Sreda, 12. marec 2014

P7_TA(2014)0230

Program nadzora Agencije ZDA za nacionalno varnost, organi nadzora v različnih državah članicah ter učinek na temeljne pravice državljanov EU

Resolucija Evropskega parlamenta z dne 12. marca 2014 o programu nadzora Agencije ZDA za nacionalno varnost, organih nadzora v različnih državah članicah ter njihovem učinku na temeljne pravice državljanov EU in čezatlantsko sodelovanje na področju pravosodja in notranjih zadev (2013/2188(INI))

(2017/C 378/14)

Evropski parlament,

— ob upoštevanju Pogodbe o Evropski uniji in zlasti členov 2, 3, 4, 5, 6, 7, 10, 11 in 21 Pogodbe,

— ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti členov 15, 16 in 218 ter naslova V Pogodbe,

— ob upoštevanju Protokola št. 36 o prehodnih določbah in njegovega člena 10 ter Izjave 50, ki se nanaša na zadevni protokol,

— ob upoštevanju Listine Evropske unije o temeljnih pravicah, zlasti njenih členov 1, 3, 6, 7, 8, 10, 11, 20, 21, 42, 47, 48 in 52,

— ob upoštevanju Evropske konvencije o človekovih pravicah, zlasti njenih členov 6, 8, 9, 10 in 13 ter protokolov,

— ob upoštevanju Splošne deklaracije o človekovih pravicah, zlasti njenih členov 7, 8, 10,11,12 in 14 ([1]),

— ob upoštevanju Mednarodnega pakta o državljanskih in političnih pravicah, zlasti njegovih členov 14, 17, 18 in 19,

— ob upoštevanju Konvencije Sveta Evrope o varstvu podatkov (ETS št. 108) in dodatnega protokola z dne 8. novembra 2001 h Konvenciji o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov v zvezi z nadzornimi organi in prenosom podatkov čez meje (ETS št. 181),

— ob upoštevanju Dunajske konvencije o diplomatskih odnosih, zlasti njenih členov 24, 27 in 40,

— ob upoštevanju Konvencije Sveta Evrope o kibernetski kriminaliteti (ETS št. 185),

— ob upoštevanju poročila posebnega poročevalca Združenih narodov za spodbujanje in varstvo človekovih pravic in temeljnih svoboščin v boju proti terorizmu, predloženega 17. maja 2010 ([2]),

— ob upoštevanju sporočila Komisije z naslovom Internetna politika in upravljanje interneta – Vloga Evrope pri oblikovanju prihodnosti upravljanja interneta (COM(2014)0072),

— ob upoštevanju poročila posebnega poročevalca Združenih narodov za spodbujanje in varstvo pravice do svobode mnenja in izražanja, predloženega 17. aprila 2013 ([3]),

— ob upoštevanju smernic o človekovih pravicah in boju proti terorizmu, ki jih je 11. julija 2002 sprejel Odbor ministrov Sveta Evrope,

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

— ob upoštevanju bruseljske deklaracije s 6. konference parlamentarnih odborov za nadzor obveščevalnih in varnostnih služb držav članic Evropske unije z dne 1. oktobra 2010,

— ob upoštevanju resolucije parlamentarne skupščine Sveta Evrope št. 1954 (2013) o nacionalni varnosti in dostopu do informacij,

— ob upoštevanju poročila o demokratičnem nadzoru varnostnih služb, ki ga je Beneška komisija sprejela 11. junija 2007 ([1]) in katerega posodobitev, napovedano za pomlad 2014, z zanimanjem pričakuje,

— ob upoštevanju pričevanj predstavnikov odborov za nadzor nad obveščevalnimi dejavnostmi Belgije, Nizozemske, Danske in Norveške,

— ob upoštevanju zadev na francoskem ([2]), poljskem in britanskem ([3]) sodišču ter na Evropskem sodišču za človekove pravice ([4]), ki se nanašajo na sisteme za množični nadzor,

— ob upoštevanju konvencije Sveta na podlagi člena 34 Pogodbe o Evropski uniji o medsebojni pomoči v kazenskih zadevah med državami članicami Evropske unije ([5]), zlasti njenega naslova III,

— ob upoštevanju Odločbe Komisije 2000/520/ES z dne 26. julija 2000 o primernosti zaščite, ki jo zagotavljajo načela zasebnosti varnega pristana in s tem povezana najpogosteje zastavljena vprašanja, ki jih je izdalo Ministrstvo za trgovino ZDA,

— ob upoštevanju ocenjevalnih poročil Komisije o izvajanju načel zasebnosti varnega pristana z dne 13. februarja 2002 (SEC(2002)0196) in z dne 20. oktobra 2004 (SEC(2004)1323),

— ob upoštevanju sporočila Komisije z dne 27. novembra 2013 o delovanju varnega pristana z vidika državljanov EU in družb, ustanovljenih v EU (COM(2013)0847), in sporočila Komisije z dne 27. novembra 2013 o obnovitvi zaupanja v pretok podatkov med EU in ZDA (COM(2013)0846),

— ob upoštevanju svoje resolucije z dne 5. julija 2000 o osnutku odločbe Komisije o ustreznosti zaščite, ki jo zagotavljajo načela zasebnosti varnega pristana in s tem povezana najpogosteje zastavljena vprašanja, ki jih je izdalo Ministrstvo za trgovino ZDA ([6]), v katerem je izrazil stališče, da ni mogoče potrditi ustreznosti sistema, in mnenj delovne skupine iz člena 29, zlasti mnenja 4/2000 z dne 16. maja 2000 ([7]),

— ob upoštevanju sporazumov med Združenimi državami Amerika in Evropsko unijo o uporabi in prenosu podatkov iz evidence podatkov o potnikih (PNR) iz leta 2004, 2007 ([8]) in 2012 ([9]),

— ob upoštevanju skupnega pregleda izvajanja Sporazuma med EU in ZDA o obdelavi in prenosu podatkov iz evidence imen letalskih potnikov Ministrstvu Združenih držav za domovinsko varnost ([10]), ki je priložen poročilu Komisije Evropskemu parlamentu in Svetu o skupnem pregledu (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 in La Ligue française pour la défense des droits de l'Homme et du Citoyen proti X; sodišče prve stopnje v Parizu.
([3]) Zadeve organizacije Privacy International in interesne skupine Liberty na preiskovalnem sodišču.
([4]) Skupna tožba v skladu s členom 34 interesnih skupin Big Brother Watch in Open Rights Group, združenja pisateljev English PEN in aktivistke dr. Constanze Kurz (tožniki) proti Združenemu kraljestvu (toženec).
([5]) UL C 197, 12.7.2000, str. 1.
([6]) UL C 121, 24.4.2001, str. 152.
([7]) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp32en.pdf
([8]) UL L 204, 4.8.2007, str. 18.
([9]) UL L 215, 11.8.2012, str. 5.
([10]) SEC(2013)0630, 27.11.2013.

Sreda, 12. marec 2014

— ob upoštevanju mnenja generalnega pravobranilca Cruza Villalóna, da je Direktiva 2006/24/ES o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, kot celota neskladna s členom 52(1) Listine Evropske unije o temeljnih pravicah in da je člen 6 neskladen s členom 7 in členom 52(1) Listine ([1]),

— ob upoštevanju Sklepa Sveta 2010/412/EU z dne 13. julija 2010 o sklenitvi Sporazuma med Evropsko unijo in Združenimi državami Amerike o obdelavi in posredovanju podatkov o sporočilih glede finančnih plačil iz Evropske unije Združenim državam Amerike za namene programa za sledenje financiranja terorističnih dejavnosti ([2]) in spremnih izjav Komisije in Sveta,

— ob upoštevanju Sporazuma o medsebojni pravni pomoči med Evropsko unijo in Združenimi državami Amerike ([3]),

— ob upoštevanju tekočih pogajanj o okvirnem sporazumu med EU in ZDA o varstvu osebnih podatkov ob njihovem prenosu ali obdelavi za potrebe preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj, vključno s terorizmom, v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah („krovnem sporazumu“),

— ob upoštevanju Uredbe Sveta (ES) št. 2271/96 z dne 22. novembra 1996 o zaščiti pred učinki ekstrateritorialne uporabe zakonodaje, ki jo sprejme tretja država, in dejanji, ki na tej zakonodaji temeljijo ali iz nje izhajajo ([4]),

— ob upoštevanju izjave predsednika Zvezne republike Brazilije ob pričetku 68. zasedanja Generalne skupščine Združenih narodov z dne 24. septembra 2013 in dela parlamentarnega odbora za preiskovanje vohunjenja, ki ga je ustanovil brazilski zvezni senat,

— ob upoštevanju zakona o domovinski varnosti ZDA, ki ga je predsednik George W. Bush podpisal 26. oktobra 2001,

— ob upoštevanju zakona o nadzoru tujih obveščevalnih podatkov (FISA) iz leta 1978 in dopolnitev tega zakona iz leta 2008,

— ob upoštevanju izvedbene uredbe št. 12333 predsednika ZDA iz leta 1981, spremenjene leta 2008,

— ob upoštevanju predsedniške politične direktive o obveščevalnih dejavnostih SIGINT, ki jo je ameriški predsednik Barack Obama izdal dne 17. januarja 2014,

— ob upoštevanju zakonodajnih predlogov, ki jih trenutno obravnava kongres ZDA, vključno z osnutkom akta o svobodi, osnutkom akta o kontroli obveščevalnih dejavnosti in reformi nadzora ter drugimi,

— ob upoštevanju pregledov, ki so jih izvedli odbor za nadzor zasebnosti in državljanskih svoboščin, nacionalni varnostni svet ZDA in predsednikova skupina za pregled nad obveščevalno in komunikacijsko tehnologijo, zlasti poročila slednje z dne 12. decembra 2013 z naslovom „Liberty and Security in a Changing World“ (Svoboda in varnost v spreminjajočem se svetu),

— ob upoštevanju sodbe okrožnega sodišča Združenih držav za Zvezno okrožje Kolumbije v zadevi Klayman et al. proti Obama et al., civilna tožba št. 13-0851 z dne 16. decembra 2013, in sodbe okrožnega sodišča Združenih držav za južno okrožje New Yorka v zadevi ACLU et al. proti James R. Clapper et al., civilna tožba št. 13-3994 z dne 11. junija 2013,

— ob upoštevanju poročila o ugotovitvah evropskih sopredsednikov ad hoc delovne skupine EU–ZDA o varstvu podatkov z dne 27. novembra 2013 ([5]),

---

([1]) Mnenje generalnega pravobranilca Cruza Villalóna z dne 12. decembra 2013 v zadevi C-293/12.
([2]) UL L 195, 27.7.2010, str. 3.
([3]) UL L 181, 19.7.2003, str. 34.
([4]) UL L 309, 29.11.1996, str. 1.
([5]) Dokument Sveta 16987/2013.

— ob upoštevanju svojih resolucij z dne 5. septembra 2001 ([1]) in 7. novembra 2002 ([2]) o obstoju globalnega sistema za prestrezanje zasebnih in komercialnih sporočil (sistem satelitskega prestrezanja ECHELON),

— ob upoštevanju svoje resolucije z dne 21. maja 2013 o Listini EU: določitev standardov za svobodo medijev v EU ([3]),

— ob upoštevanju svoje resolucije z dne 4. julija 2013 o programu nadzorovanja Agencije ZDA za nacionalno varnost (NSA), organih nadzorovanja v nekaterih državah članicah in vplivu na zasebnost državljanov EU ([4]), v kateri je svojemu Odboru za državljanske svoboščine, pravosodje in notranje zadeve naročil, da temeljito razišče zadevo,

— ob upoštevanju delovnega dokumenta 1 o programih nadzora ZDA in EU ter njihovih učinkih na temeljne pravice državljanov EU,

— ob upoštevanju delovnega dokumenta 3 o odnosu med praksami nadzora v EU in ZDA ter določbami EU o varstvu podatkov,

— ob upoštevanju delovnega dokumenta 4 o dejavnostih nadzora ZDA v zvezi s podatki iz EU in možnih pravnih posledicah za čezatlantske sporazume in sodelovanje,

— ob upoštevanju delovnega dokumenta 5 o demokratičnem nadzoru nad obveščevalnimi službami držav članic in obveščevalnimi organi EU,

— ob upoštevanju delovnega dokumenta Odbora za zunanje zadeve o zunanjepolitičnih vidikih preiskave elektronskega množičnega nadzora državljanov EU;

— ob upoštevanju svoje resolucije z dne 23. oktobra 2013 o organiziranem kriminalu, korupciji in pranju denarja: priporočila za ukrepe in pobude, ki bi jih bilo treba sprejeti ([5]),

— ob upoštevanju svoje resolucije z dne 23. oktobra 2013 o prekinitvi izvajanja sporazuma SWIFT zaradi nadzora Agencije ZDA za nacionalno varnost ([6]),

— ob upoštevanju svoje resolucije z dne 10. decembra 2013 o sprostitvi potenciala računalništva v oblaku v Evropi ([7]),

— ob upoštevanju medinstitucionalnega sporazuma med Evropskim parlamentom in Svetom o pošiljanju tajnih podatkov Sveta o zadevah, ki niso s področja skupne zunanje in varnostne politike, Evropskemu parlamentu in njihovi obdelavi s strani Evropskega parlamenta ([8]),

— ob upoštevanju Priloge VIII Poslovnika,

— ob upoštevanju člena 48 Poslovnika,

— ob upoštevanju poročila Odbora za državljanske svoboščine, pravosodje in notranje zadeve (A7-0139/2014),

Vpliv množičnega nadzora

A. ker sta varstvo podatkov in zasebnost temeljni pravici; ker je varnostne ukrepe, vključno s protiteroristističnimi ukrepi, zato treba uresničevati s pomočjo pravne države, zanje pa morajo veljati obveznosti, ki izhajajo iz temeljnih pravic, vključno s tistimi v zvezi z zasebnostjo in varstvom podatkov;

([1]) UL C 72 E, 21.3.2002, str. 221.
([2]) UL C 16 E, 22.1.2004, str. 88.
([3]) Sprejeta besedila, P7_TA(2013)0203.
([4]) Sprejeta besedila, P7_TA(2013)0322.
([5]) Sprejeta besedila, P7_TA(2013)0444.
([6]) Sprejeta besedila, P7_TA(2013)0449.
([7]) Sprejeta besedila, P7_TA(2013)0535.
([8]) UL C 353 E, 3.12.2013, str. 156.

B. ker morajo biti pretok informacij in podatki, ki danes vladajo vsakdanjemu življenju in so del integritete vsake osebe, enako varni pred posegi kot zasebni domovi;

C. ker vezi med Evropo in Združenimi državami Amerike temeljijo na duhu in načelih demokracije, pravne države, svobode, pravičnosti in solidarnosti;

D. ker sodelovanje med Združenimi državami Amerike in Evropsko unijo ter njenimi državami članicami v boju proti terorizmu ostaja ključno za varnost obeh partneric;

E. ker sta vzajemno zaupanje in razumevanje ključna dejavnika v čezatlantskem dialogu in partnerstvu;

F. ker je po 11. septembru 2001 boj proti terorizmu postal ena izmed najpomembnejših prednostnih nalog večine vlad; ker so razkritja na podlagi dokumentov, ki jih je objavil nekdanji pogodbeni sodelavec agencije NSA Edward Snowden, politične voditelje prisilila, da se soočijo z izzivi spremljanja in nadzorovanja obveščevalnih agencij pri dejavnostih nadzora in oceno učinka njihovih dejavnosti na temeljne pravice in pravno državo v demokratični družbi;

G. ker so razkritja od junija 2013 v EU povzročila številne pomisleke glede:

— obsega nadzornih sistemov, ki so bili razkriti v ZDA in državah članicah EU;

— kršitev pravnih standardov, temeljnih pravic in standardov za varstvo podatkov EU;

— stopnje zaupanja med čezatlantskima partnericama EU in ZDA;

— stopnje sodelovanja in udeležbe določenih držav članic EU v ameriških programih nadzora ali enakovrednih programih na nacionalni ravni, kot so razkrili mediji;

— pomanjkanja nadzora in učinkovitega spremljanja obveščevalnih skupnosti s strani političnih organov ZDA in določenih držav članic EU;

— možnosti, da se te dejavnosti množičnega nadzora uporabljajo v druge namene razen za nacionalno varnost in dosledno za boj proti terorizmu, na primer za gospodarsko in industrijsko vohunjenje ali oblikovanje profilov iz političnih razlogov;

— spodkopavanja svobode tiska, komunikacij s predstavniki poklicev, ki morajo zagotavljati zaupnost, kot so odvetniki in zdravniki;

— vlog in stopnje vpletenosti obveščevalnih služb oziroma zasebnih podjetij za informacijsko tehnologijo in telefonijo;

— vedno bolj zabrisanih mej med dejavnostmi kazenskega pregona in obveščevalnimi dejavnostmi, kar vodi k obravnavanju slehernega državljana kot osumljenca in nadzoru nad njim;

— groženj zasebnosti v digitalni dobi in vpliva množičnega nadzora na državljane in družbe;

H. ker razsežnost razkritega vohunjenja, ki je brez primere, zahteva, da organi ZDA, evropske institucije ter vlade, nacionalni parlamenti in sodni organi držav članic problematiko v celoti raziščejo;

I. ker so organi ZDA nekatere razkrite informacije zanikali, vendar pa velike večine informacij niso izpodbijali; ker se je v ZDA in v določenih državah članicah EU razvila obširna javna razprava; ker vlade in parlamenti EU prepogosto ne izrazijo pripomb in ne sprožijo ustreznih preiskav;

