine, a či sa zaviedli primerané opatrenia na zabránenie použitiu a ďalšiemu šíreniu týchto informácií alebo údajov; domnieva sa, že Europol by nemal spracúvať nijaké informácie ani údaje, ktoré sa získali porušením základných práv, ktoré sú chránené podľa Charty základných práv;

85. vyzýva Europol, aby plne využil svoj mandát a požiadal príslušné orgány členských štátov o začatie vyšetrovania v súvislosti s rozsiahlymi počítačovými útokmi a prienikmi do sietí IT s možnými cezhraničnými dôsledkami; je presvedčený, že mandát Europolu by sa mal posilniť, aby mohol začať vlastné vyšetrovanie na základe podozrenia z úmyselného útoku na sieť a informačné systémy viacerých členských štátov alebo orgánov Únie ([1]); vyzýva Komisiu, aby preskúmala činnosti Európskeho centra boja proti počítačovej kriminalite a aby podľa potreby predložila návrh na komplexný rámec na posilnenie jeho kompetencií;

Sloboda prejavu

86. vyjadruje hlboké znepokojenie nad rastúcimi hrozbami pre slobodu tlače a odradzujúcimi účinkami zastrašovania novinárov štátnymi orgánmi, najmä čo sa týka ochrany dôvernosti novinárskych zdrojov; pripomína výzvy vyjadrené v uznesení z 21. mája 2013 s názvom Charta EÚ: stanovenie noriem pre slobodu médií v EÚ;

87. berie na vedomie zadržanie pána Mirandu a konfiškáciu materiálov v jeho vlastníctve orgánmi Veľkej Británie podľa dodatku 7 protiteroristického zákona z roku 2000 (Terrorism Act) (ako aj požiadavku, aby denník *The Guardian* zničil alebo odovzdal materiál) a vyjadril znepokojenie, že toto predstavuje vážne zasahovanie do práva na slobodu prejavu a slobodu médií uznanú v článku 10 EDĽP a článku 11 charty EÚ a že právne predpisy určené na boj proti terorizmu by sa v takýchto prípadoch mohli zneužívať;

88. upriamuje pozornosť na kritickú situáciu informátorov a ich podporovateľov vrátane novinárov po ich odhaleniach; vyzýva Komisiu, aby preskúmala, či by sa v budúcom legislatívnom návrhu, ktorým sa zavádza účinný a komplexný európsky program na ochranu informátorov, ako sa už požadovalo v uznesení Parlamentu z 23. októbra 2013, nemali zahrnovať aj ďalšie oblasti kompetencie Únie, pričom osobitná pozornosť by sa venovala zložitému postaveniu informátorov v spravodajských službách; vyzýva členské štáty EÚ, aby dôkladne preskúmali možnosť na poskytovanie medzinárodnej ochrany informátorom v prípade trestného stíhania;

([1]) Pozícia Európskeho parlamentu z 25. februára 2014 o návrhu nariadenia Európskeho parlamentu a Rady o agentúre Európskej únie pre spoluprácu a odbornú prípravu v oblasti presadzovania práva (Europol) (Prijaté texty, P7_TA(2014)0121).

89. vyzýva členské štáty na zabezpečenie toho, aby ich právne predpisy, najmä v oblasti národnej bezpečnosti, poskytovali bezpečnú alternatívu na mlčanlivosť v prípade odhaľovania či predkladania správ o previneniach vrátane prípadov korupcie, trestných činov, porušení zákonných povinností, justičných omylov a zneužívania moci, čo je takisto v súlade s podmienkami rozličných medzinárodných nástrojov proti korupcii (OSN a Rada Európy), so zásadami zakotvenými v rezolúcie PACE 1729(2010), zásadami z Tshwane atď.;

Bezpečnosť informačných technológií (IT) v EÚ

90. zdôrazňuje, že z nedávnych udalostí jasne vyplýva kritická zraniteľnosť EÚ, najmä inštitúcií EÚ, národných vlád a parlamentov, veľkých európskych spoločností, európskych infraštruktúr a sietí IT voči rafinovaným útokom, pri ktorých sa používa zložitý softvér a malvér; konštatuje, že tieto útoky si vyžadujú finančné a ľudské zdroje takého rozsahu, že pravdepodobne majú pôvod v štátnych subjektoch konajúcich v mene zahraničných vlád; v tejto súvislosti považuje počítačového pirátstva alebo odpočúvania v sieťach telekomunikačnej spoločnosti Belgacom za znepokojivý príklad útoku proti kapacite EÚ v oblasti IT; zdôrazňuje, že posilňovanie kapacity EÚ v oblasti IT a bezpečnosti takisto zmenšuje citlivosť EÚ voči vážnym počítačovým útokom, ktoré pochádzajú z veľkých zločineckých organizácií či teroristických zoskupení;

91. zastáva názor, že odhalenia hromadného sledovania, ktoré spôsobilo túto krízu, možno využiť ako príležitosť pre Európu na prevzatie iniciatívy a vytvorenie nezávislej kapacity kľúčových zdrojov v oblasti IT, ako strategické prioritné opatrenie; zdôrazňuje, že v záujme získania dôvery by táto európska kapacita IT mala čo najviac vychádzať z otvorených noriem a bezplatného a otvoreného softvéru a podľa možnosti aj hardvéru, čo znamená, že celý dodávateľsky reťazec od návrhu spracovania až po úroveň aplikácie bude transparentný a kontrolovateľný; poukazuje na to, že v záujme opätovného nadobudnutia konkurencieschopnosti v strategickom sektore služieb v oblasti IT treba uzavrieť novú digitálnu dohodu na základe spoločného a rozsiahleho úsilia inštitúcií EÚ, členských štátov, výskumných ústavov, priemyslu a občianskej spoločnosti; vyzýva Komisiu a členské štáty, aby využili verejné obstarávanie ako pákový efekt na podporu takej kapacity zdrojov v EÚ prostredníctvom určenia noriem EÚ v oblasti bezpečnosti a súkromia za hlavné požiadavky vo verejnom obstarávaní tovarov a služieb v oblasti IT; preto naliehavo vyzýva Komisiu, aby revidovala súčasné postupy v oblasti verejného obstarávania vo veci spracúvania údajov, aby sa mohlo posúdiť obmedzenie postupov verejného obstarávania len na certifikované spoločnosti a prípadne na spoločnosti EÚ, ak ide o bezpečnostné alebo rozhodujúce záujmy;

92. rozhodne odsudzuje skutočnosť, že spravodajské služby sa usilovali o zníženie bezpečnostných noriem v oblasti IT a vkladanie vírusov typu „backdoor“ do veľkého palety systémov IT; žiada Komisiu, aby predložila návrh právnych predpisov na zákaz používania vírusov typu „backdoor“ agentúrami na presadzovanie práva; preto odporúča používanie softvéru s otvoreným kódom vo všetkých prostrediach, kde existujú obavy o bezpečnosť IT;

93. vyzýva všetky členské štáty, Komisiu, Radu a Európsku radu, aby v plnej miere podporovali rozvoj európskych inovačných a technologických kapacít v oblasti nástrojov IT, spoločností a poskytovateľov (hardvér, softvér, služby a sieť), aj v záujme počítačovej bezpečnosti, a šifrovanie a šifrovacie kapacity, a to aj pomocou financovania v oblasti výskumu a vývoja; vyzýva všetky príslušné orgány a inštitúcie EÚ a členské štáty, aby investovali do miestnych a nezávislých technológií EÚ a aby mohutne rozvíjali a zvyšovali detekčné schopnosti;

94. vyzýva Komisiu, normalizačné orgány a agentúru ENISA, aby do decembra 2014 vytvorili minimálne normy v oblasti bezpečnosti a ochrany súkromia a usmernenia pre informačné systémy, siete a služby vrátane služieb tzv. cloud computingu s cieľom lepšej ochrany osobných údajov občanov EÚ a integrity všetkých informačných systémov; domnieva sa, že tieto normy by sa mohli stať meradlom pre nové celosvetové normy a mali by sa stanoviť v otvorenom a demokratickom procese, a nemala by ich presadzovať jedna krajina, subjekt ani nadnárodná spoločnosť; domnieva sa, že aj keď treba brať do úvahy zákonné presadzovanie práva a záujmy spravodajských služieb s cieľom podporiť boj proti terorizmu, ich výsledkom by nemalo byť všeobecné oslabenie závislosti všetkých informačných systémov; vyjadruje podporu nedávnych rozhodnutí osobitnej skupiny pre internetovú techniku (IETF) o zahrnutí vlád do modelu ohrozenia internetovej bezpečnosti;

95. poukazuje na to, že EÚ a vnútroštátne telekomunikačné regulačné orgány, a v niektorých prípadoch aj telekomunikačné spoločnosti, jednoznačne zanedbávajú bezpečnosť používateľov a klientov v oblasti IT; vyzýva Komisiu, aby plne využila svoje existujúce právomoci vyplývajúce z rámcovej smernice o súkromí a elektronických komunikáciách na posilnenie ochrany dôvernosti komunikácie prostredníctvom prijatia opatrení s cieľom zabezpečiť, aby boli koncové zariadenia zlučiteľné s právom používateľov na kontrolu a ochranu svojich osobných údajov, a zabezpečiť vysokú úroveň bezpečnosti telekomunikačných sietí a služieb, a to aj používaním najmodernejšieho šifrovania komunikácie po celej dĺžke spojenia;

96. podporuje stratégiu počítačovej bezpečnosti EÚ, ale domnieva sa, že nezahrnuje všetky možné hrozby a mala by sa posilniť tak, aby zahŕňala konanie štátu so zlým úmyslom; poukazuje na potrebu robustnejšej informačnej bezpečnosti a odolnosti informačných systémov;

97. vyzýva Komisiu, aby najneskôr do januára 2015 predložila akčný plán na posilnenie nezávislosti EÚ v odvetví IT vrátane súdržnejšieho prístupu k podpore európskych technologických kapacít v odvetví IT (vrátane informačných systémov, zariadení, služieb, cloud computingu, šifrovania a anonymizácie) a k ochrane kritickej informačnej infraštruktúry (aj z hľadiska vlastníctva a zraniteľnosti);