J. ker je predsednik Obama pred kratkim napovedal reformo agencije NSA in njenih programov nadzora;

K. ker je Evropski parlament v primerjavi z ukrepi institucij EU in določenih držav članic EU zelo resno vzel svojo obveznost, da pojasni razkritja o vsesplošnih praksah množičnega nadzora državljanov EU, in je s svojo resolucijo z dne 4. julija 2013 o programu nadzorovanja Agencije ZDA za nacionalno varnost (NSA), organih nadzora v nekaterih državah članicah in vplivu na zasebnost državljanov EU naročil svojemu Odboru za državljanske svoboščine, pravosodje in notranje zadeve, naj temeljito razišče zadevo;

L. ker je dolžnost evropskih institucij zagotavljati, da se pravo EU v celoti izvaja v korist evropskih državljanov in da podcenjevalno sprejemanje ekstrateritorialnih učinkov standardov ali ukrepov tretjih držav ne spodkopava pravne veljave Pogodb EU;

Razvoj dogodkov v ZDA v zvezi z reformo obveščevalne dejavnosti

M. ker je okrajno sodišče Zveznega okrožja Kolumbija v svoji odločitvi z dne 16. decembra 2013 razsodilo, da neprečiščena zbirka metapodatkov agencije NSA predstavlja kršitev četrtega amandmaja k ameriški ustavi ([1]); ker je okrožno sodišče za južno okrožje New Yorka v svoji odločitvi z dne 27. decembra 2013 kljub temu razsodilo, da je to zbiranje zakonito;

N. ker odločba okrožnega sodišča za vzhodno okrožje Michigana pravi, da četrti amandma zahteva utemeljenost pri vseh preiskavah, predhodni sodni nalog za vsako utemeljeno preiskavo, pri čemer mora sodni nalog temeljiti na predhodno ugotovljenem utemeljenem razlogu, poleg tega pa se o osebah, krajih in stvareh odloča posamično in med uradniki pregona izvršilne veje in državljani mora posredovati neodvisen sodnik ([2]);

O. ker je predsednikova delovna skupina za pregled obveščevalne in komunikacijske tehnologije (Review Group on Intelligence and Communication Technology) v svojem poročilu z dne 12. decembra 2013 predsedniku ZDA predlagala 46 priporočil; ker priporočila poudarjajo potrebo po sočasni zaščiti tako nacionalne varnosti kot zasebnosti posameznika in državljanskih svoboščin; ker delovna skupina v zvezi s tem poziva vlado ZDA, naj preneha z zbiranjem neprečiščenih telefonskih zapisov državljanov in rezidentov ZDA v skladu s členom 215 zakona o domovinski varnosti ZDA, kakor hitro je to izvedljivo, temeljito pregleda agencijo NSA in pravni okvir ameriške obveščevalne dejavnosti, da se zagotovi spoštovanje pravice do zasebnosti, naj si neha prizadevati za kvarjenje in povečevanje ranljivosti komercialne programske opreme (stranska vrata in zlonamerna programska oprema), naj poveča uporabo šifriranja, zlasti pri podatkih v tranzitu, in naj ne spodkopava prizadevanj za oblikovanje standardov šifriranja, naj uvede zagovornika javnega interesa (Public Interest Advocate), ki bo zastopal zasebnost in državljanske svoboščine pred sodiščem za nadzor tujih obveščevalnih podatkov (FISC), naj odboru za nadzor zasebnosti in državljanskih pravic (Privacy and Civil Liberties Oversight Board) podeli pooblastila za spremljanje dejavnosti obveščevalne skupnosti za namene zbiranja tujih obveščevalnih podatkov – in ne samo za protiteroristične namene – ter za sprejemanje pritožb prijaviteljev nepravilnosti, naj za pridobivanje elektronskih komunikacij uporablja pogodbe o medsebojni pravni pomoči ter naj nadzora ne uporablja za krajo poslovnih skrivnosti;

P. ker v skladu z odprtim memorandumom, ki so ga predsedniku Obami predložili nekdanji vodilni uslužbenci agencije NSA in skupina veteranov *Veteran Intelligence Professionals for Sanity – VIPS* dne 7. januarja 2014 ([3]), množično zbiranje podatkov ne krepi zmožnosti preprečevanja terorističnih napadov v prihodnosti; ker avtorji poudarjajo, da množično nadzorovanje s strani agencije NSA ni preprečilo nobenega napada in da so bile potrošene milijarde dolarjev za programe, ki so manj učinkoviti in veliko bolj vdirajo v zasebnost državljanov kot lastna tehnologija, imenovana Thinthread, ki je bila razvita leta 2001;

Q. ker je v priporočilih predsedniku ZDA glede obveščevalnih dejavnosti v zvezi z osebami, ki niso državljani ali rezidenti ZDA, v skladu s členom 702 zakona FISA priznano temeljno načelo spoštovanja zasebnosti in človekovega dostojanstva, zapisanega v členu 12 Splošne deklaracije o človekovih pravicah in členu 17 Mednarodnega pakta o državljanskih in političnih pravicah; ker se v njih ne priporoča, da bi osebam, ki niso državljani ali rezidenti ZDA, dodelili enake pravice in zaščito kot državljanom in rezidentom ZDA;

([1]) Klayman in drugi proti Obami in drugim, civilna tožba št. 13-0851, 16. december 2013.
([2]) ACLU proti NSA št. 06-CV-10204, 17. avgust 2006.
([3]) http://consortiumnews.com/2014/01/07/nsa-insiders-reveal-what-went-wrong.

R. ker je predsednik ZDA Barack Obama v svoji predsedniški politični direktivi o obveščevalnih dejavnostih SIGINT z dne 17. januarja 2014 in s tem povezanem govoru izjavil, da je množični elektronski nadzor potreben za zaščito nacionalne varnosti Združenih držav Amerike, ameriških državljanov in državljanov zaveznic in partneric ZDA ter za uveljavljanje ameriških zunanjepolitičnih interesov; ker ta politična direktiva vsebuje določena načela glede zbiranja, uporabe in izmenjave podatkov SIGINT in razširja določene zaščitne ukrepe na osebe, ki niso državljani ZDA, in jim s tem delno zagotavlja enakovredno obravnavo, kot jo uživajo državljani ZDA, vključno z zaščitnimi ukrepi za osebne podatke vseh posameznikov, ne glede na njihovo državljanstvo ali prebivališče; ker pa predsednik Obama ni napovedal nobenih konkretnih predlogov, zlasti ne glede prepovedi dejavnosti množičnega nadzora in uvedbe upravnega in sodnega varstva za osebe, ki niso državljani ali rezidenti ZDA;

Pravni okvir

Temeljne pravice

S. ker poročilo o ugotovitvah evropskih sopredsednikov ad hoc delovne skupine EU-ZDA o varstvu podatkov navaja pregled pravnega položaja v ZDA, vendar ni ugotovilo dejstev o programih nadzora ZDA; ker ni na voljo nobenih informacij o tako imenovani delovni skupini „drugega tira“, v kateri države članice dvostransko razpravljajo z organi ZDA o zadevah v zvezi z nacionalno varnostjo;

T. ker so temeljne pravice, zlasti svoboda izražanja, tiska, misli, vesti, vere in združevanja, zasebno življenje, varstvo podatkov pa tudi pravica do učinkovitega pravnega sredstva, domneva nedolžnosti in pravica do poštenega sojenja in nediskriminacije, ki so zapisane v Listini Evropske unije o temeljnih pravicah in Evropski konvenciji o človekovih pravicah, temelji demokracije; ker je množični nadzor ljudi nezdružljiv s temi temelji;

U. ker zakonodaja v vseh državah članicah varuje pred razkrivanjem podatkov, sporočenih v zaupnem odnosu med odvetnikom in stranko, to načelo pa priznava tudi Sodišče Evropske unije ([1]);

V. ker je Evropski parlament v svoji resoluciji z dne23. oktobra 2013 o organiziranem kriminalu, korupciji in pranju denarja Komisijo pozval, naj pripravi zakonodajni predlog o ustanovitvi učinkovitega in celovitega evropskega programa za zaščito prijaviteljev, da se zaščitijo finančni interesi EU, in preuči vprašanje, ali naj prihodnja zakonodaja vključuje tudi druga področja, ki so v pristojnosti Unije;

Pristojnosti Unije na področju varnosti

W. ker si EU v skladu s členom 67(3) PDEU „prizadeva zagotoviti visoko raven varnosti“; ker določbe Pogodb (zlasti člen 4(2) PEU in člena 72 in 73 PDEU) posredno dokazujejo, da ima EU določene pristojnosti v zadevah v zvezi s kolektivno varnostjo Unije; ker ima EU pristojnosti v zadevah notranje varnosti (člen 4(j) PDEU), ki jih izvršuje z odločanjem o številnih zakonodajnih instrumentih in sklepanjem mednarodnih sporazumov (PNR, TFTP), namenjenih boju proti hudim kaznivim dejanjem in terorizmu, ter z vzpostavitvijo strategije notranje varnosti in agencij, ki delujejo na tem področju;

X. ker Pogodba o delovanju Evropske unije določa, da je „[d]ržavam članicam […] prepuščeno, da med seboj in v okviru lastne odgovornosti organizirajo takšne oblike sodelovanja in usklajevanja med pristojnimi službami svojih uprav, odgovornimi za zagotavljanje nacionalne varnosti, kakor se jim zdijo ustrezne“ (člen 73 PDEU);

Y. ker člen 276 PDEU določa, da „[p]ri izvajanju pristojnosti glede določb poglavij 4 in 5 poglavja V tretjega dela glede območja svobode, varnosti in pravice Sodišče Evropske unije ni pristojno za preverjanje veljavnosti ali sorazmernosti ukrepov policije ali drugih organov kazenskega pregona države članice ali za odločanje o izpolnjevanju obveznosti držav članic glede vzdrževanja javnega reda in varovanja notranje varnosti“;

([1]) Sodba z dne 18. maja 1982 v zadevi C-155/79, AM&S Europe Limited proti Komisiji Evropskih skupnosti.

Z. ker se pojmi „nacionalna varnost“, „notranja varnost“ „notranja varnost EU“ in „mednarodna varnost“ med seboj prekrivajo; ker Dunajska konvencija o pravu mednarodnih pogodb, načelo lojalnega sodelovanja med državami članicami in načelo ozkega tolmačenja vseh izjem v skladu s pravom o človekovih pravicah usmerjajo k omejevalni razlagi pojma „nacionalna varnost“ in zahtevajo, da se države članice vzdržijo posegov v pristojnosti EU;

AA. ker ustanovne pogodbe Evropski komisiji dodeljujejo vlogo „varuhinje Pogodb“, zaradi česar je zakonita vloga Evropske komisije preiskovanje vseh morebitnih kršitev zakonodaje EU;

AB. ker morajo v skladu s členom 6 PEU, ki se nanaša na Listino Evropske unije o temeljnih pravicah in EKČP, tudi agencije držav članic in celo subjekti zasebnega prava, ki delujejo na področju nacionalne varnosti, spoštovati pravice iz EKČP, najsi gre za njihove državljane ali državljane drugih držav;

Ekstrateritorialnost

AC. ker lahko ekstrateritorialna uporaba zakonov, predpisov in drugih zakonodajnih ali izvedbenih instrumentov tretjih držav v razmerah, ki sodijo pod pristojnost EU ali njenih držav članic, vpliva na uveljavljeni pravni red in vladavino prava ali celo krši mednarodno pravo ali pravo EU, vključno s pravicami fizičnih in pravnih oseb, če se upoštevata obseg in zadani ali dejanski namen te uporabe; ker je treba v teh izrednih okoliščinah ukrepati na ravni Unije, da se znotraj EU zagotovi spoštovanje vrednot EU, zapisanih v členu 2 PEU, Listini EU o temeljnih pravicah, EKČP, ki se nanašajo na temelje pravice, demokracijo in vladavino prava ter pravice fizičnih in pravnih oseb, določenih v sekundarni zakonodaji, ki uporablja ta temeljna načela, na primer z odpravljanjem, izničenjem, preprečevanjem ali odvračanjem kako drugače učinkov zadevne tuje zakonodaje;

Mednarodni prenosi podatkov

AD. ker bi bila ob prenosu osebnih podatkov s strani institucij, organov, uradov ali agencij EU ali držav članic v ZDA za namene kazenskega pregona brez ustreznih zaščitnih ukrepov in varoval glede spoštovanja temeljnih pravic državljanov EU, zlasti pravice do zasebnosti in varstva osebnih podatkov, zadevna institucija, organ, urad ali agencija EU ali država članica v skladu s členom 340 PDEU ali ustaljeno sodno prakso Sodišča Evropske unije ([1]) odgovorna za kršitev prava EU, to pa vključuje tudi vse kršitve temeljnih pravic iz Listine EU o temeljnih pravicah;

AE. ker prenosi podatkov niso geografsko omejeni in ker se zlasti v kontekstu vse večje globalizacije in svetovnega komuniciranja zakonodajalec EU sooča z novimi izzivi, kar zadeva varstvo osebnih podatkov in komunikacij; ker je zato izjemno pomembno spodbujati pravne okvire o skupnih standardih;

AF. ker množično zbiranje osebnih podatkov za komercialne namene in boj proti terorizmu in hudemu mednarodnemu kriminalu ogroža osebne podatke in pravico do zasebnosti državljanov EU;

Prenosi v ZDA na podlagi načela varnega pristana ZDA

AG. ker pravni okvir ZDA za varstvo podatkov ne zagotavlja ustrezne ravni zaščite za državljane EU;

AH. ker je Komisija z namenom omogočiti upravljavcem podatkov iz EU, da prenesejo osebne podatke subjektu v ZDA, v svoji Odločbi 2000/520/ES razglasila ustreznost zaščite, ki jo zagotavljajo načela zasebnosti varnega pristana in s tem povezana pogosto zastavljena vprašanja, ki jih je izdalo ministrstvo za trgovino ZDA, za osebne podatke, ki se prenašajo iz Unije v organizacije s sedežem v ZDA, pridružene sporazumu o varnem pristanu;

([1]) Glej zlasti združeni zadevi C-6/90 in C-9/90, Francovich in drugi proti Italiji, sodba z dne 19. novembra 1991.

AI. ker je Evropski parlament v svoji resoluciji z dne 5. julija 2000 izrazil dvom in zaskrbljenost glede ustreznosti varnega pristana in pozval Komisijo, naj pravočasno ponovno pregleda odločbo v luči izkušenj in morebitnih zakonodajnih sprememb;

AJ. ker sta poročevalca v delovnem dokumentu 4 Evropskega parlamenta o dejavnostih nadzora ZDA v zvezi s podatki iz EU in možnih pravnih posledicah za čezatlantske sporazume in sodelovanje z dne 12. decembra 2013 izrazila dvome in pomisleke glede ustreznosti sporazuma o varnem pristanu in pozvala Komisijo, naj prekliče ustreznost varnega pristana in poišče nove pravne rešitve;

AK. ker Odločba Komisije 2000/520/ES določa, da lahko pristojni organi v državah članicah uporabijo svoja obstoječa pooblastila za prekinitev prenosa podatkov organizaciji, ki se je samocertificirano zavezala načelom varnega pristana, da bi zaščitili posameznike, kar zadeva obdelavo njihovih osebnih podatkov, v primerih, ko je zelo verjetno, da se načela varnega pristana kršijo ali da bi nadaljnji prenos podatkov povzročil neposredno nevarnost za nastanek velike škode za osebe, na katere se podatki nanašajo;

AL. ker Odločba Komisije 2000/520/ES navaja tudi, da mora Komisija, kadar se dokaže, da odgovorni za zagotavljanje upoštevanja načel varnega pristana svoje vloge ne opravljajo učinkovito, obvestiti ministrstvo za trgovino ZDA in po potrebi predložiti ukrepe za razveljavitev ali odložitev te odločbe ali omejitev njenega področja uporabe;

AM. ker je Komisija v svojih prvih dveh poročilih o izvajanju varnega pristana iz let 2002 in 2004 ugotovila več pomanjkljivosti v zvezi z ustreznim izvajanjem sporazuma o varnem pristanu ter organom ZDA podala več priporočil za odpravo teh nepravilnosti;

AN. ker je Komisija v svojem tretjem poročilu o izvajanju z dne 27. novembra 2013, devet let po drugem poročilu in ne da bi bile pomanjkljivosti, ugotovljene v tem predhodnem poročilu, odpravljene, ugotovila nadaljnje obsežne slabosti in pomanjkljivosti varnega pristana ter sklenila, da sedanjega načina izvajanja sporazuma ni mogoče ohraniti; ker je Komisija poudarila, da obsežno dostopanje ameriških obveščevalnih agencij do podatkov, ki so jih v ZDA prenesli subjekti, vključeni v varni pristan, poraja nova resna vprašanja glede neprekinjenosti zaščite podatkov o posameznikih iz EU; ker je Komisija na organe ZDA naslovila 13 priporočil in se obvezala, da bo do poletja 2014 skupaj z organi ZDA opredelila pravna sredstva, ki jih je treba čim prej uveljaviti, ter tako oblikovala podlago za popoln pregled delovanja načel varnega pristana;

AO. ker se je delegacija Odbora za državljanske svoboščine, pravosodje in notranje zadeve Evropskega parlamenta (odbora LIBE) v Washingtonu med 28. in 31. oktobrom 2013 srečala z ministrstvom za trgovino ZDA in zvezno komisijo ZDA za trgovino; ker je ministrstvo za trgovino potrdilo obstoj organizacij, ki so samocertificirano pristopile k načelom varnega pristana, vendar jasno kažejo „status mirovanja“, kar pomeni, da družba ne izpolnjuje zahtev varnega pristana, čeprav še vedno prejema osebne podatke iz EU; ker je zvezna komisija za trgovino priznala, da je treba sporazum o varnem pristanu ponovno pregledati in ga izboljšati, predvsem kar zadeva pritožbe in alternativne sisteme za reševanje sporov;

AP. ker se lahko načela varnega pristana omejijo, „če je to potrebno za izpolnjevanje zahtev nacionalne varnosti, javnega interesa ali odkrivanja in pregona“; ker je treba takšno izjemo, kot odstopanje od temeljne pravice, vedno razlagati restriktivno in jo omejiti na to, kar je v demokratični družbi nujno in sorazmerno, zakon pa mora jasno določati pogoje in zaščitne ukrepe, da je taka omejitev legitimna; ker bi morale ZDA in EU, zlasti Komisija, področje uporabe te izjeme razjasniti, da bi se izognile kakršnemu koli tolmačenju ali izvajanju, ki bi izničilo bistvo, med drugim, temeljne pravice do zasebnosti in varstva podatkov; ker se ta izjema posledično ne sme uporabljati na način, ki bi spodkopaval ali izničil varstvo, kakršnega zagotavljajo Listina temeljnih pravic, EKČP, zakonodaja EU o varstvu podatkov in načela varnega pristana; vztraja, da je treba v primeru sklicevanja na izjemo zaradi nacionalne varnosti določiti, v skladu s katero nacionalno zakonodajo velja;

AQ. ker je obsežno dostopanje obveščevalnih agencij ZDA močno spodkopalo čezatlantsko zaupanje in negativno vplivalo na zaupanje v ameriške organizacije, ki delujejo v EU; ker se to še stopnjuje zaradi pomanjkanja sodnih in upravnih sredstev za pritožbo za državljane EU v skladu s pravom ZDA, zlasti v primerih dejavnosti nadzora v obveščevalne namene;

Prenosi v tretje države s sklepom o ustreznosti

AR. ker so v skladu z razkritimi informacijami in ugotovitvami odbora LIBE agencije za nacionalno varnost Nove Zelandije, Kanade in Avstralije v velikem obsegu vključene v množični nadzor elektronskih komunikacij in so dejavno sodelovale z ZDA v tako imenovanem programu „petih oči“ ter si med seboj verjetno izmenjavale osebne podatke državljanov EU, ki so bili preneseni iz EU;

AS. ker je Komisija v svojem Sklepu 2013/65/EU ([1]) in Odločbi 2002/2/ES ([2]) razglasila, da novozelandski zakon o zasebnosti in kanadski zakon o varstvu osebnih podatkov in elektronskih dokumentih zagotavljata ustrezno raven zaščite; ker že omenjena razkritja resno ogrožajo tudi zaupanje v pravne sisteme teh držav, kar zadeva neprekinjenost zaščite, ki jo uživajo državljani EU; ker Komisija tega vidika ni preučila;

Prenosi na podlagi pogodbenih klavzul in drugih instrumentov

AT. ker Direktiva 95/46/ES določa, da se lahko prenosi podatkov v tretje države izvajajo tudi s posebnimi instrumenti, pri čemer upravljavec navede ustrezne zaščitne ukrepe v zvezi z varovanjem zasebnosti in temeljnih pravic in svoboščin posameznika ter v zvezi z izvajanjem ustreznih pravic;

AU. ker lahko takšni zaščitni ukrepi izhajajo predvsem iz primernih pogodbenih klavzul;

AV. ker je Komisija v skladu z Direktivo 95/46/ES pooblaščena za odločanje, ali določena standardna pogodbena klavzula nudi zadostne zaščitne ukrepe, ki jih zahteva direktiva, in ker je Komisija na podlagi tega sprejela tri modele standardnih pogodbenih klavzul za prenose upravljavcem in obdelovalcem podatkov (ter njihovim podizvajalcem) v tretjih državah;

AW. ker sklepi Komisije o standardnih pogodbenih klavzulah določajo, da lahko pristojni organi v državah članicah izvajajo svoja obstoječa pooblastila za prekinitev prenosa podatkov, če se ugotovi, da zakonodaja, ki velja za uvoznika ali podizvajalca obdelave podatkov, od njiju zahteva odstopanja od veljavnih zakonov o varstvu podatkov, ki presegajo omejitve, nujne v demokratični družbi, kot je določeno v členu 13 Direktive 95/46/ES, če je verjetno, da bodo te zahteve močno negativno vplivale na jamstva, ki jih zagotavljajo veljavna zakonodaja o varstvu podatkov in standardne pogodbene klavzule, ali če je zelo verjetno, da se standardne pogodbene klavzule iz priloge ne spoštujejo ali se ne bodo spoštovale ter bi nadaljnji prenos podatkov povzročil neposredno nevarnost za nastanek velike škode za osebe, na katere se podatki nanašajo;

AX. ker so nacionalni organi za varstvo podatkov razvili zavezujoča poslovna pravila, da bi olajšali mednarodne prenose podatkov znotraj multinacionalnih družb z ustreznimi zaščitnimi ukrepi, kar zadeva zaščito zasebnosti in posameznikovih temeljnih pravic in svoboščin ter izvajanje ustreznih pravic; ker morajo zavezujoča poslovna pravila pred začetkom uporabe potrditi pristojni organi držav članic, potem ko ocenijo skladnost z evropsko zakonodajo o varstvu podatkov; ker so bila zavezujoča poslovna pravila za obdelovalce podatkov v poročilu odbora LIBE o splošni uredbi o varstvu podatkov zavrnjena, saj v skladu z njimi upravljavec podatkov in oseba, na katero se podatki nanašajo, ne bi imela nikakršnega vpliva na jurisdikcijo, v kateri se podatki obdelujejo;

([1]) UL L 28, 30.1.2013, str. 12.
([2]) UL L 2, 4.1.2002, str. 13.

AY. ker je Evropski parlament glede na svojo pristojnost, ki jo določa člen 218 PDEU, odgovoren za stalno spremljanje vrednosti mednarodnih sporazumov, ki jih je odobril;

Prenosi na podlagi sporazuma o programu za sledenje financiranja terorističnih dejavnosti (TFTP) in sporazuma o evidenci imen letalskih potnikov (PNR)

AZ. ker je Evropski parlament v svoji resoluciji z dne 23. oktobra 2013 izrazil resno zaskrbljenost v zvezi z dejavnostmi agencije NSA, kar zadeva neposredni dostop do sporočil o finančnih plačilih in s tem povezanih podatkov, kar bi predstavljalo jasno kršitev sporazuma TFTP in zlasti njegovega člena 1;

BA. ker je sledenje financiranja terorističnih dejavnosti bistveno orodje v boju proti financiranju terorizma in hudim kaznivim dejanjem, ki protiteroristični preiskovalcem omogoča odkrivanje povezav med osebami, ki so v postopku preiskave, in drugimi morebitnimi osumljenci, povezanimi s širšimi terorističnimi mrežami, za katere obstaja sum, da financirajo terorizem;

BB. ker je Evropski parlament pozval Komisijo, naj začasno preneha z izvajanjem sporazuma, in zahteval, da se za razpravo v Evropskem parlamentu nemudoma zagotovijo vse zadevne informacije in dokumenti; ker Komisija ni naredila ne enega ne drugega;

BC. ker se je Komisija po objavi domnev v medijih odločila za začetek posvetovanj z ZDA v zvezi s členom 19 sporazuma TFTP; ker je komisarka Malmströmova dne 27. novembra 2013 obvestila odbor LIBE, da se je Komisija po sestanku z organi ZDA in glede na odgovore, ki so jih ti podali v svojih pismih in na sestankih, odločila, da ne bo nadaljevala s posvetovanji, ker ni elementov, ki bi kazali, da je vlada ZDA ukrepala v nasprotju z določbami sporazuma, in ker so ZDA podale pisno zagotovilo, da ni bilo neposrednega zbiranja podatkov v nasprotju z določbami sporazuma TFTP; ker ni jasno, ali so organi ZDA obšli sporazum z dostopanjem do teh podatkov z drugimi sredstvi, kot je zapisano v pismu organov ZDA z dne 18. septembra 2013 ([1]);

BD. ker se je delegacija odbora LIBE v Washingtonu med 28. in 31. oktobrom 2013 sestala z ministrstvom za finance ZDA; ker je ameriško ministrstvo za finance izjavilo, da vse od začetka veljavnosti sporazuma TFTP ni imelo dostopa do podatkov organizacije SWIFT v EU, razen v okviru sporazuma TFTP; ker ministrstvo za finance ZDA ni želelo komentirati, ali je do podatkov organizacije SWIFT zunaj sporazuma TFTP dostopal kateri koli drug organ ali ministrstvo in ali se administracija ZDA zaveda dejavnosti množičnega nadzora agencije NSA; ker je Glenn Greenwald dne 18. decembra 2013 pred preiskovalnim odborom LIBE izjavil, da sta agenciji NSA in GCHQ usmerjali svoje delovanje v mreže SWIFT;

BE. ker sta se belgijski in nizozemski organ za varstvo podatkov dne 13. novembra 2013 odločila, da bosta izvedla skupno preiskavo o varnosti plačilnih mrež organizacije SWIFT, da bi ugotovila, ali lahko tretje osebe nepooblaščeno ali nezakonito dostopajo do bančnih podatkov evropskih državljanov ([2]);

BF. ker je v skladu s skupnim pregledom sporazuma PNR med EU in ZDA ministrstvo ZDA za domovinsko varnost agenciji NSA razkrilo 23 nizov podatkov PNR na podlagi posamičnih primerov v podporo protiterorističnim zadevam, in sicer na način, ki je skladen s posebnimi pogoji sporazuma;

BG. ker poročilo o skupnem pregledu ne omenja dejstva, da v primeru obdelave osebnih podatkov v obveščevalne namene v skladu z zakonodajo ZDA osebe, ki niso državljani ZDA, nimajo na voljo nobene sodne ali upravne poti za zaščito svojih pravic in da ustavno varstvo uživajo samo državljani in rezidenti ZDA; ker ta odsotnost sodnih ali upravnih pravic izniči varovala za državljane EU, ki so določena v obstoječem sporazumu PNR;

([1]) V pismu je zapisano, da vlada ZDA išče in pridobiva finančne podatke, ki se zbirajo prek rednih, diplomatskih, obveščevalnih kanalov in kanalov kazenskega pregona ter prek izmenjav s tujimi partnerji, in da vlada ZDA uporablja sistem TFTP za pridobivanje podatkov SWIFT, ki jih ne dobi iz drugih virov.

([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

Prenosi na podlagi sporazuma med EU in ZDA o medsebojni pravni pomoči v kazenskih zadevah

BH. ker je sporazum med EU in ZDA o medsebojni pravni pomoči v kazenskih zadevah z dne 6. junija 2003 ([1]) začel veljati 1. februarja 2010, namenjen pa je lajšanju sodelovanja med EU in ZDA za učinkovitejši boj proti kriminalu ob ustreznem upoštevanju pravic posameznikov in načela pravne države;

Okvirni sporazum o varstvu podatkov na področju policijskega in pravosodnega sodelovanja („krovni sporazum")

BI. ker je namen tega splošnega sporazuma vzpostavitev pravnega okvira za vse prenose osebnih podatkov med EU in ZDA izključno za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj, vključno s terorizmom, v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah; ker je Svet dne 2. decembra 2010 odobril pogajanja; ker je ta sporazum izjemno pomemben in naj bi predstavljal podlago za pospeševanje prenosa podatkov v okviru policijskega in pravosodnega sodelovanja ter v kazenskih zadevah;

BJ. ker bi moral ta sporazum zagotoviti jasna in natančna pravno zavezujoča načela za obdelavo podatkov in zlasti priznati pravico državljanov EU do pravnega dostopa, popravka in izbrisa njihovih osebnih podatkov v ZDA ter pravico do učinkovitega mehanizma upravnega ali sodnega varstva za državljane EU v ZDA ter zagotoviti neodvisen nadzor dejavnosti obdelave podatkov;

BK. ker je Komisija v svojem sporočilu z dne 27. novembra 2013 zapisala, da bi moral krovni sporazum prispevati k visoki ravni zaščite državljanov na obeh straneh Atlantika in okrepiti zaupanje Evropejcev v izmenjave podatkov med EU in ZDA s tem, da bi zagotovil podlago, na kateri bi lahko še naprej razvijali varnostno sodelovanje in partnerstvo med EU in ZDA;

BL. ker pogajanja o sporazumu ne napredujejo zaradi vztrajnega stališča vlade ZDA, da ne prizna pravic do učinkovitega upravnega in sodnega varstva za državljane EU, in zaradi namere, da se zagotovijo široka odstopanja od načel varstva podatkov, ki bi jih določal sporazum, kot so načela omejitve namena, hrambe podatkov ali nadaljnjih prenosov doma ali v tujino;

Reforma varstva podatkov

BM. ker trenutno poteka ponovni pregled pravnega okvira EU za varstvo podatkov z namenom, da se vzpostavi celovit, skladen, sodoben in trden sistem za vse dejavnosti obdelave podatkov v Uniji; ker je Komisija januarja 2012 predstavila sveženj zakonodajnih predlogov: splošno uredbo o varstvu podatkov ([2]), ki bo nadomestila Direktivo 95/46/ES in vzpostavila enotno zakonodajo po vsej EU, in direktivo ([3]), ki bo določila usklajen okvir za vse dejavnosti obdelave podatkov s strani organov kazenskega pregona v namene kazenskega pregona in zmanjšala trenutne razlike med nacionalnimi zakonodajami;

BN. ker je odbor LIBE 21. oktobra 2013 sprejel svoji zakonodajni poročili o obeh predlogih in sklep o začetku pogajanj s Svetom, da bi bili pravni instrumenti sprejeti v tem mandatnem obdobju;

BO. ker Evropski svet kljub temu, da je na svojem zasedanju 24. in 25. oktobra 2013 pozval k pravočasnemu sprejetju trdnega splošnega okvira EU za varstvo podatkov, da bi spodbudili zaupanje državljanov in podjetij v digitalno gospodarstvo, po dveh letih posvetovanj še vedno ni sprejel splošne usmeritve o napovedanih splošni uredbi o varstvu podatkov in direktivi ([4]);

([1]) UL L 181, 19.7.2003, str. 25.
([2]) COM(2012)0011, 25.1.2012.
([3]) COM(2012)0010, 25.1.2012
([4]) http://register.consilium.europa.eu/pd/sl/13/st00/st00169.sl13.pdf

Informacijskotehnološka varnost in računalništvo v oblaku

BP. ker je v zgoraj omenjeni resoluciji Parlamenta z dne 10. decembra 2013 poudarjen gospodarski potencial podjetij, ki se ukvarjajo z „računalništvom v oblaku“, za rast in zaposlovanje; ker predvidena splošna gospodarska vrednost trga računalništva v oblaku do leta 2016 znaša 207 milijard USD letno, kar je dvakrat več kot leta 2012;

BQ. ker raven varstva podatkov v okolju za računalništvo v oblaku na splošno ne sme biti nižja od ravni varstva, ki se zahteva v katerem koli drugem okviru obdelave podatkov; ker zakonodaja EU o varstvu podatkov že v celoti velja za storitve računalništva v oblaku, ki delujejo v EU, saj je tehnološko nevtralna;

BR. ker dejavnosti množičnega nadzora obveščevalnim agencijam omogočajo dostop do osebnih podatkov, ki jih posamezniki iz EU shranjujejo ali kako drugače obdelujejo v okviru sporazumov o storitvah v oblaku, sklenjenih s pomembnimi ameriškimi ponudniki teh storitev; ker so obveščevalni organi ZDA dostopali do osebnih podatkov, shranjenih ali drugače obdelanih na strežnikih na ozemlju EU, tako da so se priključili na notranje mreže podjetij Yahoo in Google; ker te dejavnosti pomenijo kršitev mednarodnih obveznosti in evropskih standardov temeljnih pravic, vključno s pravico do zasebnega in družinskega življenja, zaupnosti komunikacij, domneve nedolžnosti, svobodo izražanja in dostopa do informacij ter svobodo zbiranja in združevanja in pa svobodo gospodarske pobude; ker ni izključeno, da so obveščevalne agencije dostopale tudi do informacij, ki jih v oblaku shranjujejo javni organi držav članic ali podjetja in institucije;

BS. ker imajo obveščevalne agencije ZDA politiko sistematičnega spodkopavanja kriptografskih protokolov in izdelkov, da bi lahko prestrezale celo šifrirane komunikacije; ker je Agencija ZDA za nacionalno varnost zbrala veliko število varnostnih vrzeli v informacijski tehnologiji (t.i. „zero-day exploits“), ki javnosti ali prodajalcu izdelka še niso znane; ker takšne dejavnosti močno spodkopavajo svetovna prizadevanja za izboljšanje varnosti informacijske tehnologije;

BT. ker je dejstvo, da so obveščevalne agencije dostopale do osebnih podatkov uporabnikov spletnih storitev, močno omajalo zaupanje državljanov v takšne storitve, kar negativno vpliva na podjetja, ki vlagajo v razvoj novih storitev, ki uporabljajo velike količine podatkov, ter novih aplikacij, kot je internet stvari;