98. vyzýva Komisiu, aby v rámci budúceho pracovného programu v rámci programu Horizont 2020 nasmerovala viac zdrojov na podporu európskeho výskumu, rozvoja, inovácií a odbornej prípravy v oblasti IT technológií, najmä technológií a infraštruktúr na zvýšenie ochrany súkromia, šifrovanie, bezpečných výpočtových riešení, čo najlepších bezpečnostných riešení otvoreného zdrojového kódu a ďalších služieb informačnej spoločnosti. a podporovala vnútorný trh s európskym softvérom, hardvérom a šifrovacími prostriedkami a komunikačnými infraštruktúrami vrátane vývoja komplexnej priemyselnej stratégie EÚ pre odvetvie informačných technológií; domnieva sa, že malé a stredné podniky zohrávajú vo výskume osobitnú úlohu; zdôrazňuje, že prostriedky EÚ by sa nemali vyčleňovať na projekty, ktorých jediným cieľom je vývoj nástrojov na získavanie nelegálnej prístupu do systémov IT;

99. žiada Komisiu, aby najneskôr do decembra 2014 rozvrhla súčasné zodpovednosti a preskúmala, či ENISA, Európske centrum boja proti počítačovej kriminalite, CERT-EU a EDPS a ďalšie centrá Únie so špecializovanými skúsenosťami potrebujú rozsiahlejší mandát, lepšiu koordináciu a/alebo ďalšie zdroje a technické kapacity, aby mohli zohrávať dôležitú úlohu pri zabezpečovaní európskych komunikačných systémov, boli efektívnejšie v predchádzaní a vo vyšetrovaní závažných porušení v EÚ v oblasti IT a vykonávania (alebo pomoci členským štátom a orgánom EÚ pri vykonávaní) technických vyšetrovaní na mieste týkajúcich sa závažných porušení v oblasti IT; osobitne vyzýva Komisiu, aby posúdila posilnenie úlohy ENISA pri obrane interných systémov v inštitúciách EÚ a vybudovala v rámci ENISA štruktúru zodpovedného tímu na reakcie na núdzové počítačové situácie (CERT) pre EÚ a členské štáty;

100. žiada Komisiu, aby vyhodnotila potrebu európskej akadémie pre informačné technológie, v ktorej sú združení najlepší nezávislí európski a medzinárodní odborníci vo všetkých súvisiacich oblastiach a ktorej úlohou je poskytovať všetkým dôležitým inštitúciám a orgánom EÚ vedecké poradenstvo v oblasti informačných technológií vrátane bezpečnostných stratégií;

101. vyzýva príslušné útvary sekretariátu Európskeho parlamentu, aby pod záštitou predsedu EP najneskôr do júna 2015 vykonali dôkladné preskúmanie a najneskôr do decembra 2014 predložili predbežnú správu a posúdenie závislosti počítačovej bezpečnosti Európskeho parlamentu zamerané na: rozpočtové prostriedky, ľudské zdroje, technickú kapacitu, vnútornú organizáciu a všetky príslušné prvky s cieľom dosiahnuť vysokú úroveň bezpečnosti informačných systémov Parlamentu; domnieva sa, že v rámci takého posúdenia by sa mali poskytnúť aspoň informácie, analýza a odporúčania týkajúce sa:

— nevyhnutnosti vykonávať pravidelné, prísne a nezávislé bezpečnostné audity a skúšky odolnosti voči prienikom, pričom sa vyberú externí bezpečnostní experti, čím sa zabezpečí transparentnosť a zaručí ich mandát vo vzťahu k tretím krajinám alebo akýmkoľvek záujmovým skupinám,

— začlenenia osobitných požiadaviek v oblasti bezpečnosti informačných technológií/ochrany súkromia, ktoré vychádzajú z najlepších postupov, do postupu obstarávania nových informačných systémov vrátane možnosti začleniť požiadavku slobodného softvéru ako podmienku obstarania alebo požiadavku, aby sa dôveryhodné európske spoločnosti zúčastnili na postupe obstarávania v prípade, že sú dotknuté citlivé oblasti súvisiace s bezpečnosťou,

Streda 12. marca 2014

— zoznamu spoločností, ktoré uzatvorili zmluvu s Európskym parlamentom v oblasti informačných technológií a telekomunikácií, so zreteľom na akúkoľvek informáciu o ich spolupráci so spravodajskými agentúrami, ktorá vyjde najavo (napríklad odhalenia týkajúce sa zmlúv, ktoré uzatvoril národný bezpečnostný orgán so spoločnosťou ako RSA, ktorej výrobky používa Európsky parlament na údajnú ochranu vzdialeného prístupu svojich poslancov a zamestnancov k údajom), vrátane možnosti poskytovania tých istých služieb inými, najlepšie európskymi spoločnosťami,

— spoľahlivosti a odolnosti softvéru, najmä štandardne dostupného komerčného softvéru, ktorý inštitúcie EÚ využívajú vo svojich informačných systémoch, z hľadiska prieniku a narušení zo strany orgánov presadzovania práva alebo spravodajských orgánov z EÚ či tretích krajín, aj so zreteľom na medzinárodné normy, najlepšie zásady manažmentu bezpečnostných rizík a dodržiavanie noriem EÚ pre informačnú bezpečnosť siete v oblasti porušení bezpečnosti;