BU. ker prodajalci informacijske tehnologije pogosto dobavljajo proizvode, ki niso bili ustrezno preizkušeni glede informacijskotehnološke varnosti ali ki jim prodajalec včasih celo namerno vgradi stranska vrata; ker je pomanjkanje pravil o odgovornosti prodajalcev programske opreme pripeljalo do takšnih razmer, ki jih izkoriščajo obveščevalne agencije, hkrati pa obstaja tudi tveganje za napade drugih subjektov;

BV. ker je za družbe, ki zagotavljajo takšne nove storitve in aplikacije, bistveno, da spoštujejo pravila o varstvu podatkov in zasebnost oseb, katerih podatki se zbirajo, obdelujejo in analizirajo, da bi med državljani ohranile visoko raven zaupanja;

Demokratični nadzor obveščevalnih služb

BW. ker so obveščevalnim službam v demokratičnih družbah dodeljena posebna pooblastila in zmogljivosti za varovanje temeljnih pravic, demokracije in pravne države, pravic državljanov in države pred notranjimi in zunanjimi nevarnostmi in so demokratično odgovorne in pod sodnim nadzorom; ker so jim izključno v ta namen dodeljena posebna pooblastila in zmogljivosti; ker bi morale ta pooblastila uporabljati znotraj meja pravne države, njihova uporaba pa bi morala biti strogo nadzorovana, sicer bi izgubile legitimnost in tvegale spodkopavanje demokracije;

BX. ker je obveščevalnim službam sicer dovoljena določena stopnja tajnosti, namenjena preprečevanju ogrožanja tekočih operacij, razkrivanja metod dela ali spravljanja agentov v življenjsko nevarnost, vendar ta tajnost ne sme prevladati nad pravili o demokratičnem in sodnem nadzoru in preverjanju dejavnosti obveščevalnih služb ali jih izključevati, enako pa velja tudi za pravila o preglednosti, zlasti kar zadeva spoštovanje temeljnih pravic in pravne države, ki so temelji demokratične družbe;

BY. ker je bila večina obstoječih nacionalnih nadzornih mehanizmov in organov ustanovljena ali prenovljena v 90. letih prejšnjega stoletja in ni bila nujno prilagojena hitremu političnemu in tehnološkemu razvoju v zadnjem desetletju, ki je privedel do povečanega mednarodnega sodelovanja med obveščevalnimi službami, ki vključuje tudi izmenjavo osebnih podatkov in pogosto zabriše mejo med obveščevalnimi dejavnostmi in dejavnostmi kazenskega pregona;

BZ. ker se demokratični nadzor obveščevalnih dejavnosti – kljub povečani izmenjavi informacij med državami članicami EU ter med državami članicami in tretjimi državami – še vedno izvaja le na nacionalni ravni; ker se povečuje vrzel med stopnjo mednarodnega sodelovanja na eni strani in nadzornimi zmogljivostmi, ki so omejene na nacionalno raven, na drugi, kar vodi do nezadostnega in neučinkovitega demokratičnega nadzora;

CA. ker nacionalni nadzorni organi pogosto nimajo polnega dostopa do obveščevalnih podatkov, prejetih od tuje obveščevalne agencije, kar lahko pripelje do vrzeli, v katerih se mednarodne izmenjave podatkov lahko vršijo brez ustreznega pregleda; ker razmere še dodatno otežuje t.i. „pravilo tretje osebe“ ali načelo „nadzora originatorja“, ki je bilo vzpostavljeno, da se originatorju omogoči ohranjanje nadzora nad nadaljnjim razširjanjem občutljivih informacij, vendar se žal pogosto razlaga v smislu, da velja tudi za organ, ki izvaja nadzor nad službo, ki prejema informacije;

CB. ker so zasebne in javne pobude za reformo preglednosti ključne za zagotavljanje zaupanja javnosti v dejavnosti obveščevalnih agencij; ker pravni sistemi podjetjem ne bi smeli preprečevati, da javnosti razkrijejo podatke o tem, kako obravnavajo vse vrste vladnih zahtev in sodnih nalogov za dostop do podatkov o uporabnikih, vključno z možnostjo razkritja zbirnih informacij o številu zahtev in nalogov, ki so jim ugodili oziroma so jih zavrnili;

Glavne ugotovitve

1. meni, da so nedavna razkritja prijaviteljev nepravilnosti in novinarjev v medijih skupaj z navedbami izvedencev, podanimi v okviru te preiskave, priznanji organov in nezadostnim odzivom na te obtožbe pripeljala do prepričljivih dokazov o obstoju daljnosežnih, zapletenih in tehnološko izjemno naprednih sistemov, ki so jih obveščevalne službe ZDA in nekaterih držav članic oblikovale za zbiranje, hrambo in analizo podatkov, povezanih s komuniciranjem, vključno s podatki o vsebini, in podatkov o lokaciji ter metapodatkov vseh državljanov po vsem svetu v obsegu brez primere in na vsesplošen način, ki ne temelji na sumu;

2. posebej opozarja na obveščevalne programe ameriške agencije NSA, ki omogočajo množični nadzor državljanov EU z neposrednim dostopom do osrednjih strežnikov vodilnih internetnih podjetij v ZDA (program PRISM), analizo vsebine in metapodatkov (program Xkeyscore), izogibanje spletnemu šifriranju (BULLRUN), dostop do računalniških in telefonskih omrežij in podatkov o lokacijah, ter na sisteme britanske obveščevalne agencije GCHQ, kot so program za dejavnost nadzora bliže viru (Tempora) in program za dešifriranje (Edgehill), ciljni napadi vrinjenega napadalca na informacijske sisteme (programa Quantumtheory in Foxacid) ter zbiranje in hramba 200 milijonov besedilnih sporočil SMS na dan (program Dishfire);

3. ugotavlja, da naj bi britanska obveščevalna agencija GCHQ domnevno vdrla v računalniške sisteme podjetja Belgacom oziroma se priključila nanje; ugotavlja, da je podjetje Belgacom izjavilo, da ne more ne potrditi ne zanikati, da je bila ta dejavnost usmerjena na institucije EU oziroma da jih je prizadela, ter da je bila uporabljena zlonamerna programska oprema izjemno zapletena in da so bili za njen razvoj in uporabo potrebni obširni finančni in kadrovski viri, ki jih zasebna podjetja in hekerji običajno nimajo na voljo;

4. poudarja, da je bilo zaupanje močno omajano: zaupanje med obema čezatlantskima partnericama, zaupanje med državljani in njihovimi vladami, zaupanje v delovanje demokratičnih institucij na obeh straneh Atlantika, zaupanje v spoštovanje načela pravne države ter v varnost storitev informacijske tehnologije in komunikacij; meni, da je za ponovno vzpostavitev zaupanja v vseh teh razsežnostih potreben načrt za takojšen in celovit odziv, ki bi zajemal številne ukrepe, ki bodo podvrženi nadzoru javnosti;

5. ugotavlja, da nekatere vlade zatrjujejo, da so ti programi za množični nadzor nujni za boj proti terorizmu; ostro obsoja terorizem, vendar je trdno prepričan, da boj proti njemu nikoli ne sme biti opravičilo za neciljne, tajne ali celo nezakonite programe množičnega nadzora; meni, da so takšni programi neskladni z načeloma nujnosti in sorazmernosti v demokratični družbi;

6. opozarja na trdno prepričanje EU, da je treba doseči pravo ravnovesje med varnostnimi ukrepi ter varstvom državljanskih svoboščin in temeljnih pravic ter hkrati zagotoviti kar največje spoštovanje zasebnosti in varstva podatkov;

7. meni, da se zbiranje podatkov v takšnem obsegu vzbuja precejšnje dvome, ali se to res izvaja samo zaradi boja proti terorizmu, saj vključuje zbiranje vseh mogočih podatkov o vseh državljanih; zato opozarja na možnost prisotnosti drugih namenov, vključno s političnim in gospodarskim vohunjenjem, in meni, da je treba te dvome v celoti odpraviti;

8. dvomi v združljivost dejavnosti množičnega gospodarskega vohunjenja nekaterih držav članic z zakonodajo o notranjem trgu EU in konkurenci, ki je zapisana pod naslovoma I in VII Pogodbe o delovanju Evropske unije; ponovno poudarja načelo lojalnega sodelovanja, kot je zapisano v členu 4(3) Pogodbe o Evropski uniji, in načelo, da se države članice „vzdržijo vseh ukrepov, ki bi lahko ogrozili uresničevanje ciljev Unije“;

9. ugotavlja, da mednarodne pogodbe, zakonodaja EU in ZDA ter nacionalni nadzorni mehanizmi niso uspeli zagotoviti potrebnega sistema medsebojnega nadzora in demokratične odgovornosti;

10. obsoja obširno, sistematično in splošno zbiranje podatkov nedolžnih ljudi, pri čemer gre pogosto za intimne osebne podatke; poudarja, da sistemi vsesplošnega množičnega nadzora s strani obveščevalnih služb predstavljajo resen poseg v temeljne pravice državljanov; poudarja, da zasebnost ni luksuzna pravica, temveč temeljni kamen svobodne in demokratične družbe; poleg tega opozarja, da ima množični nadzor lahko resne posledice za svobodo tiska, misli in govora kot tudi za svobodo zbiranja in združevanja ter ponuja precejšnje možnosti za zlorabo zbranih podatkov proti političnim nasprotnikom; poudarja, da te dejavnosti množičnega nadzora vključujejo tudi nezakonita dejanja obveščevalnih služb in da se ob njih zastavljajo vprašanja v zvezi z ekstrateritorialnostjo nacionalne zakonodaje;

11. meni, da je nujno treba zaščititi pravico do zaupnosti, ki jo uživajo poklici, kot so odvetniki, novinarji, zdravniki in pripadniki drugih reguliranih poklicev, pred dejavnostmi množičnega nadzora; zlasti poudarja, da bi lahko kakršna koli negotovost o zaupnosti komunikacije med odvetniki in njihovimi strankami negativno vplivala na pravico državljanov EU do dostopa do pravnega in sodnega varstva ter pravice do pravičnega sojenja;

12. meni, da so programi nadzora še en korak k vzpostavitvi preventivne države v polnem pomenu besede, ki spreminja ustaljeno paradigmo kazenskega prava v demokratičnih družbah, v skladu s katero mora vsak poseg v temeljne pravice osumljenca potrditi sodnik ali tožilec na podlagi utemeljenega suma, kot to določa zakonodaja, in namesto nje spodbuja mešanico ukrepov kazenskega pregona in obveščevalnih dejavnosti z nejasnimi in oslabljenimi pravnimi jamstvi, kar pogosto ni v skladu z demokratičnimi sistemi medsebojnega nadzora in temeljnimi pravicami, zlasti kar zadeva domnevo nedolžnosti; v zvezi s tem opozarja na odločitev nemškega zveznega ustavnega sodišča ([1]) o prepovedi uporabe preventivnega mrežnega izsledovanja („präventive Rasterfahndung“), razen če obstaja dokaz o konkretni nevarnosti za druge pomembne zakonsko zavarovane pravice, pri čemer razmere splošne nevarnosti ali mednarodne napetosti ne zadostujejo za upravičenje takšnih ukrepov;

13. je prepričan, da tajni zakoni in sodišča kršijo načelo pravne države; poudarja, da se nobena sodba sodišča in nobena odločba upravnega organa države, ki ni članica EU, ki neposredno ali posredno dovoljuje izmenjavo osebnih podatkov, ne sme na noben način priznati ali izvršiti, razen če obstajajo pogodbe o medsebojni pravni pomoči ali veljavni mednarodni sporazum med tretjo državo prosilko in Unijo ali državo članico in predhodno dovoljenje pristojnega nadzornega organa; opozarja, da se ne prizna in ne izvrši nobena sodba tajnega sodišča in nobena odločba upravnega organa države, ki ni članica EU, ki tajno neposredno ali posredno dovoljuje dejavnosti nadzora;

([1]) Št. 1 BvR 518/02 z dne 4. aprila 2006.

14. meni, da so zgoraj omenjeni pomisleki zaradi hitrega tehnološkega in družbenega razvoja še toliko bolj pereči, saj internet in mobilne naprave prisotni povsod v sodobnem vsakodnevnem življenju („vseprisotno računalništvo“) in poslovni model večine internetnih podjetij temelji na obdelavi osebnih podatkov; meni, da je tako obsežnega in resnega tovrstnega problema še ni bilo; ugotavlja, da lahko to pripelje do stanja, kjer je mogoče infrastrukturo za množično zbiranje in obdelovanje podatkov zlorabiti v primeru spremembe političnega režima;

15. ugotavlja, da ni zagotovila za javne institucije EU niti za državljane, da je mogoče njihovo informacijskotehnološko varnost ali zasebnost zaščititi pred napadi dobro opremljenih vsiljivcev („ni stoodstotne informacijskotehnološke varnosti“); opozarja, da morajo biti Evropejci za doseganje čim večje informacijskotehnološke varnosti pripravljeni nameniti dovolj človeških in finančnih virov za ohranjanje neodvisnosti in samozadostnosti Evrope na področju informacijske tehnologije;

16. odločno zavrača stališče, da so vsa vprašanja v zvezi s programi množičnega nadzora le stvar nacionalne varnosti in zato v izključni pristojnosti držav članic; poziva države članice, naj v celoti spoštujejo zakonodajo EU in EKČP, hkrati pa ukrepajo, da bi zagotovile svojo nacionalno varnost; opozarja na nedavno sodbo Sodišča Evropske unije, v kateri je zapisano: „čeprav so države članice pristojne za sprejetje ukrepov, primernih za zagotavljanje njihove notranje in zunanje varnosti, pa zgolj dejstvo, da se odločba nanaša na državno varnost, ne more imeti za posledico izključitev uporabe prava Unije“ ([1]); poleg tega poudarja, da gre za varstvo zasebnosti vseh državljanov EU ter varnost in zanesljivost vseh komunikacijskih omrežij EU; zato meni, da razprava in ukrepi na ravni EU niso zgolj legitimni, temveč so tudi stvar neodvisnosti EU;

17. izraža pohvalo institucijam in strokovnjakom, ki so prispevali k tej preiskavi; obžaluje dejstvo, da je več organov držav članic zavrnilo sodelovanje v preiskavi, ki jo je Evropski parlament izvajal v imenu državljanov; pozdravlja odprtost nekaterih članov ameriškega kongresa in poslancev nacionalnih parlamentov;

18. se zaveda, da je bilo mogoče v tako omejenem časovnem okviru izvesti samo predhodno preiskavo vseh vprašanj, ki so se pojavila od julija 2013; priznava resnost zadevnih razkritij in dejstvo, da se razkrivanje nadaljuje; zato sprejema pristop v prihodnost usmerjenega načrtovanja, ki je sestavljen iz vrste konkretnih predlogov in mehanizma za nadaljnje ukrepe v naslednjem parlamentarnem obdobju, kar zagotavlja, da bodo ugotovitve ostale na samem vrhu političnega seznama prednostnih nalog EU;

19. namerava zahtevati trdno politično zavezo nove Evropske komisije, ki bo imenovana po evropskih volitvah maja 2014, da bo izvedla predloge in priporočila te preiskave;

Priporočila

20. poziva organe ZDA in države članice EU, naj prepovejo dejavnosti vsesplošnega množičnega nadzora, kjer še niso prepovedane;

21. poziva države članice EU, zlasti tiste, ki sodelujejo v tako imenovanih programih „devetih oči“ in „štirinajstih oči“ ([2]), naj celovito ocenijo in po potrebi ponovno pregledajo svojo nacionalno zakonodajo in prakse v zvezi z dejavnostmi obveščevalnih služb, da bi zagotovili, da so te podvržene parlamentarnemu in sodnemu nadzoru ter nadzoru javnosti, da spoštujejo načela zakonitosti, nujnosti, sorazmernosti, ustreznega postopka, obveščanja uporabnikov in preglednosti, vključno s skladnostjo z zbirkami OZN o dobrih praksah in priporočili Beneške komisije, ter da so skladne s standardi Evropske konvencije o človekovih pravicah in spoštujejo obveznosti držav članic v zvezi s temeljnimi pravicami, zlasti kar zadeva varstvo podatkov, zasebnost in domnevo nedolžnosti;

([1]) Sodba v zadevi C-300/11, ZZ proti Secretary of State for the Home Department, 4. junij 2013.

([2]) Program devetih oči sestavljajo ZDA, Združeno kraljestvo, Kanada, Avstralija, Nova Zelandija, Danska, Francija, Norveška in Nizozemska; program štirinajstih oči sestavljajo omenjene države in še Nemčija, Belgija, Italija, Španija in Švedska.

22. poziva vse države članice EU, ob upoštevanju resolucije z dne 4. julija 2013 in predstavitev v okviru preiskave pa še zlasti Združeno kraljestvo, Francijo, Nemčijo, Švedsko, Nizozemsko in Poljsko, naj zagotovijo, da so njihovi sedanji ali prihodnji zakonodajni okviri in nadzorni mehanizmi, ki urejajo dejavnosti obveščevalnih agencij, v skladu s standardi Evropske konvencije o človekovih pravicah in zakonodajo Evropske unije o varstvu podatkov; poziva te države članice, naj pojasnijo domneve o dejavnostih množičnega nadzora, vključno z množičnim nadzorom čezmejnih telekomunikacij, neciljnim nadzorom na kabelskih komunikacijah, morebitnimi dogovori med obveščevalnimi službami in telekomunikacijskimi družbami, kar zadeva dostop do osebnih podatkov in njihovo izmenjavo ter dostop do čezatlantskih kablov, in prisotnostjo osebja in opreme obveščevalnih služb ZDA na ozemlju EU brez pregleda nad njihovimi nadzornimi operacijami, ter njihovo skladnost z zakonodajo EU; poziva nacionalne parlamente teh držav, naj okrepijo sodelovanje svojih organov za nadzor nad obveščevalnimi dejavnostmi na evropski ravni;

23. poziva zlasti Združeno kraljestvo, naj glede na obširno poročanje medijev o dejavnostih množičnega nadzora s strani obveščevalne službe GCHQ ponovno pregleda sedanji pravni okvir, ki je sestavljen iz „zapletenega vzajemnega delovanja“ treh ločenih zakonodajnih aktov – zakona o človekovih pravicah iz leta 1998, zakona o obveščevalnih službah iz leta 1994 in zakona o urejanju preiskovalnih pooblastil iz leta 2000;

24. je seznanjen s pregledom nizozemskega zakona o obveščevalni in varnostni dejavnosti iz leta 2002 (poročilo Dessensove komisije z dne 2. decembra 2013); podpira tista priporočila revizijske komisije, katerih namen je povečanje preglednosti nizozemskih obveščevalnih služb ter nadzora nad njimi; poziva Nizozemsko, naj se vzdrži širjenja pooblastil obveščevalnih služb na način, da bi lahko opravljale neciljno in obsežno nadziranje kabelskih komunikacij nedolžnih državljanov, zlasti glede na dejstvo, da je ena izmed največjih internetnih izmenjevalnih točk na svetu ravno v Amsterdamu (AMS-IX); poziva k previdnosti pri opredeljevanju nalog in zmogljivosti nove Skupne kibernetske enote za komunikacijske signale (Joint Sigint Cyber Unit) ter pri prisotnosti in delovanju osebja obveščevalnih služb ZDA na nizozemskem ozemlju;

25. poziva države članice, tudi kadar jih zastopajo njihove obveščevalne agencije, naj se vzdržijo sprejemanja podatkov od tretjih držav, ki so bili zbrani nezakonito, in naj na svojem ozemlju ne dovolijo dejavnosti nadzora s strani vlad ali agencij tretjih držav, ki so po nacionalni zakonodaji nezakonite ali ne izpolnjujejo določb o pravnih jamstvih iz mednarodnih instrumentov ali instrumentov EU, vključno z določbami o varstvu človekovih pravic iz PEU, EKČP in Listine EU o temeljnih pravicah;

26. poziva vse tajne službe, naj prenehajo množično prestrezati in obdelovati posnetke spletnih kamer; poziva države članice, naj celovito preiščejo, ali, kako in v kakšni meri so bile njihove tajne službe udeležene v zbiranju in obdelavi posnetkov spletnih kamer, ter zbrišejo vse shranjene posnetke, zbrane s tovrstnimi programi za množični nadzor;

27. poziva države članice, naj nemudoma izpolnijo svojo obveznost iz Evropske konvencije o človekovih pravicah, da bodo varovale svoje državljane pred nadzorom tretjih držav ali lastnih obveščevalnih služb, ki ni v skladu z zahtevami konvencije, tudi takrat, ko je nadzor namenjen ohranjanju nacionalne varnosti, in zagotovile, da pravna država ne bo oslabljena zaradi ekstrateritorialne uporabe zakonodaje tretje države;

28. poziva generalnega sekretarja Sveta Evrope, naj sproži postopek iz člena 52, v skladu s katerim „mora na zahtevo generalnega sekretarja Sveta Evrope vsaka Visoka pogodbena stranka predložiti pojasnila o tem, kako njeno notranje pravo zagotavlja učinkovito uveljavljanje vseh določb te konvencije“;

29. poziva države članice, naj takoj ustrezno ukrepajo, vključno s sodnimi postopki, proti kršitvam svoje suverenosti in s tem splošnega mednarodnega javnega prava, ki se vršijo s programi za množični nadzor; nadalje poziva države članice, naj uporabijo vse razpoložljive mednarodne ukrepe za zaščito temeljnih pravic državljanov EU, zlasti s sprožitvijo meddržavnega pritožbenega postopka iz člena 41 Mednarodnega pakta o državljanskih in političnih pravicah (ICCPR);

30. poziva države članice, naj vzpostavijo učinkovite mehanizme, v okviru katerih bodo tisti, ki so odgovorni za programe (množičnega) nadzorovanja, ki so v nasprotju s pravno državo in kršijo temeljne pravice državljanov, odgovarjali za to zlorabo moči;

31. poziva ZDA, naj nemudoma ponovno pregledajo svojo zakonodajo in jo uskladijo z mednarodnim pravom, priznajo pravico do zasebnosti in druge pravice državljanov EU, zagotovijo sodno varstvo za državljane EU in njihove pravice obravnavajo enako kot pravice državljanov ZDA ter podpišejo izbirni protokol, ki omogoča pritožbe posameznikov v skladu z ICCPR;

32. v zvezi s tem pozdravlja podane pripombe in predsedniško politično direktivo, ki jo je predsednik ZDA Obama podal 17. januarja 2014, kot korak k omejevanju pooblastil za uporabo nadzora in obdelave podatkov za namene nacionalne varnosti in k enaki obravnavi osebnih podatkov vseh posameznikov, ne glede na njihovo državljanstvo ali prebivališče, s strani ameriške obveščevalne skupnosti; vendar v okviru odnosov med EU in ZDA pričakuje nadaljnje konkretne korake, ki bodo predvsem okrepili zaupanje v čezatlantske prenose podatkov in zagotovili zavezujoča jamstva za izvršljive pravice državljanov EU do zasebnosti, kot je podrobno opisano v tem poročilu;

33. poudarja svoje resne pomisleke glede dela v Odboru Sveta Evrope za konvencijo o kibernetski kriminaliteti v zvezi s tolmačenjem člena 32 Konvencije o kibernetski kriminaliteti z dne 23. novembra 2001 (Konvencije iz Budimpešte) o čezmejnem dostopu do shranjenih računalniških podatkov s privolitvijo ali v primeru javne dostopnosti in nasprotuje kakršni koli sklenitvi dodatnega protokola ali smernic z namenom, da se razširi področje uporabe te določbe in preseže sedanja ureditev, določena s to konvencijo, ki je že tako velika izjema od načela teritorialnosti, saj bi to lahko pripeljalo do neoviranega dostopa organov kazenskega pregona na daljavo do strežnikov in računalnikov v drugih jurisdikcijah, ne da bi pri tem spoštovali sporazume o medsebojni pravni pomoči in druge instrumente pravosodnega sodelovanja, ki obstajajo z namenom zagotavljanja temeljnih pravic posameznikov, vključno z varstvom podatkov in načelom ustreznega postopka, zlasti s Konvencijo Sveta Evrope št. 108;

34. poziva Komisijo, naj pred julijem 2014 oceni možnost uporabe Uredbe (ES) št. 2271/96 v primerih kolizije zakonov o prenosu osebnih podatkov;

35. poziva Agencijo za temeljne pravice, naj opravi poglobljeno raziskavo o varstvu temeljnih pravic v okviru opravljanja nadzora, in zlasti o trenutnem pravnem stanju državljanov EU, kar zadeva pravna sredstva, ki so jim na voljo v zvezi z omenjenimi dejavnostmi;

Mednarodni prenosi podatkov

Pravni okvir ZDA za varstvo podatkov in načela varnega pristana ZDA

36. ugotavlja, da so podjetja, ki so jih mediji razkrili kot sodelujoča v obširnem množičnem nadzoru posameznikov iz EU, na katere se nanašajo osebni podatki, s strani ameriške agencije NSA, sama potrdila svojo vključitev v instrument varnega pristana in da se varni pristan uporablja kot pravni instrument za prenos osebnih podatkov iz EU v ZDA (primeri so Google, Microsoft, Yahoo!, Facebook, Apple in LinkedIn); izraža zaskrbljenost nad dejstvom, da te organizacije ne šifrirajo podatkov in komunikacij, ki se prenašajo med njihovimi podatkovnimi središči, s čimer obveščevalnim službam omogočajo prestrezanje informacij; pozdravlja naknadne izjave nekaterih ameriških podjetij, da bodo pospešila načrte za začetek šifriranja podatkovnih tokov med svojimi svetovnimi podatkovnimi središči;

37. meni, da obširni dostop obveščevalnih agencij ZDA do osebnih podatkov iz EU, ki se obdelujejo po načelih varnega pristana, ne izpolnjuje meril za odstopanja zaradi „nacionalne varnosti“;

38. ker v trenutnih okoliščinah načela varnega pristana ne zagotavljajo ustrezne zaščite za državljane EU, meni, da bi se morali ti prenosi izvajati v skladu z drugimi instrumenti, kot so pogodbene klavzule ali zavezujoča poslovna pravila, pod pogojem, da ti instrumenti določajo specifične zaščitne ukrepe in varovala ter da jih drugi pravni okviri ne morejo obiti;

39. meni, da Komisija ni uspela ukrepati tako, da bi odpravila znane pomanjkljivosti sedanjega izvajanja sporazuma o varnem pristanu;

40. poziva Komisijo, naj predstavi ukrepe za zagotovitev takojšnjega prenehanja izvajanja Odločbe Komisije 2000/520/ES, s katero je razglasila primernost načel zasebnosti varnega pristana in s tem povezanih pogosto zastavljenih vprašanj, ki jih je izdalo ministrstvo za trgovino ZDA; poziva oblasti ZDA, naj pripravijo predlog za nov okvir za prenos osebnih podatkov iz EU v ZDA, ki bo izpolnjeval zahteve zakonodaje EU o varstvu podatkov in ki bo nudil zahtevano ustrezno raven varstva;

41. poziva pristojne organe držav članic, zlasti organe za varstvo podatkov, naj uporabijo svoja obstoječa pooblastila in takoj ustavijo prenos podatkov vsem organizacijam, ki so same zase potrdile, da spoštujejo načela varnega pristana ZDA, ter zahtevajo, naj se takšen prenos podatkov izvaja samo v skladu z drugimi instrumenti pod pogojem, da ti vsebujejo potrebne zaščitne ukrepe in varovala, kar zadeva zaščito zasebnosti, temeljnih pravic in svoboščin posameznika;

42. poziva Komisijo, naj do decembra 2014 predstavi celovito oceno okvira ZDA za zagotavljanje zasebnosti, ki bo zajemala poslovne dejavnosti, dejavnosti kazenskega pregona in obveščevalne dejavnosti ter konkretna priporočila na podlagi dejstva, da v ZDA ni splošnega zakona o varstvu podatkov; spodbuja Komisijo, naj sodeluje z administracijo ZDA pri vzpostavljanju pravnega okvira, ki bo nudil visoko raven varstva posameznikov v smislu varstva njihovih osebnih podatkov pri prenosu v ZDA in zagotovil enakovrednost okvirov EU in ZDA za zagotavljanje zasebnosti;

Prenosi v druge tretje države s sklepom o ustreznosti

43. opozarja, da Direktiva 95/46/ES določa, da lahko prenosi podatkov v tretjo državo potekajo samo pod pogojem – brez poseganja v spoštovanje nacionalnih določb, sprejetih v skladu z drugimi določbami te direktive – da zadevna tretja država zagotavlja ustrezno raven zaščite, pri čemer je namen te določbe zagotoviti neprekinjenost zaščite, kakršno zagotavlja zakonodaja EU o varstvu podatkov, v primeru prenosa osebnih podatkov iz EU;

44. opozarja, da je treba v skladu z Direktivo 95/46/ES primernost ravni zaščite s strani tretje države oceniti v luči vseh okoliščin prenosa podatkov ali niza prenosov podatkov; prav tako opozarja, da omenjena direktiva Komisiji podeljuje tudi izvedbena pooblastila za razglasitev, da tretja država zagotavlja ustrezno raven zaščite glede na merila, ki jih določa Direktiva 95/46/ES; opozarja, da Direktiva 95/46/ES podeljuje Komisiji tudi pooblastila, da razglasi, da tretja država ne zagotavlja ustrezne ravni zaščite;

45. opozarja, da morajo države članice v tem primeru sprejeti potrebne ukrepe za preprečitev vseh prenosov podatkov iste vrste v zadevno tretjo državo in da bi morala Komisija začeti pogajanja z namenom, da se razmere uredijo;

46. poziva Komisijo in države članice, naj nemudoma ocenijo, ali je vpletenost nacionalnih obveščevalnih agencij teh dveh držav v množični nadzor državljanov EU vplivala na primernost ravni zaščite na podlagi novozelandskega zakona o zasebnosti in kanadskega zakona o varstvu osebnih podatkov in elektronskih dokumentih, ki jo je razglasila Komisija v svojem Sklepu 2013/65/EU in Odločbi 2002/2/ES, in po potrebi sprejmejo ustrezne ukrepe za prekinitev ali razveljavitev sklepa o ustreznosti; Komisijo poziva tudi, naj ovrednoti razmere v drugih državah, ki so prejele oceno ustreznosti; pričakuje, da bo Komisija o ugotovitvah v zvezi z omenjenima državama poročala Parlamentu najpozneje do decembra 2014;

Prenosi na podlagi pogodbenih klavzul in drugih instrumentov

47. opozarja, da so nacionalni organi za varstvo podatkov navedli, da standardne pogodbene klavzule in zavezujoča poslovna pravila niso bila oblikovana ob upoštevanju razmer dostopa do osebnih podatkov v namene množičnega nadzora in da tak dostop ne bi bil skladen z določbami o odstopanju iz pogodbenih klavzul ali zavezujočih poslovnih pravil, ki se nanašajo na izredna odstopanja zaradi upravičenega interesa v demokratični družbi, če je to nujno in sorazmerno;

48. poziva države članice, naj prepovejo ali začasno ustavijo pretok podatkov v tretje države na podlagi standardnih pogodbenih klavzul, pogodbenih klavzul ali zavezujočih poslovnih pravil, ki so jih odobrili pristojni nacionalni organi, če zakon, ki velja za prejemnike podatkov, tem verjetno nalaga zahteve, ki presegajo omejitve, ki so potrebne, ustrezne in sorazmerne v demokratični družbi, in bodo verjetno škodljivo vplivale na jamstva, ki jih zagotavljajo veljavna zakonodaja o varstvu podatkov in standardne pogodbene klavzule, ali če bi nadaljnji prenos povzročil nevarnost za nastanek škode za osebe, na katere se podatki nanašajo;

49. poziva delovno skupino iz člena 29, naj izda smernice in priporočila glede zaščitnih ukrepov in varoval, ki bi jih morali vsebovati pogodbeni instrumenti za mednarodni prenos osebnih podatkov iz EU, da se zagotovi zaščita zasebnosti, temeljnih pravic in svoboščin posameznika, pri tem pa se zlasti upoštevata zakonodaja tretjih držav o obveščevalni dejavnosti in nacionalni varnosti ter vključenost podjetij, ki v tretji državi prejemajo podatke, v dejavnosti množičnega nadzora s strani obveščevalnih agencij tretje države;

50. poziva Komisijo, naj nemudoma preuči standardne pogodbene klavzule, ki jih je določila, ter oceni, ali zagotavljajo potrebno zaščito, kar zadeva dostop do osebnih podatkov, prenesenih na podlagi teh klavzul v obveščevalne namene, in jih po potrebi revidira;

Prenosi na podlagi sporazuma o medsebojni pravni pomoči

51. poziva Komisijo, naj pred koncem leta 2014 poglobljeno ovrednoti obstoječi sporazum o medsebojni pravni pomoči v skladu s členom 17 tega sporazuma, da se preveri njegovo izvajanje v praksi, še zlasti to, ali so ga ZDA dejansko uporabile za pridobivanje podatkov ali dokazov v EU in ali so sporazum obšle, da bi pridobile informacije neposredno v EU, ter oceni vpliv na temeljne pravice posameznika; takšna ocena ne sme navajati samo uradnih izjav ZDA kot zadostne osnove za analizo, temveč mora temeljiti na posebnih ocenah EU; ta temeljiti pregled bi moral obravnavati tudi posledice uporabe ustavne strukture Unije za ta instrument, da bi ga uskladili z zakonodajo Unije ob upoštevanju zlasti Protokola št. 36 in člena 10 tega protokola ter Izjave 50 v zvezi s tem protokolom; prav tako poziva Svet in Komisijo, naj ocenita dvostranske sporazume med državami članicami in ZDA z namenom, da se zagotovi skladnost omenjenih dvostranskih sporazumov s sporazumi, ki jih je oziroma jih bo EU sklenila z ZDA;

Medsebojna pomoč EU v kazenskih zadevah

52. poziva Svet in Komisijo, naj seznanita Parlament s tem, kako države članice dejansko uporabljajo Konvencijo o medsebojni pomoči v kazenskih zadevah med državami članicami, zlasti naslov III o prestrezanju telekomunikacij; poziva Komisijo, naj poda predlog v skladu z Izjavo 50 v zvezi s Protokolom št. 36, kot je zahtevano, pred koncem leta 2014, da se konvencija prilagodi okviru Lizbonske pogodbe;

Prenosi na podlagi sporazuma o programu za sledenje financiranja terorističnih dejavnosti (TFTP) in sporazuma o evidenci imen letalskih potnikov (PNR)