— väčšieho použitia bezplatných systémov a systémov z otvorených zdrojov,

— krokov a opatrení prijatých s cieľom riešiť zvýšené používanie mobilných nástrojov (napr. inteligentné telefóny, tablety, a to na odbornej, ako aj osobnej úrovni) a ich vplyv na informačnú bezpečnosť systému,

— bezpečnosti komunikácie medzi rozličnými pracoviskami Parlamentu a bezpečnosti informačných systémov používaných v Parlamente,

— používania a umiestnenia serverov a centier IT pre informačné systémy Parlamentu a následkov na bezpečnosť a integritu systémov,

— skutočného vykonania existujúcich pravidiel týkajúcich sa narušenia bezpečnosti a rýchleho oznámenia, ktoré poskytnú poskytovatelia verejne dostupných telekomunikačných sietí príslušným orgánom,

— používania cloud computingu a služieb ukladania údajov na vzdialených počítačových zariadeniach (cloud) zo strany Parlamentu vrátane druhu takto ukladaných údajov, spôsobu ochrany obsahu a prístupu k nim a umiestnenia cloud serverov, pričom sa spresní uplatniteľný právny rámec ochrany údajov a spravodajských služieb a posúdi sa možnosť využívať iba cloud servery, ktoré sa nachádzajú na území EÚ;

— plánu, v ktorom sa počíta s väčším použitím šifrovacích technológií, najmä šifrovania overeného po celej dĺžke spojenia pre všetky počítačové a komunikačné služby, ako sú cloud computing, elektronická pošta, služby rýchlych správ a telefónia,

— používania elektronického podpisu v elektronickej pošte,

— plánu používania pravidla automatického šifrovania elektronickej pošty, napríklad GNU Privacy Guard, ktoré by súčasne umožnilo používať digitálne podpisy,

— možnosti vytvorenia bezpečnej služby rýchlych správ v Parlamente, ktorá by umožňovala bezpečnú komunikáciu, pričom na serveri by sa zobrazil len šifrovaný obsah;

102. vyzýva všetky inštitúcie a agentúry EÚ, najmä Európsku radu, Radu, Európsku službu pre vonkajšiu činnosť (vrátane delegácií EÚ), Komisiu, Súdny dvor a Európsku centrálnu banku, aby v spolupráci s agentúrou ENISA, Europolom a tímami CERT najneskôr do júna 2015 vykonali podobnú úlohu a predložili predbežnú správu do decembra 2014; vyzýva členské štáty, aby vykonali podobné posúdenie;

103. zdôrazňuje, že pokiaľ ide o vonkajšiu činnosť EÚ, v prípade Európskej služby pre vonkajšiu činnosť (ESVČ) by sa malo vykonať posúdenie súvisiacich rozpočtových potrieb a bezodkladne prijať prvé opatrenia, a že v návrhu rozpočtu na rok 2015 treba vyčleniť primerané finančné prostriedky;

104. domnieva sa, že rozsiahle informačné systémy, ktoré sa používajú v oblasti slobody, bezpečnosti a spravodlivosti, ako sú Schengenský informačný systém II, vízový informačný systém, Eurodac a prípadné budúce systémy, napríklad EU-ESTA, by sa mali vytvoriť a prevádzkovať tak, aby sa zabezpečilo, že údaje sa na základe žiadostí od orgánov tretích krajín neprezradia; žiada agentúru eu-LISA, aby do konca roka 2014 podala Parlamentu správu o spoľahlivosti zavedených systémov;

105. vyzýva Komisiu a ESVČ, aby v spolupráci so zainteresovanými partnermi prijali opatrenia na medzinárodnej úrovni, najmä v OSN, s cieľom realizovať stratégiu EÚ pre demokratickú správu internetu, a tak zabrániť nenáležitému vplyvu jednotlivých subjektov, spoločností alebo krajín na činnosti ICANN a IANA zabezpečením primeraného zastúpenia všetkých zainteresovaných strán v týchto orgánoch a súčasne sa vyhnúť možnosti štátnej kontroly, cenzúry alebo delenia a roztrieštenosti internetu;

106. vyzýva EÚ, aby sa postavila na čelo snáh o pretvorenie štruktúry a správy internetu s cieľom riešiť riziká týkajúce sa tokov údajov a ich ukladania, pričom je potrebné usilovať sa viac o minimalizáciu dát a transparentnosť a menej o hromadné ukladanie nespracovaných údajov, ako aj o presmerovanie internetovej prevádzky alebo úplné šifrovanie internetovej prevádzky po celej dĺžke, aby sa tak zabránilo súčasným rizikám spojeným so zbytočným presmerovaním prevádzky cez územie krajín, ktoré nespĺňajú základné normy v oblasti základných práv, ochrany údajov a súkromia;

107. žiada podporu pre:

— vyhľadávače EÚ a sociálne siete EÚ, ktoré sú hodnotným krokom smerujúcim k informačnej nezávislosti EÚ,

— európskych poskytovateľov informačných služieb,

— šifrovanú komunikáciu všeobecne vrátane e-mailovej a SMS komunikácie,

— európske informačné kľúčové prvky, napríklad riešenia pre operačné systémy klient – server, využívanie štandardov otvoreného zdrojového kódu, rozvoj európskych prvkov pre spájanie siete, napr. smerovače (routery);

108. vyzýva Komisiu, aby predložila právny návrh systému EÚ týkajúceho sa presmerovania vrátane spracovania podrobných záznamov hovorov (CDR) na úrovni EÚ, ktorý bude subštruktúrou existujúceho internetu a nebude prekračovať hranice EÚ; konštatuje, že všetky údaje zo systému presmerovania a CDR by sa mali spracovávať v súlade s právnymi rámcami EÚ;

109. vyzýva členské štáty, aby v spolupráci s agentúrou ENISA, Centrom boja proti počítačovej kriminalite zriadeným v rámci Europolu, tímami CERT, vnútroštátnymi orgánmi pre ochranu údajov a oddeleniami zaoberajúcimi sa počítačovou kriminalitou rozvíjali kultúru bezpečnosti a začali vzdelávaciu a informačnú kampaň s cieľom umožniť občanom prijať informovanejšie rozhodnutia týkajúce sa otázky, ktoré osobné údaje poskytnú on-line a ako ich lepšie chrániť, a to aj prostredníctvom šifrovania a bezpečného cloud computingu, pričom sa v plnom rozsahu využije platforma pre informácie vo verejnom záujme ustanovená v smernici o univerzálnej službe;

110. vyzýva Komisiu, aby do decembra 2014 predložila legislatívne návrhy na podporu výrobcov softvéru a hardvéru, aby do svojich výrobkov zaviedli viac bezpečnostných prvkov, prvkov ochrany súkromia už v štádiu návrhu a prvkov štandardnej ochrany súkromia, a to aj zavedením odradzujúcich opatrení pre prípady nenáležitého a neprimeraného zhromažďovania hromadných osobných údajov a stanovením právnej zodpovednosti výrobcov za neopravené známe slabé miesta, chybné alebo nezabezpečené výrobky alebo používanie tajných postranných riešení umožňujúcich neoprávnený prístup k údajom a ich neoprávnené spracovanie; v tejto súvislosti vyzýva Komisiu, aby vyhodnotila možnosť vytvorenia certifikačného alebo overovacieho systému pre informačný hardvér vrátane testovacích postupov na úrovni EÚ s cieľom zaistiť integritu a bezpečnosť produktov;

Obnovenie dôvery

111. domnieva sa, že vyšetrovanie ukázalo, že okrem nutnosti legislatívnej zmeny je potrebné, aby Spojené štáty obnovili dôveru svojich partnerov, keďže ide najmä o činnosti spravodajských služieb Spojených štátov;

Streda 12. marca 2014

112. poukazuje na to, že vzniknutá kríza dôvery sa týka aj:

— ducha spolupráce v rámci EÚ, keďže niektoré činnosti vnútroštátnych spravodajských služieb môžu ohrozovať dosiahnutie cieľov Únie,

— občanov, ktorí si uvedomujú, že nielen tretie krajiny alebo nadnárodné spoločnosti, ale aj ich vlastné vlády ich môžu sledovať,

— dodržiavania základných práv, demokracie a zásad právneho štátu, ako aj dôveryhodnosti demokratických, súdnych a parlamentných záruk a dohľadu v digitálnej spoločnosti;

Medzi EÚ a Spojenými štátmi

113. pripomína dôležité historické a strategické partnerstvo medzi členskými štátmi EÚ a Spojenými štátmi založené na spoločnej viere v demokraciu, právny štát a základné práva;

114. domnieva sa, že hromadné sledovanie občanov a vedúcich politických predstaviteľov Spojenými štátmi vážne narušilo vzťahy medzi EÚ a Spojenými štátmi a negatívne ovplyvnilo dôveru k organizáciám Spojených štátov pôsobiacim v EÚ; to sa ešte prehĺbilo nedostatkom súdnych a správnych opravných prostriedkov pre občanov EÚ v rámci právnych predpisov Spojených štátov, najmä v prípadoch sledovania na spravodajské účely;

115. vzhľadom na globálne výzvy, ktorým čelia EÚ a Spojené štáty, uznáva, že treba viac posilniť transatlantické partnerstvo a že je dôležité, aby transatlantická spolupráca v oblasti boja proti terorizmu pokračovala na novom dôveryhodnom základe, ktorý sa bude opierať o skutočné spoločné rešpektovanie zásad právneho štátu a zamietanie všetkých svojvoľných postupov hromadného sledovania; preto trvá na tom, aby Spojené štáty prijali jasné opatrenia s cieľom obnoviť dôveru a znovu zdôrazniť spoločné základné hodnoty, na ktorých je partnerstvo založené;