53. meni, da informacije, ki sta jih zagotovila Evropska komisija in ministrstvo za finance ZDA, ne pojasnjujejo, ali ameriške obveščevalne agencije dostopajo do finančnih sporočil SWIFT v EU s prestrezanjem v omrežjih organizacije SWIFT ali operacijskih sistemih oziroma komunikacijskih omrežjih bank, same ali v sodelovanju z nacionalnimi obveščevalnimi agencijami EU in brez uporabe obstoječih dvostranskih kanalov za medsebojno pravno pomoč in pravosodno sodelovanje;

54. ponovno opozarja na svojo resolucijo z dne 23. oktobra 2013 in poziva Komisijo, naj prekine izvajanje sporazuma TFTP;

55. poziva Komisijo, naj se odzove na pomisleke, da med največjimi računalniškimi sistemi rezervacij, ki jih uporabljajo letalske družbe po vsem svetu, trije delujejo v ZDA in da se podatki PNR shranjujejo v sistemih v oblaku, ki delujejo na ozemlju ZDA in v skladu z zakonodajo ZDA, ta pa ne zagotavlja ustreznega varstva podatkov;

Okvirni sporazum o varstvu podatkov na področju policijskega in pravosodnega sodelovanja („krovni sporazum")

56. meni, da je zadovoljiva rešitev v „krovnem sporazumu" predpogoj za popolno obnovo zaupanja med čezatlantskima partnericama;

57. poziva k takojšnjemu nadaljevanju pogajanj z ZDA o „krovnem sporazumu", ki bi moral pravice državljanov EU izenačiti s pravicami državljanov ZDA; poleg tega poudarja, da bi moral ta sporazum vključevati učinkovita in izvršljiva upravna in sodna sredstva za vse državljane EU v ZDA brez kakršne koli diskriminacije;

58. poziva Komisijo in Svet, naj ne dajeta pobud za nove sektorske sporazume ali dogovore o prenosu osebnih podatkov za namene kazenskega pregona z ZDA, dokler ne bo začel veljati „krovni sporazum";

59. poziva Komisijo, naj do aprila 2014 podrobno poroča o različnih točkah pogajalskega mandata in najnovejšem stanju;

Reforma varstva podatkov

60. poziva predsedstvo Sveta in države članice, naj pospešijo svoje delo v zvezi s celotnim svežnjem ukrepov za varstvo podatkov, da se omogoči sprejetje le-tega v letu 2014 in da bodo državljani EU že v bližnji prihodnosti deležni visoke ravni varstva podatkov; poudarja, da odločno ukrepanje in celovita podpora Sveta predstavljajo nujen pogoj za dokaz verodostojnosti in odločnosti v odnosu do tretjih držav;

61. poudarja, da sta tako uredba o varstvu podatkov kot direktiva o varstvu podatkov nujno potrebni za zaščito temeljnih pravic posameznika, zato ju je treba obravnavati kot sveženj in ju sprejeti hkrati, da se zagotovi, da bodo vse dejavnosti obdelave podatkov v EU zagotavljale visoko raven varstva v vseh okoliščinah; poudarja, da bo nadaljnje ukrepe v zvezi s sodelovanjem na področju kazenskega pregona sprejel šele, ko bo Svet začel pogajanja s Parlamentom in Komisijo glede svežnja o varstvu podatkov;

62. opozarja, da pojma „vgrajene zasebnosti" in „privzete pravice do zasebnosti" krepita varstvo podatkov ter da bi morala imeti status vodila za vse izdelke, storitve in sisteme, ki so na voljo na internetu;

63. meni, da so višji standardi preglednosti in varnosti na spletnem in telekomunikacijskem področju nujno potrebni za boljšo ureditev varstva podatkov; zato poziva Komisijo, naj predstavi zakonodajni predlog o standardiziranih splošnih pogojih za spletne in telekomunikacijske storitve ter pooblasti nadzorni organ, ki bo spremljal spoštovanje splošnih pogojev;

Računalništvo v oblaku

64. ugotavlja, da so zgoraj omenjene prakse negativno vplivale na zaupanje v ameriško računalništvo v oblaku in ponudnike storitev v oblaku; zato poudarja, da je razvoj evropskih storitev v oblaku in rešitev IT bistven element za rast, zaposlovanje in zaupanje v storitve računalništva v oblaku in ponudnike teh storitev ter za zagotavljanje visoke ravni varstva osebnih podatkov;

65. poziva vse javne organe v Uniji, naj ne uporabljajo storitev v oblaku, če lahko zanje veljajo zakoni, ki niso zakoni EU;

66. ponovno izraža resne pomisleke v zvezi z obveznim neposrednim razkritjem osebnih podatkov in informacij iz EU, ki so bili obdelani v skladu s sporazumi o opravljanju storitev v oblaku, organom tretjih držav s strani ponudnikov storitev v oblaku, za katere velja zakonodaja tretjih držav ali ki uporabljajo strežnike za shranjevanje v tretjih državah, ter v zvezi z neposrednim dostopom organov kazenskega pregona in obveščevalnih služb tretjih držav na daljavo do obdelovanih osebnih podatkov in informacij;

67. obžaluje, da tak dostop do podatkov organi tretjih držav običajno izvedejo z neposredno izvršitvijo svojih pravnih predpisov, ne da bi uporabili mednarodne instrumente, vzpostavljene za pravno sodelovanje, kot so sporazumi o medsebojni pravni pomoči ali druge oblike pravosodnega sodelovanja;

68. poziva Komisijo in države članice, naj pospešijo delo za vzpostavitev evropskega partnerstva za računalništvo v oblaku ob polnem sodelovanju s civilno družbo in tehnično skupnostjo, na primer projektno skupino za internetno tehnologijo (IETF), ter vanj vključijo vidike varstva podatkov;

69. poziva Komisijo, naj pri pogajanjih o mednarodnih sporazumih, ki vključujejo obdelavo osebnih podatkov, upošteva zlasti tveganja in izzive, ki jih prinaša računalništvo v oblaku v zvezi s temeljnimi pravicami, predvsem, vendar ne izključno, v zvezi s pravico do zasebnosti in varstvom osebnih podatkov, kot je določeno v členih 7 in 8 Listine Evropske unije o temeljnih pravicah; poleg tega poziva Komisijo, naj upošteva notranje predpise pogajalskega partnerja, ki urejajo dostop služb kazenskega pregona in obveščevalnih služb do osebnih podatkov, obdelanih v okviru storitev računalništva v oblaku, zlasti z zahtevo, da je mogoče dostop odobriti le ob polnem spoštovanju sodnega postopka in na nedvoumni pravni podlagi in da se pogoji dostopa, namen tovrstnega dostopa, varnostni ukrepi, ki se izvajajo pri prevzemu podatkov, pravice posameznikov ter pravila glede nadzora in učinkovitih pravnih sredstev natančno opredelijo;

70. opozarja, da morajo vsa podjetja, ki ponujajo storitve v EU, brez izjeme spoštovati pravo EU in so odgovorna za vse kršitve, ter poudarja pomen učinkovitih, sorazmernih in odvračilnih upravnih sankcij, ki se lahko izrečejo ponudnikom storitev računalništva v oblaku, ki ne spoštujejo standardov za varstvo podatkov EU;

71. poziva Komisijo in pristojne organe držav članic, naj ocenijo, v kolikšni meri sta sodelovanje pravnih subjektov EU s tajnimi službami ali upoštevanje sodnih nalogov, ki so jih izdali organi tretjih držav in so v nasprotju z zakonodajo EU o varstvu podatkov zahtevali osebne podatke državljanov EU, kršila predpise EU o zasebnosti in varstvu podatkov;

72. poziva podjetja, ki ponujajo nove storitve z uporabo velikih količin podatkov, in nove aplikacije, kot je „internet stvari“, naj že v fazi razvoja vključijo ukrepe za varstvo podatkov in tako ohranijo visoko stopnjo zaupanja med državljani;

Čezatlantski sporazum o partnerstvu za trgovino in naložbe (TTIP)

73. se zaveda, da se EU in ZDA pogajata o Čezatlantskem partnerstvu za trgovino in naložbe, ki je strateško izjemno pomembno za zagotavljanje nadaljnje gospodarske rasti;

74. glede na pomembnost digitalnega gospodarstva v tem odnosu in z namenom ponovne vzpostavitve zaupanja med EU in ZDA odločno poudarja, da bi bila lahko privolitev Evropskega parlamenta v končni sporazum TTIP ogrožena, dokler se v celoti ne ustavijo dejavnosti vsesplošnega množičnega nadzora in prestrezanje komunikacij v institucijah in diplomatskih predstavništvih EU in dokler se ne najde ustrezna rešitev za pravice državljanov EU do zasebnosti podatkov,

vključno z upravnim in sodnim varstvom; poudarja, da lahko Parlament privoli v končni sporazum TTIP pod pogojem, da bo ta v celoti spoštoval med drugim temeljne pravice, ki jih priznava Listina EU o temeljnih pravicah, in da bo varstvo zasebnosti posameznikov v zvezi z obdelavo in posredovanjem osebnih podatkov še naprej urejal člen XIV sporazuma GATS; poudarja, da se pri izvajanju člena XIV sporazuma GATS zakonodaja EU o varstvu podatkov ne sme razumeti kot samovoljna ali neutemeljena diskriminacija;

Demokratični nadzor obveščevalnih služb

75. poudarja, da kljub dejstvu, da bi moral nadzor dejavnosti obveščevalnih služb temeljiti na demokratični legitimnosti (trdnem pravnem okviru, predhodni odobritvi in naknadnem preverjanju) ter ustrezni tehnični zmogljivosti in strokovnem znanju, večini nadzornih organov EU in ZDA v veliki meri primanjkuje obojega, zlasti tehničnih zmogljivosti;

76. kot je to storil v primeru Echelon, poziva vse nacionalne parlamente, ki tega še niso naredili, naj vzpostavijo resen nadzor nad obveščevalnimi dejavnostmi, ki ga bodo izvajali poslanci ali strokovni organi s pravnimi pooblastili za preiskovanje; poziva nacionalne parlamente, naj zagotovijo, da bodo imeli ti nadzorni odbori/organi dovolj virov, tehničnega strokovnega znanja in pravnih sredstev, vključno s pravico do nadzora na kraju samem, da bodo lahko učinkovito nadzirali obveščevalne službe;

77. poziva k vzpostavitvi skupine poslancev in strokovnjakov, ki bi na pregleden način in v sodelovanju z nacionalnimi parlamenti preučila priporočila za okrepljen demokratični nadzor obveščevalnih služb, vključno s parlamentarnim nadzorom, in okrepljeno sodelovanje pri nadzoru v EU, zlasti kar zadeva njegovo čezmejno razsežnost; meni, da bi morala skupina preučiti zlasti možnost minimalnih evropskih standardov ali smernic za (predhodni in naknadni) nadzor obveščevalnih služb na podlagi obstoječih najboljših praks in priporočil mednarodnih teles (ZN, Svet Evrope), vključno z vprašanjem, ali naj se nadzorni organi štejejo za tretje osebe na podlagi „pravila tretje osebe“ oziroma po načelu „nadzora organa izvora“, kar zadeva nadzor in odgovornost obveščevalnih podatkov tujih držav, merila za okrepljeno preglednost, oblikovana na podlagi splošnega načela dostopa do informacij in tako imenovanih „Tshwanskih načel“ ([1]), pa tudi načela, ki zadevajo omejitve trajanja in obsega vsakega nadzora ter zagotavljajo, da je ta nadzor sorazmeren glede na svoje namene in omejen nanje;

78. poziva to skupino, naj do začetka leta 2015 pripravi poročilo za konferenco Parlamenta z nacionalnimi nadzornimi organi, parlamentarnimi ali neodvisnimi, ter pomaga pri pripravah na to konferenco;

79. poziva države članice, naj se oprejo na najboljše prakse, da se izboljša dostop njihovih nadzornih organov do informacij o obveščevalnih dejavnostih (vključno z zaupnimi informacijami in informacijami iz drugih služb), ter določijo pooblastila za izvajanje nadzora na kraju samem in trden niz pristojnosti za izvajanje zaslišanj, priskrbijo ustrezne vire in tehnično strokovno znanje, zagotovijo popolno neodvisnost nadzornih organov od nacionalne vlade ter uvedejo obveznost poročanja nacionalnemu parlamentu;

80. poziva države članice, naj razvijejo sodelovanje med nadzornimi organi, zlasti v okviru Evropske mreže nacionalnih obveščevalnih nadzornikov (ENNIR);

81. poziva visoko predstavnico in podpredsednico, naj pristojnim organom Parlamenta redno pojasnjuje delovanje Centra Evropske unije za analizo obveščevalnih podatkov (IntCen), ki je del Evropske službe za zunanje delovanje, vključno s popolnim spoštovanjem temeljnih pravic in veljavnih predpisov EU o zasebnosti podatkov, s čimer bo omogočen izboljšan nadzor Parlamenta nad zunanjo razsežnostjo politik EU; poziva Komisijo ter visoko predstavnico in podpredsednico, naj predstavi predlog za pravno podlago delovanja centra IntCen, če so predvidene dejavnosti ali prihodnje pristojnosti na področju obveščevalnih podatkov ali lastnih zmogljivosti za zbiranje podatkov, ki bi lahko vplivale na strategijo EU za notranjo varnost;

([1]) The Global Principles on National Security and the Right to Information (Globalna načela o nacionalni varnosti in pravici do informacij), junij 2013.

82. poziva Komisijo, naj do decembra 2014 predstavi predlog za postopek pridobitve varnostne odobritve EU za vse funkcionarje EU, saj sedanji sistem, ki temelji na varnostni odobritvi s strani države članice, katere državljan je kandidat, vključuje različne zahteve in trajanja postopkov v nacionalnih sistemih, kar povzroča različno obravnavo poslancev Parlamenta in njihovega osebja glede na njihovo nacionalno pripadnost;

83. opozarja na določbe medinstitucionalnega sporazuma med Evropskim parlamentom in Svetom o pošiljanju tajnih podatkov Sveta o zadevah, ki niso s področja skupne zunanje in varnostne politike, Parlamentu in njihovi obdelavi s strani Evropskega parlamenta, saj bi bilo treba te določbe uporabiti za izboljšanje nadzora na ravni EU;

Agencije EU

84. poziva skupni nadzorni organ Europola in nacionalne organe za varstvo podatkov, naj pred koncem leta 2014 izvedejo skupen pregled, da se ugotovi, ali so nacionalni organi informacije in osebne podatke, izmenjane z Europolom, pridobili zakonito, še zlasti če so informacije ali podatke prvotno pridobile obveščevalne službe v EU ali tretji državi, in ali so sprejeti ustrezni ukrepi za preprečitev uporabe in nadaljnjega posredovanja takšnih informacij ali podatkov; meni, da Europol ne bi smel obdelovati informacij ali podatkov, pridobljenih s kršenjem temeljnih pravic, zagotovljenih z Listino o temeljnih pravicah;

85. poziva Europol, naj v skladu s svojim mandatom pozove pristojne organe držav članic, naj sprožijo kazenske preiskave večjih kibernetskih napadov in vdorov v informacijsko infrastrukturo z morebitnimi čezmejnimi posledicami; meni, da bi bilo treba mandat Europola spremeniti tako, da bi imel možnost sprožiti svojo lastno preiskavo v primeru suma zlonamernega napada na omrežne in informacijske sisteme dveh ali več držav članic ali organov Unije ([1]); poziva Komisijo, naj pregleda dejavnosti Europolovega Evropskega centra za boj proti kibernetski kriminaliteti (EC3) in pripravi predlog celovitega okvira za okrepitev njegovih pristojnosti;

Svoboda izražanja

86. izraža globoko zaskrbljenost glede čedalje večjih groženj za svobodo tiska in negativnega vpliva ustrahovanja s strani državnih organov na novinarje, zlasti kar zadeva zaščito zaupnosti novinarskih virov; ponovno poudarja pozive iz svoje resolucije z dne 21. maja 2013 z naslovom: „Listina EU: določitev standardov za svobodo medijev v EU“;

87. jemlje na znanje, da so britanske oblasti pridržale Davida Mirando in zasegle material, ki ga je posedoval, v skladu s Prilogo 7 britanskega zakona o terorizmu iz leta 2000 (in tudi zahtevale, da časnik The Guardian material uniči ali preda), ter izraža svojo zaskrbljenost, da ta dejanja predstavljajo morebiten resen poseg v pravico do svobode izražanja in svobode medijev, ki jo priznavata člen 10 EKČP in člen 11 Listine EU o temeljnih pravicah, in da je v takšnih razmerah mogoča zloraba zakonodaje, ki je namenjena boju proti terorizmu;

88. opozarja na težke razmere prijaviteljev nepravilnosti in njihovih podpornikov, vključno z novinarji, ki spremljajo njihova razkritja; poziva Komisijo, naj preuči vprašanje, ali naj prihodnji zakonodajni predlog za vzpostavitev učinkovitega in celovitega evropskega programa za zaščito prijaviteljev nepravilnosti, kot ga je Parlament že zahteval v resoluciji z dne 23. oktobra 2013, vsebuje tudi druga področja pristojnosti Unije, pri čemer je treba posebno pozornost posvetiti zapletenosti prijavljanja nepravilnosti na področju obveščevalnih dejavnosti; poziva države članice, naj temeljito preučijo možnost, da se prijaviteljem nepravilnosti dodeli mednarodna zaščita pred pregonom;

([1]) Stališče Evropskega parlamenta z dne 25. februarja 2014 o predlogu uredbe Evropskega parlamenta in Sveta o Agenciji Evropske unije za sodelovanje na področju kazenskega pregona in usposabljanja (Europol) (Srpejeta besedila, P7_TA(2014)0121).