116. je pripravený aktívne sa zapojiť do dialógu s partnermi zo Spojených štátov, aby sa v prebiehajúcej americkej verejnej diskusii a diskusii v kongrese o reforme sledovania a preskúmaní dohľadu nad spravodajskými službami zaručili práva na súkromie a iné práva občanov EÚ, obyvateľov EÚ alebo iných osôb chránených zákonmi EÚ a rovnaké práva na informácie a ochranu súkromia pred súdmi Spojených štátov vrátane prostriedkov právnej nápravy, napríklad prostredníctvom revízie zákona o ochrane súkromia a zákona o ochrane súkromia v rámci elektronickej komunikácie a prostredníctvom ratifikácie prvého opčného protokolu k Medzinárodnému paktu o občianskych a politických právach, aby tak nepokračovala súčasná diskriminácia;

117. trvá na tom, aby sa vykonali nevyhnutné reformy a aby sa Európanom poskytli účinné záruky s cieľom zabezpečiť, aby použitie sledovania a spracovania údajov na účely cudzích spravodajských služieb bolo primerané, aby sa vymedzilo prostredníctvom jednoznačne určených podmienok a aby súviselo s odôvodneným podozrením alebo pravdepodobnou príčinou teroristickej činnosti; zdôrazňuje, že na tento účel sa musí vzťahovať transparentný súdny dohľad;

118. domnieva sa, že naši americkí partneri musia vyslať jasné politické signály s cieľom preukázať, že Spojené štáty rozlišujú spojencov a protivníkov;

119. nalieha na Európsku komisiu a vládu Spojených štátov, aby sa v súvislosti s prebiehajúcimi rokovaniami o zastrešujúcej dohode medzi EÚ a Spojených štátmi o prenose údajov na účely presadzovania práva zaoberali právom občanov EÚ na informácie a na súdny nápravný prostriedok a aby do leta 2014 uzatvorili tieto rokovania v súlade so záväzkom, ktorý prijali na zasadnutí ministrov spravodlivosti a vnútra, ktoré sa konalo 18. novembra 2013;

120. nabáda Spojené štáty, aby pristúpili k Dohovoru Rady Európy o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (dohovor č. 108), keďže v roku 2001 pristúpili k Dohovoru o počítačovej kriminalite, a tak posilnili spoločný právny základ medzi transatlantickými spojencami;

121. vyzýva inštitúcie EÚ, aby preskúmali možnosti vytvorenia kódexu správania spolu so Spojenými štátmi, prostredníctvom ktorého sa zaručí, že Spojené štáty nebudú vykonávať špionážnu činnosť zameranú na inštitúcie a zariadenia EÚ;

V rámci Európskej únie

122. domnieva sa tiež, že zapojenie a činnosti členských štátov EÚ spôsobili stratu dôvery, a to medzi členskými štátmi navzájom aj medzi občanmi EÚ a orgánmi ich členských štátov; zastáva názor, že len prostredníctvom úplnej transparentnosti, pokiaľ ide o účely a prostriedky sledovania, verejnej diskusie a napokon preskúmania právnych predpisov vrátane zastavenia hromadného sledovania a posilnenia systému súdneho a parlamentného dohľadu bude možné obnoviť stratenú dôveru; pripomína ťažkosti súvisiace s rozvojom komplexných bezpečnostných politík EÚ v situácii, keď sa uskutočňujú takéto činnosti hromadného sledovania, a zdôrazňuje, že podľa zásady lojálnej spolupráce EÚ členské štáty nesmú vykonávať spravodajské činnosti na území iného členského štátu;

123. vníma si, že niektoré členské štáty vedú dvojstrannú komunikáciu s orgánmi Spojených štátov o údajnej špionážnej činnosti a že niektoré z nich uzatvorili (Spojené kráľovstvo) alebo plánujú uzatvoriť (Nemecko, Francúzsko) tzv. dohody o nevykonávaní špionáže; zdôrazňuje, že je nevyhnutné, aby tieto členské štáty v plnom rozsahu rešpektovali záujmy a legislatívny rámec EÚ ako celku; považuje takéto dvojstranné dohody za kontraproduktívne a bezpredmetné, keďže k tomuto problému treba pristupovať na európskej úrovni; žiada Radu, aby informovala Parlament o tom, ako členské štáty napredujú v otázke vzájomnej dohody EÚ o nevykonávaní špionáže;

124. domnieva sa, že tieto dohody by nemali byť v rozpore so zmluvami Únie, najmä so zásadou lojálnej spolupráce (podľa článku 4 ods. 3 ZEÚ), ani by nemali oslabovať politiky EÚ vo všeobecnosti a konkrétne vnútorný trh, spravodlivú hospodársku súťaž a hospodársky, priemyselný a sociálny rozvoj; je rozhodnutý preskúmať zlučiteľnosť takýchto dohôd s európskym právom a vyhradzuje si právo na začatie postupov podľa zmluvy v prípade, keď sa preukáže, že tieto dohody sú v rozpore so zásadou súdržnosti Únie alebo s jej základnými zásadami, na ktorých je založená;