89. poziva države članice, naj zagotovijo, da njihova zakonodaja zlasti na področju državne varnosti ponuja varno alternativo molčanju, kar zadeva razkrivanje ali prijavo nepravilnosti, vključno s korupcijo, kazenskimi dejanji, kršitvami zakonskih obveznosti, sodnimi zmotami in zlorabo položaja, kar je tudi v skladu z določbami različnih mednarodnih (OZN in Svet Evrope) instrumentov proti korupciji, načeli iz resolucije parlamentarne skupščine Sveta Evrope št. 1729(2010), Tshwanskimi načeli itd;

Informacijskotehnološka varnost EU

90. poudarja, da nedavni dogodki jasno kažejo veliko izpostavljenost EU, še zlasti institucij EU, nacionalnih vlad in parlamentov, velikih evropskih podjetij, evropske infrastrukture in omrežij IT, kompleksnim oblikam napadov z zapleteno programsko opremo, tudi zlonamerno; ugotavlja, da ti napadi zahtevajo tolikšne finančne in človeške vire, da verjetno prihajajo s strani državnih akterjev, ki delujejo v imenu tujih vlad; v tem okviru meni, da je primer vdora v telekomunikacijsko podjetje Belgacom oziroma prisluškovanja le-temu zaskrbljujoč primer napada na zmogljivosti IT Evropske unije; poudarja, da krepitev zmogljivosti in varnosti informacijskih tehnologij Evropske unije zmanjšuje ranljivost EU za resne kibernetske napade, za katere so odgovorne velike hudodelske združbe ali teroristične skupine;

91. meni, da se lahko razkritja o množičnem nadzoru, ki so sprožila to krizo, uporabijo kot priložnost, da Evropa prevzame pobudo in kot prednostni strateški ukrep vzpostavi močne in neodvisne ključne zmogljivosti IT; poudarja, da bi morala takšna evropska zmogljivost IT, da bi ponovno pridobila zaupanje, čim bolj temeljiti na odprtih standardih ter odprtokodni programski in, če je mogoče, tudi strojni opremi, da je celotna dobavna veriga, od zasnove procesorja do uporabniške ravni, jasna in pregledna; poudarja še, da je za obnovitev konkurenčnosti v strateškem sektorju storitev IT potreben „digitalni new deal“ s skupnimi in obsežnimi prizadevanji institucij EU, držav članic, raziskovalnih ustanov, industrije in civilne družbe; poziva Komisijo in države članice, naj uporabijo javno naročanje kot vzvod za podporo takšni razpoložljivosti virov IT v EU, tako da vključijo evropske standarde varnosti in zasebnosti kot ključno zahtevo pri javnih naročilih na področju blaga in storitev informacijske tehnologije; zato poziva Komisijo, naj pregleda trenutno prakso javnega naročanja na področju obdelave podatkov in preuči možnost, da bi javna naročila omejili samo na certificirana podjetja in po možnosti na podjetja iz EU, če gre za varnostne ali druge bistvene interese;

92. strogo obsoja dejstvo, da so obveščevalne službe poskušale znižati varnostne standarde IT in vgraditi stranska vrata v številne sisteme IT; poziva Komisijo, naj predstavi osnutek zakonodaje, ki bo organom pregona prepovedala uporabo stranskih vrat; zato priporoča uporabo odprtokodne programske opreme v vseh okoljih, v katerih je varnost IT pomembna;

93. poziva države članice, Komisijo, Svet in Evropski svet, naj v celoti, tudi prek financiranja raziskav in razvoja, podprejo razvoj evropskih inovativnih in tehnoloških zmogljivosti, kar zadeva orodja, podjetja in ponudnike informacijskih tehnologij (strojne in programske opreme, storitev in omrežij), tudi za namene kibernetske varnosti, ter šifrirnih in kriptografskih zmogljivosti; poziva vse pristojne institucije EU in države članice, naj vlagajo v lokalne in neodvisne tehnologije v EU ter množično razvijajo in povečujejo zmogljivosti odkrivanja;

94. poziva Komisijo, organe za standardizacijo in Evropsko agencijo za varnost omrežij in informacij, naj do decembra 2014 razvijejo minimalne standarde varnosti in zasebnosti ter smernice za sisteme, omrežja in storitve IT, vključno s storitvami računalništva v oblaku, da bodo osebni podatki državljanov EU in celovitost vseh sistemov IT bolje zaščiteni; meni, da bi takšni standardi lahko postali merilo za nove svetovne standarde in da je treba takšne standarde določiti z odprtim in demokratičnim postopkom, ki ga ne vodi ena sama država, subjekt ali multinacionalna družba; meni, da je treba upoštevati legitimne interese s področja kazenskega pregona in obveščevalnih dejavnosti, da se podpre boj proti terorizmu, vendar ti ne smejo pripeljati do splošnega spodkopavanja zanesljivosti vseh sistemov IT; podpira nedavno odločitev projektne skupine za internetno tehnologijo (IETF), da vključi vlade v model groženj za varnost na internetu;

95. poudarja, da so tako evropski kot nacionalni regulativni organi za telekomunikacije, v nekaterih primerih pa tudi telekomunikacijska podjetja, očitno zanemarili informacijskotehnološko varnost svojih uporabnikov in strank; poziva Komisijo, naj v celoti uporabi svoja obstoječa pooblastila v skladu z okvirno direktivo o e-zasebnosti in elektronskih komunikacijah, da se varstvo zaupnosti komunikacij okrepi s sprejetjem ukrepov za zagotovitev, da je terminalska oprema skladna s pravico uporabnikov, da nadzirajo in zaščitijo svoje osebne podatke, ter da se zagotovi visoka raven varnosti telekomunikacijskih omrežij in storitev, vključno z zahtevami po najsodobnejšem neprekinjenem šifriranju komunikacij;

96. podpira kibernetsko strategijo EU, vendar meni, da ne zajema vseh možnih nevarnosti in bi jo bilo treba razširiti, da bi zajemala zlonamerno ravnanje držav; poudarja potrebo po boljši informacijskotehnološki varnosti in odpornosti informacijskotehnoloških sistemov;

97. poziva Komisijo, naj najpozneje do januarja 2015 predloži akcijski načrt za razvoj večje neodvisnosti EU v sektorju IT, vključno z bolj usklajenim pristopom k spodbujanju evropskih tehnoloških zmogljivosti na področju informacijskih tehnologij (vključno s sistemi IT, opremo, storitvami, računalništvom v oblaku, šifriranjem in anonimizacijo) in k zaščiti kritične informacijske infrastrukture (vključno v smislu lastništva in ranljivosti);

98. poziva Komisijo, naj v okviru naslednjega delovnega načrta za program Obzorje 2020 nameni več sredstev krepitvi evropskih raziskav, razvoja, inovacij in usposabljanja na področju informacijskih tehnologij, zlasti tehnologij in infrastrukture za izboljšanje zasebnosti, kriptologije, varnega računalništva, najboljših varnostnih rešitev, vključno z odprtokodno varnostjo, in drugih storitev informacijske družbe, ter podpre notranji trg za evropsko programsko in strojno opremo, šifrirane komunikacije in komunikacijsko infrastrukturo, vključno z razvijanjem celovite industrijske strategije EU za informacijskotehnološko industrijo; meni, da imajo mala in srednja podjetja posebno vlogo v raziskovalnih dejavnostih; poudarja, da projektom, katerih namen je izključno razvijanje orodij za pridobitev nezakonitega dostopa v informacijskotehnološke sisteme, ne bi smeli dodeliti nobenih sredstev EU;

99. poziva Komisijo, naj začrta sedanje pristojnosti in najpozneje do decembra 2014 pregleda potrebe po širših pooblastilih, boljšem usklajevanju in/ali dodatnih virih in tehničnih zmogljivostih v Evropski agenciji za varnost omrežij in informacij, Europolovem Centru za boj proti kibernetski kriminaliteti in drugih centrih strokovnega znanja Unije, odzivnem centru za obravnavo omrežnih incidentov CERT-EU ter pri evropskem nadzorniku za varstvo podatkov, da se jim omogoči poglavitna vloga pri zaščiti evropskih komunikacijskih sistemov, večja učinkovitost pri preprečevanju in preiskovanju hujših vdorov v informacijsko infrastrukturo v EU in izvajanju (ali pomoči državam članicam in organom EU pri izvajanju) tehničnih preiskav na kraju samem v zvezi s hujšimi vdori v informacijsko infrastrukturo; še zlasti poziva Komisijo, naj preuči krepitev vloge Evropske agencije za varnost omrežij in informacij pri varovanju notranjih sistemov v institucijah EU ter da se znotraj njene strukture vzpostavi odzivni center za obravnavo omrežnih incidentov (CERT) za EU in njene države članice;

100. poziva Komisijo, naj preuči tudi potrebo po akademiji EU za informacijske tehnologije, ki bo združevala najboljše neodvisne evropske in mednarodne strokovnjake z vseh sorodnih področij in katere naloga bo zagotavljati znanstveno svetovanje o informacijskih tehnologijah, vključno s strategijami v zvezi z varnostjo, vsem ustreznim institucijam in organom EU;

101. poziva pristojne službe sekretariata Evropskega parlamenta, naj v okviru odgovornosti predsednika Parlamenta najpozneje do junija 2015, z vmesnim poročilom najpozneje do decembra 2014 opravijo temeljit pregled in oceno zanesljivosti informacijskotehnološke varnosti Parlamenta s poudarkom na: proračunskih sredstvih, kadrovskih virih, tehničnih zmogljivostih, notranji organizaciji in vseh pomembnih elementih, da se doseže visoka raven varnosti informacijskih sistemov Parlamenta; meni, da bi morala takšna ocena zagotoviti informacije, analizo in priporočila vsaj v zvezi s:

— potrebo po rednih, temeljitih in neodvisnih pregledih varnosti in testnih vdorih z izbiro zunanjih strokovnjakov za varnost, ki zagotavljajo preglednost in jamstva o njihovi verodostojnosti v odnosu do tretjih držav ali v zvezi s kakršnimi koli drugimi interesi;

— vključitvijo posebnih zahtev, ki izhajajo iz najboljše prakse, glede informacijskotehnološke varnosti ali zasebnosti v razpisne postopke za nove informacijske sisteme, vključno z možnostjo, da se kot pogoj za nakup zahteva odprtokodna programska oprema ali da se zahteva sodelovanje zaupanja vrednih evropskih podjetij, ko gre za občutljiva področja, povezana z varnostjo;

— seznamom podjetij, ki imajo sklenjeno pogodbo s Parlamentom na področju informacijskih tehnologij in telekomunikacij, ob upoštevanju vseh javno dostopnih informacij o njihovem sodelovanju z obveščevalnimi službami (npr. razkritij o pogodbah agencije NSA s podjetjem, kot je RSA, katerega izdelke uporablja Parlament z namenom varovanja dostopa poslancev in osebja EP do njihovih podatkov na daljavo), vključno z možnostjo, da bi iste storitve izvajala druga, po možnosti evropska podjetja;

— zanesljivostjo in odpornostjo programske opreme, zlasti serijske komercialne programske opreme, ki jo uporabljajo institucije EU v svojih informacijskih sistemih, kar zadeva vstope in posege s strani organov kazenskega pregona in obveščevalnih organov iz EU ali tretjih držav, upoštevajoč tudi ustrezne mednarodne standarde, načela najboljših praks pri upravljanju varnostnih tveganj in upoštevanje standardov EU o varnosti informacij v omrežjih glede kršitev varnosti;

— uporabo več odprtokodnih sistemov;

— ukrepi, ki jih je treba sprejeti za obravnavo vse večje uporabe mobilnih orodij (npr. službenih ali osebnih pametnih telefonov in tabličnih računalnikov), in vplivi te uporabe na informacijskotehnološko varnost sistema;

— varnostjo komunikacij med različnimi kraji dela Parlamenta in informacijskih sistemov, ki se uporabljajo v Parlamentu;

— uporabo in lokacijo strežnikov in informacijskotehnoloških centrov za informacijske sisteme Parlamenta ter posledicami za varnost in neoporečnost sistemov;

— dejanskim izvajanjem obstoječih pravil o kršitvah varnosti in takojšnjem obveščanju pristojnih organov s strani ponudnikov javno dostopnih telekomunikacijskih omrežij;

— koriščenjem storitev računalništva in shranjevanja v oblaku s strani Parlamenta, vključno z naravo podatkov, ki se shranjujejo v oblaku, zaščito vsebine in dostopa do njih in lokacijo strežnikov v oblaku, s čimer se pojasni, kateri pravni okvir za varstvo podatkov in obveščevalne dejavnosti se uporablja, in presojo možnosti, da bi uporabljali le tiste strežnike v oblaku, ki so na ozemlju EU;

— načrtom, ki omogoča uporabo več tehnologij šifriranja, zlasti neprekinjeno overjeno enkripcijo za vse informacijske in komunikacijske storitve, kot so računalništvo v oblaku, elektronska pošta, neposredna sporočila in telefonija;

— uporabo elektronskega podpisa v elektronski pošti;

— načrtom za uporabo privzetega standarda za šifriranje, kot je program GNU Privacy Guard, za elektronsko pošto, ki bi hkrati omogočal uporabo digitalnih podpisov;

— možnostjo vzpostavitve varne storitve neposrednih sporočil znotraj Parlamenta, ki bi omogočala varno komunikacijo, saj bi bila na strežniku razvidna samo šifrirana vsebina;

102. poziva vse institucije in agencije EU, naj v sodelovanju z Evropsko agencijo za varnost omrežij in informacij, Europolom in odzivnimi centri za obravnavo omrežnih incidentov opravijo podobne ocene najpozneje do junija 2015, z vmesnim poročilom do decembra 2014, zlasti Evropski svet, Svet, Evropsko službo za zunanje delovanje (vključno z delegacijami EU), Komisijo, Sodišče Evropske unije in Evropsko centralno banko; poziva države članice, naj opravijo podobno vrednotenje;

103. poudarja, da je treba v zvezi z zunanjim delovanjem EU izvesti ocene s tem povezanih proračunskih potreb in nemudoma sprejeti prve ukrepe v primeru Evropske službe za zunanje delovanje ter v predlogu proračuna za leto 2015 za ta namen dodeliti ustrezna sredstva;

104. meni, da se morajo večji informacijski sistemi, ki se uporabljajo na področju svobode, varnosti in pravice, kot so Schengenski informacijski sistem II, vizumski informacijski sistem, Eurodac in morebitni prihodnji sistemi, kot je EU-ESTA, razvijati in delovati na način, ki zagotavlja, da podatki niso ogroženi zaradi zahtev oblasti tretjih držav; poziva agencijo eu-LISA, naj poroča Parlamentu o zanesljivosti sedanjih sistemov do konca leta 2014;

105. poziva Komisijo in Evropsko službo za zunanje delovanje, naj ukrepata na mednarodni ravni, zlasti pri OZN, ter naj v sodelovanju z zainteresiranimi partnerji izvajata strategijo EU za demokratično upravljanje z internetom, da se preprečijo neupravičeni vplivi katerega koli posamičnega subjekta, podjetja ali države na dejavnosti organizacije ICANN in oddelka IANA z zagotavljanjem ustrezne zastopanosti vseh zainteresiranih strani v teh telesih, ob tem pa naj se izogneta spodbujanju državnega nadzora ali cenzure ter drobitvi interneta;

106. poziva EU, naj prevzame vodilno vlogo pri preoblikovanju strukture in upravljanja interneta, da bi obravnavali tveganja, ki izhajajo iz pretoka in hrambe podatkov, pri čemer bi si prizadevali za zmanjšanje količine podatkov, preglednost in manj centralizirano množično shranjevanje neobdelanih podatkov ter preusmerjanje internetnega prometa oziroma neprekinjeno šifriranje vsega internetnega prometa, da bi se izognili trenutnim tveganjem v zvezi z nepotrebnim usmerjanjem prometa prek ozemlja držav, ki ne izpolnjujejo osnovnih standardov na področju temeljnih pravic, varstva podatkov in zasebnosti;

107. poziva k spodbujanju:

— iskalnikov iz EU in družabnih omrežij iz EU kot pomembnega koraka v smeri neodvisnosti EU na področju informacijskih tehnologij;

— evropskih ponudnikov informacijskotehnoloških storitev;

— šifriranja komunikacij na splošno, vključno z elektronsko pošto in sporočili SMS;

— ključnih elementov evropskih informacijskih tehnologij, na primer rešitev za operacijske sisteme po modelu odjemalec/strežnik, uporabe odprtokodnih standardov, razvoja evropskih elementov za združevanje omrežij, npr. usmerjevalnikov;

108. poziva Komisijo, naj predlaga zakonski predlog za sistem usmerjanja v EU, ki bo vključeval obdelavo evidenc podatkov o klicih na ravni EU, bo podstruktura obstoječega interneta in ne bo segal čez meje EU; opozarja, da se morajo vsi podatki o usmerjanju in evidence podatkov o klicih obdelovati v skladu s pravnimi okviri EU;

109. poziva države članice, naj v sodelovanju z Evropsko agencijo za varnost omrežij in informacij, Europolovim centrom za boj proti kibernetski kriminaliteti, odzivnimi centri za obravnavo omrežnih incidentov, nacionalnimi organi za varstvo podatkov in enotami za kibernetsko kriminaliteto razvijejo kulturo varnosti in začnejo izvajati kampanjo za izobraževanje in ozaveščanje, da se državljanom omogoči bolj osveščeno odločanje o tem, katere osebne podatke dajejo na splet in kako jih lahko bolje zaščitijo, med drugim s šifriranjem in varnim računalništvom v oblaku, pri čemer naj v celoti uporabijo platformo za informacije v javnem interesu, kot predvideva direktiva o univerzalnih storitvah;