125. vyzýva členské štáty, aby vyvinuli maximálne úsilie o zabezpečenie lepšej spolupráce s cieľom poskytnúť záruky proti špionáži, a to v spolupráci s príslušnými orgánmi a agentúrami EÚ, v záujme ochrany občanov a inštitúcií EÚ, európskych spoločností, priemyslu EÚ, infraštruktúry a sietí IT a európskeho výskumu;, domnieva sa, že aktívne zapojenie zainteresovaných strán EÚ je základnou podmienkou účinnej výmeny informácií; poukazuje na to, že bezpečnostné hrozby majú medzinárodnejší rozmer, sú rozptýlenejšie a komplexnejšie, čo si vyžaduje posilnenie európskej spolupráce; je presvedčený, že tento vývoj by sa mal lepšie premietnuť do zmlúv, a preto žiada revíziu zmlúv s cieľom posilniť koncepciu lojálnej spolupráce medzi členskými štátmi a Úniou, pokiaľ ide o cieľ zrealizovať priestor bezpečnosti a zabrániť vzájomnej špionáži medzi členskými štátmi v rámci Únie;

126. považuje za absolútnu nevyhnutnosť komunikačné štruktúry, ktoré nie je možné odpočúvať (e-mail, telekomunikácie vrátane pevných liniek a mobilných telefónov), a zasadacie miestnosti vo všetkých príslušných inštitúciách EÚ a delegáciách EÚ, ktoré nie je možné odpočúvať; preto požaduje vytvorenie šifrovaného vnútorného e-mailového systému EÚ;

127. vyzýva Radu a Komisiu, aby bezodkladne odsúhlasili návrh nariadenia Európskeho parlamentu o podrobných ustanoveniach o výkone vyšetrovacích právomocí Európskeho parlamentu, ktorým sa zrušuje rozhodnutie Európskeho parlamentu, Rady a Komisie 95/167/ES, Euratom, ESUO, predložený na základe článku 226 ZFEÚ, ktorý Európsky parlament prijal 23. mája 2012; žiada, aby sa zrevidovala zmluva s cieľom rozšíriť tieto vyšetrovacie právomoci bez obmedzení či výnimiek na všetky oblasti pôsobnosti alebo činnosti Únie a začleniť možnosť vypočúvania pod prísahou;

Medzinárodne

128. vyzýva Komisiu, aby najneskôr do januára 2015 predložila stratégiu EÚ pre demokratickú správu internetu;

Streda 12. marca 2014

129. vyzýva členské štáty, aby sa riadili výzvou 35. Medzinárodnej konferencie splnomocnencov pre ochranu údajov a súkromia, aby „presadzovali prijatie dodatočného protokolu k článku 17 Medzinárodného paktu o občianskych a politických právach, ktoré by malo byť založené na normách, ktoré vytvorila a schválila medzinárodná konferencia, a ustanoveniach všeobecnej poznámky Výboru pre ľudské práva č. 16 k paktu s cieľom vytvoriť globálne uplatniteľné normy na ochranu údajov a ochranu súkromia v súlade so zásadou právneho štátu“; žiada členské štáty, aby pritom požadovali vytvorenie medzinárodnej agentúry OSN zodpovednej najmä za monitorovanie vzniku nástrojov dohľadu a reguláciu a vyšetrovanie ich používania; žiada vysokú predstaviteľku/podpredsedníčku Komisie a Európsku službu pre vonkajšiu činnosť, aby zaujali aktívny postoj;

130. vyzýva členské štáty, aby v rámci OSN vytvorili súdržnú a pevnú stratégiu, ktorou podporia najmä uznesenie s názvom Právo na súkromie v digitálnom veku, ktoré vzniklo na podnet Brazílie a Nemecka a ktoré 27. novembra 2013 prijal tretí výbor Valného zhromaždenia OSN (Výbor pre ľudské práva), aby prijali ďalšie kroky na obranu základného práva na súkromie a na ochranu údajov na medzinárodnej úrovni a aby súčasne zabránili možnosti štátnej kontroly, cenzúry alebo roztrieštenosti internetu, pričom súčasťou tohto úsilia by mala byť aj iniciatíva za medzinárodnú zmluvu, ktorou sa zakážu činnosti hromadného sledovania, a za zriadenie agentúry na dohľad nad vykonávaním tejto zmluvy;

Prioritný plán: Európsky habeas corpus v digitálnej oblasti – ochrana základných práv v digitálnom veku

131. je rozhodnutý predložiť občanom, inštitúciám a členským štátom EÚ uvedené odporúčania ako prioritný plán na nasledujúce legislatívne obdobie; vyzýva Komisiu a ďalšie orgány a inštitúcie, úrady a agentúry EÚ uvedené v tomto uznesení, aby v súlade s článkom 265 ZFEÚ konali na základe odporúčaní a výziev obsiahnutých v tomto uznesení;

132. je rozhodnutý začať vykonávať plán Európsky habeas corpus v digitálnej oblasti – ochrana základných práv v digitálnom veku, ktorý obsahuje týchto osem opatrení, na ktorých plnenie bude dohliadať:

— opatrenie 1: prijať súbor opatrení v oblasti ochrany údajov v roku 2014,

— opatrenie 2: uzavrieť zastrešujúcu dohodu medzi EÚ a Spojenými štátmi, ktorá zaručuje základné právo občanov na súkromie a ochranu údajov a zabezpečuje riadne mechanizmy uplatňovania nárokov na nápravu pre občanov EÚ, a to aj v prípade prenosu údajov z EÚ do Spojených štátov na účely presadzovania práva,

— opatrenie 3: pozastaviť „bezpečný prístav“, kým sa nevykoná celkové preskúmanie a neodstránia sa súčasné medzery, pričom treba zabezpečiť, aby sa prenos osobných údajov z Únie do Spojených štátov na komerčné účely uskutočnil len v súlade s najprísnejšími normami EÚ,

— opatrenie 4: pozastaviť dohodu o TFTP, kým sa: (i) neuzatvoria rokovania o zastrešujúcej dohode (ii) a neukončí sa dôkladné vyšetrovanie založené na analýze EÚ a riadne sa nevyriešia všetky otázky, ktoré Parlament uviedol vo svojom uznesení z 23. októbra 2013;

— opatrenie 5: vyhodnotiť každú dohodu, mechanizmus alebo výmenu s tretími krajinami, ktorej súčasťou sú osobné údaje, s cieľom zaistiť, že práva na súkromie a na ochranu osobných údajov nie sú porušené vplyvom činností dohľadu, a prijať následné potrebné opatrenia,

— opatrenie 6: chrániť zásadu právneho štátu a základné práva občanov EÚ (a to aj pred ohrozením slobody tlače), právo verejnosti na nestranné informácie a služobné tajomstvo (vrátane vzťahu medzi právnym zástupcom a klientom) a tiež zabezpečiť zvýšenú ochranu informátorov,

— opatrenie 7: vytvoriť európsku stratégiu pre väčšiu nezávislosť v oblasti informačných technológií (tzv. novú digitálnu dohodu vrátane vyčlenenia primeraných zdrojov na vnútroštátnej aj európskej úrovni) s cieľom oživiť odvetvie informačných technológií a umožniť európskym spoločnostiam, aby využili konkurenčnú výhodu, ktorú EÚ ponúka v oblasti súkromia;

— opatrenie 8: vytvoriť z EÚ referenčný subjekt pre demokratickú a neutrálnu správu internetu;

133. vyzýva inštitúcie EÚ a členské štáty, aby presadzovali plán Európsky habeas corpus v digitálnej oblasti – ochrana základných práv v digitálnom veku; zaväzuje sa vystupovať ako obhajca práv občanov EÚ, pričom bude dodržiavať tento harmonogram na monitorovanie plnenia:

— apríl 2014 – marec 2015: monitorovacia skupina založená na vyšetrovacej skupine výboru LIBE, zodpovedná za monitorovanie všetkých nových odhalení týkajúcich sa vyšetrovacieho mandátu a za kontrolu vykonávania tohto uznesenia,

— od júla 2014: stály mechanizmus dohľadu nad prenosom údajov a súdnymi nápravnými prostriedkami v príslušnom výbore,

— jar 2014: formálna výzva určená Európskej rade, aby začlenila plán Európsky habeas corpus v digitálnej oblasti – ochrana základných práv v digitálnom veku do usmernení, ktoré sa prijmú podľa článku 68 ZFEÚ,

— jeseň 2014: záväzok, aby sa plán Európsky habeas corpus v digitálnej oblasti – ochrana základných práv v digitálnom veku a príslušné odporúčania používali ako hlavné kritériá pri schvaľovaní budúcej Komisie,

— 2014: konferencia európskych expertov na vysokej úrovni z rozličných oblastí súvisiacich s bezpečnosťou informačných technológií (vrátane matematiky, šifrovania a technológií na zvýšenie ochrany súkromia) s cieľom pomôcť posilniť stratégiu EÚ v oblasti informačných technológií v nasledujúcom legislatívnom období;

— 2014-2015: skupina pre dôveru/údaje/práva občanov, ktorá sa bude pravidelne schádzať medzi Európskym parlamentom a Kongresom Spojených štátov, ako aj s ostatnými zapojenými parlamentmi tretích krajín vrátane parlamentu Brazílie,

— 2014-2015: konferencia s orgánmi európskych národných parlamentov vykonávajúcimi dohľad nad spravodajskými službami,

o

o o

134. poveruje svojho predsedu, aby postúpil toto uznesenie Európskej rade, Rade, Komisii, parlamentom a vládam členských štátov, vnútroštátnym orgánom na ochranu údajov, EDPS, eu-LISA, ENISA, Agentúre pre základné práva, pracovnej skupine zriadenej podľa článku 29, Rade Európy, Kongresu Spojených štátov amerických, vláde Spojených štátov amerických, prezidentovi, vláde a parlamentu Brazílskej federatívnej republiky a generálnemu tajomníkovi OSN;

135. poveruje Výbor pre občianske slobody, spravodlivosť a vnútorné veci, aby do jedného roka po prijatí tohto uznesenia informoval o tejto záležitosti Parlament na plenárnom zasadaní; považuje za nevyhnutné posúdiť, v akom rozsahu boli dodržiavané odporúčania prijaté Parlamentom, a analyzovať prípady, v ktorých sa nedodržiavali.