110. poziva Komisijo, naj do decembra 2014 predloži zakonodajne osnutke za spodbujanje proizvajalcev strojne in programske opreme, da bi uvedli več varnosti in zasebnosti v svoje izdelke s pomočjo vgrajenih in privzetih značilnosti, in sicer z uvedbo odvračalnih ukrepov za neupravičeno in nesorazmerno množično zbiranje osebnih podatkov in pravne odgovornosti proizvajalca za znane ranljive točke, za katere niso priskrbeli popravkov, pomanjkljive ali nezanesljive izdelke ali vgradnjo skrivnih stranskih vrat, ki omogočajo nedovoljen dostop do podatkov in njihovo obdelavo; s tem v zvezi poziva Komisijo, naj oceni možnost vzpostavitve sistema za certificiranje ali potrjevanje informacijske strojne opreme, vključno s postopki preskušanja na ravni EU, da se zagotovita celovitost in varnost izdelkov;

Ponovna vzpostavitev zaupanja

111. meni, da se je v preiskavi poleg potrebe po zakonodajnih spremembah pokazala potreba po tem, da ZDA ponovno vzpostavijo zaupanje v odnosu s svojimi partnericami v EU, saj so pod vprašajem predvsem dejavnosti ameriških obveščevalnih agencij;

112. poudarja, da se je povzročena kriza zaupanja razširila na:

— duh sodelovanja znotraj EU, saj lahko nekatere državne obveščevalne dejavnosti ogrozijo doseganje ciljev Unije;

— državljane, ki ugotavljajo, da morebiti za njimi vohunijo ne le tretje države ali multinacionalne družbe, ampak tudi njihova lastna vlada;

— spoštovanje temeljnih pravic, demokracije in pravne države ter verodostojnost demokratičnih, sodnih in parlamentarnih zaščitnih ukrepov in nadzora v digitalni družbi;

Med EU in ZDA

113. opozarja na pomembno zgodovinsko in strateško partnerstvo med državami članicami EU in ZDA, ki temelji na skupnem zaupanju v demokracijo, pravno državo in temeljne pravice;

114. meni, da sta množični nadzor državljanov in vohunjenje za političnimi voditelji s strani ZDA povzročila resno škodo v odnosih med EU in ZDA ter negativno vplivala na zaupanje v organizacije ZDA, ki delujejo v EU; ti učinki so še stopnjevani zaradi pomanjkanja sodnih in upravnih sredstev za pritožbo v pravu ZDA za državljane EU, zlasti v primerih dejavnosti nadzora v obveščevalne namene;

115. v luči globalnih izzivov, s katerimi se soočata EU in ZDA, priznava, da je treba čezatlantsko partnerstvo še okrepiti in da je bistveno, da se čezatlantsko sodelovanje v boju proti terorizmu nadaljuje na novi osnovi zaupanja, ki temelji na resničnem skupnem spoštovanju načela pravne države in zavračanju vseh vsesplošnih praks množičnega nadzora; zato vztraja, da morajo ZDA sprejeti jasne ukrepe, da se ponovno vzpostavi zaupanje in se znova poudarijo osnovne skupne vrednote, na katerih temelji partnerstvo;

116. se je pripravljen vključiti v dialog z ustreznimi organi ZDA, da bi v ameriški javni in kongresni razpravi o reformi nadzora in pregledu kontrole obveščevalnih služb, ki trenutno poteka, zagotovili upoštevanje pravice do zasebnosti in drugih pravic državljanov EU, prebivalcev ali drugih oseb, ki jih ščiti pravo EU, ter enake pravice do obveščenosti in do zaščite zasebnosti na sodiščih ZDA, vključno s pravnimi sredstvi, na primer z revizijo zakona o zasebnosti in zakona o zasebnosti elektronskih komunikacij ter z ratifikacijo prvega izbirnega protokola k Mednarodnemu paktu o državljanskih in političnih pravicah (ICCPR), da bi s tem odpravili sedanjo diskriminacijo;

117. vztraja, da se je treba lotiti nujnih reform in Evropejcem zagotoviti učinkovita jamstva, da bo uporaba nadzora in obdelave podatkov za namene zbiranja obveščevalnih podatkov iz tujine sorazmerna in omejena z jasno opredeljenimi pogoji ter povezana z utemeljenim sumom ali utemeljenim razlogom v zvezi s teroristično dejavnostjo; poudarja, da mora biti ta razlog predmet preglednega sodnega nadzora;

118. meni, da morajo naši ameriški partnerji izraziti jasne politične znake, ki bodo pokazali, da ZDA razlikujejo med zavezniki in nasprotniki;

119. poziva Komisijo in vlado ZDA, naj v okviru pogajanj, ki trenutno potekajo o krovnem sporazumu med EU in ZDA o prenosu podatkov za namene kazenskega pregona, obravnavata pravice državljanov EU do obveščenosti in sodnega varstva ter zaključita ta pogajanja pred poletjem 2014 v skladu z zavezo, ki sta jo sprejeli na srečanju ministrov za pravosodje in notranje zadeve EU–ZDA dne 18. novembra 2013;

120. spodbuja ZDA, naj pristopi h Konvenciji Sveta Evrope o varstvu posameznikov pri avtomatski obdelavi osebnih podatkov (Konvencija 108), kot je pristopila h Konvenciji o kibernetski kriminaliteti iz leta 2001, ter tako okrepi skupno pravno podlago čezatlantskih zaveznic;

121. poziva institucije EU, naj raziščejo možnosti za oblikovanje kodeksa ravnanja skupaj z ZDA, ki bi zagotavljal, da ZDA ne bodo izvajale vohunjenja proti institucijam in zmogljivostim EU;

V Evropski uniji

122. meni tudi, da so vpletenost in dejavnosti držav članic EU pripeljale do izgube zaupanja tako med državami članicami kot med državljani EU in njihovimi nacionalnimi organi; meni, da je mogoče samo s popolno jasnostjo namenov in sredstev nadzora, javno razpravo in, navsezadnje, revizijo zakonodaje in prenehanjem dejavnosti množičnega nadzora in krepitvijo sistema pravosodnega in parlamentarnega nadzora ponovno vzpostaviti izgubljeno zaupanje; ponovno izpostavlja težave pri razvoju celovite varnostne politike EU zaradi delovanja tovrstnih dejavnosti množičnega nadzora ter poudarja, da se morajo po načelu lojalnega sodelovanja Evropske unije države članice vzdržati izvajanja obveščevalnih dejavnosti na ozemlju drugih držav članic;

123. ugotavlja, da si nekatere države članice prizadevajo za dvostransko sporazumevanje z organi ZDA o domnevah glede vohunjenja in da so nekatere sklenile (Združeno kraljestvo) ali nameravajo skleniti (Nemčija, Francija) tako imenovane dogovore „proti vohunjenju“; poudarja, da morajo te države članice v celoti upoštevati interese in zakonodajni okvir EU kot celote; meni, da imajo tovrstni dvostranski dogovori nasprotni učinek od želenega in da so nebistveni, saj je za to problematiko potrebna rešitev na evropski ravni; poziva Svet, naj obvešča Parlament o razvoju dogodkov med državami članicami glede dogovora o vzajemnem nevohunjenju, ki bo veljal za vso Evropsko unijo;

124. meni, da takšni dogovori ne bi smeli kršiti Pogodb Evropske unije, zlasti načela lojalnega sodelovanja (iz člena 4(3) PEU), ali spodkopavati politik EU na splošno in, konkretneje, v zvezi z notranjim trgom, pošteno konkurenco ter gospodarskim, industrijskim in družbenim razvojem; je sklenil, da bo pregledal skladnost takšnih dogovorov z evropskim pravom, in si pridržuje pravico do sprožitve postopkov iz Pogodb v primeru, da se dokaže, da takšni dogovori nasprotujejo koheziji Unije ali temeljnim načelom, na katerih temelji EU;

125. poziva države članice, naj v sodelovanju z ustreznimi organi in agencijami EU storijo vse za boljše sodelovanje pri oblikovanju zaščite pred vohunjenjem za zaščito državljanov in institucij EU, evropskih podjetij, industrije ter informacijske infrastrukture in omrežij, kot tudi evropskih raziskav; meni, da je dejavno sodelovanje zainteresiranih strani iz EU pogoj za uspešno izmenjavo informacij; poudarja, da so varnostna tveganja postala bolj mednarodna, razpršena in kompleksna, kar zahteva krepitev evropskega sodelovanja; meni, da bi morale Pogodbe bolje odražati ta razvoj dogodkov, zato poziva k reviziji Pogodb, da bi okrepili idejo lojalnega sodelovanja med državami članicami in Unijo, kar zadeva vzpostavitev območja varnosti, in preprečili vohunjenje držav članic za drugimi državami članicami v Uniji;

126. meni, da so v vseh ustreznih institucijah in delegacijah EU absolutno potrebne komunikacijske strukture (elektronska pošta in telekomunikacije, vključno s stacionarnimi in prenosnimi telefoni) in sejne sobe, ki jim ni mogoče prisluškovati; zato poziva k oblikovanju šifriranega sistema EU za notranjo elektronsko pošto;

127. poziva Svet in Komisijo, naj brez odlašanja odobrita predlog Evropskega parlamenta z dne 23. maja 2012 o uredbi Evropskega parlamenta o podrobnih določbah o uresničevanju pravice Evropskega parlamenta do preiskave in razveljavitvi Sklepa 95/167/ES, Euratom, ESPJ Evropskega parlamenta, Sveta in Komisije, predstavljen na podlagi člena 226 PDEU; poziva k reviziji Pogodb, da bi takšna pooblastila o preiskavi razširili, da bi brez omejitev ali izjem vključevala vsa področja pristojnosti ali dejavnosti Unije in možnost zaslišanja pod prisego;

Na mednarodni ravni

128. poziva Komisijo, naj najpozneje januarja 2015 predstavi strategijo EU za demokratično upravljanje interneta;

129. poziva države članice, naj se odzovejo pozivu 35. mednarodne konference komisarjev za varstvo podatkov in zasebnost ter zagovarjajo sprejetje dodatnega protokola k členu 17 Mednarodnega pakta o državljanskih in političnih pravicah (ICCPR), ki bi moral temeljiti na standardih, ki jih je razvila in sprejela mednarodna konferenca, ter na določbah splošne opombe odbora za človekove pravice št. 16 k paktu, da bi se oblikovali svetovno veljavni standardi za varstvo podatkov in zaščito zasebnosti v skladu z načelom pravne države; poziva države članice, naj se pri tem zavzemajo za mednarodno agencijo OZN, odgovorno zlasti za spremljanje novih orodij za nadzor ter za reguliranje in raziskovanje njihove uporabe; poziva visoko predstavnico in podpredsednico Komisije ter Evropsko službo za zunanje delovanje, naj zavzameta proaktivno stališče;

130. poziva države članice, naj razvijejo usklajeno in trdno strategijo znotraj OZN, ki bo podpirala zlasti resolucijo o „pravici do zasebnosti v digitalni dobi“, ki sta jo predlagali Brazilija in Nemčija, sprejel pa jo je tretji odbor generalne skupščine OZN (odbor za človekove pravice) dne 27. novembra 2013, ter nadalje ukrepala v obrambo temeljne pravice do zasebnosti in varstva podatkov na mednarodni ravni, obenem pa se izognila spodbujanju državnega nadzora ali cenzure ter drobitvi interneta, vključno s pobudo za mednarodno pogodbo, s katero bi prepovedali dejavnosti množičnega nadzora, in za agencijo za nadzor te pogodbe;

Načrt prednostnih nalog: Evropski digitalni habeas corpus – varstvo temeljnih pravic v digitalni dobi

131. sklene, da bo državljanom, institucijam in državam članicam EU predložil navedena priporočila kot načrt prednostnih nalog za naslednje zakonodajno obdobje; poziva Komisijo ter druge institucije, organe, urade in agencije EU, ki so omenjeni v tej resoluciji, v skladu s členom 265 PDEU, naj ukrepajo na podlagi priporočil in pozivov iz te resolucije;

132. sklene, da bo vzpostavil institut „Evropski digitalni habeas corpus – za varstvo temeljnih pravic v digitalni dobi“ na podlagi naslednjih osmih ukrepov z Evropskim parlamentom kot nadzornikom njihovega izvajanja:

— Ukrep 1: sprejetje svežnja ukrepov za varstvo podatkov v letu 2014;

— Ukrep 2: sklenitev krovnega sporazuma med EU in ZDA, ki bo jamčil temeljno pravico državljanov do zasebnosti in varstva podatkov ter zagotovil ustrezna pravna sredstva za državljane EU, tudi v primeru prenosa podatkov iz EU v ZDA za namene kazenskega pregona;

— Ukrep 3: prenehanje izvajanja sporazuma o varnem pristanu, dokler se ne opravi popoln pregled in odpravijo sedanje vrzeli ter se zagotovi, da prenos podatkov iz Unije v ZDA v komercialne namene lahko poteka samo v skladu z najstrožjimi standardi EU;

— Ukrep 4: prenehanje izvajanja sporazuma TFTP, dokler se ne (i) zaključijo pogajanja o krovnem sporazumu; (ii) in dokler se ne opravi temeljita preiskava na podlagi analize EU in ustrezno rešijo vsi pomisleki, ki jih je izrazil Parlament v svoji resoluciji z dne 23. oktobra 2013;

— Ukrep 5: ocena vseh sporazumov, mehanizmov ali izmenjav s tretjimi državami, ki vključujejo osebne podatke, da se zagotovi, da pravica do zasebnosti in varstva osebnih podatkov ni kršena zaradi dejavnosti nadzora, ter sprejetje potrebnih nadaljnjih ukrepov;

— Ukrep 6: zaščita načela pravne države in temeljnih pravic državljanov EU, (vključno z zaščito svobode tiska pred grožnjami) pravice javnosti do nepristranskih informacij in poklicne tajnosti (vključno z odnosi med odvetnikom in stranko) ter okrepljena zaščita prijaviteljev nepravilnosti;

— Ukrep 7: razvoj evropske strategije za večjo informacijskotehnološko neodvisnost („digitalni new deal“), ki vključuje dodelitev ustreznih sredstev na nacionalni ravni in ravni EU, kar bo spodbudilo informacijsko industrijo in evropskim podjetjem omogočilo izkoriščanje konkurenčne prednosti EU na področju zasebnosti;

— Ukrep 8: razvoj EU kot referenčnega akterja za demokratično in nevtralno upravljanje interneta;

133. poziva institucije EU in države članice, naj spodbujajo evropski digitalni habeas corpus za varstvo temeljnih pravic v digitalni dobi; se obvezuje, da bo deloval kot zastopnik pravic državljanov EU, izvajanje pa bo spremljal s pomočjo naslednjega časovnega razporeda:

— od aprila 2014 do marca 2015: spremljevalna skupina na podlagi preiskovalne ekipe odbora LIBE, odgovorna za spremljanje morebitnih novih razkritij v zvezi z nalogami preiskave in za nadzor izvajanja te resolucije;

— od julija 2014: trajen nadzorni mehanizem za prenos podatkov in pravna sredstva znotraj pristojnega odbora;

— spomladi 2014: uradni poziv Evropskemu svetu, naj vključi „evropski digitalni habeas corpus – varstvo temeljnih pravic v digitalni dobi“ v smernice, ki jih je treba sprejeti v skladu s členom 68 PDEU;

— jeseni 2014: zaveza, da bodo „evropski digitalni habeas corpus – varstvo temeljnih pravic v digitalni dobi“ in s tem povezana priporočila služili kot ključna merila za potrditev prihodnje Komisije;

— 2014: konferenca, ki bo združila evropske strokovnjake na visoki ravni z različnih področij, ki prispevajo k informacijskotehnološki varnosti (vključno z matematiko, kriptografijo in tehnologijami za boljše varovanje zasebnosti), da bi pripomogli k spodbujanju informacijskotehnološke strategije EU za naslednje zakonodajno obdobje;

— 2014-2015: Evropski parlament in kongres ZDA bosta redno sklicevala skupino za zaupanje/podatke/pravice državljanov, vključeni pa bodo tudi drugi zainteresirani parlamenti tretjih držav, vključno z brazilskim;

— 2014-2015: konferenca z organi za nadzor obveščevalnih služb iz evropskih nacionalnih parlamentov;

o

o o

134. naroči svojemu predsedniku, naj to resolucijo posreduje Evropskemu svetu, Svetu, Komisiji, parlamentom in vladam držav članic, nacionalnim organom za varstvo podatkov, evropskemu nadzorniku za varstvo podatkov, agenciji eu-LISA, Evropski agenciji za varnost omrežij in informacij, Agenciji za temeljne pravice, delovni skupini iz člena 29, Svetu Evrope, kongresu Združenih držav Amerike, vladi ZDA, predsednici, vladi in parlamentu Federativne republike Brazilije ter generalnemu sekretarju OZN;

135. naroči svojemu Odboru za državljanske svoboščine, pravosodje in notranje zadeve, naj to zadevo predstavi na plenarnem zasedanju Parlamenta leto dni po sprejetju te resolucije; meni, da je bistveno oceniti, v kakšnem obsegu so bila upoštevana priporočila, ki jih je sprejel Parlament, in analizirati morebitne primere, ko ta priporočila niso bila upoštevana.