Srijeda, 12. ožujka 2014.

P7_TA(2014)0230

Program nadzora američke Nacionalne sigurnosne agencije (NSA), nadzorna tijela u različitim državama članicama i njihov utjecaj na temeljna prava građana EU-a

Rezolucija Europskog parlamenta od 12. ožujka 2014. o programu nadzora Agencije za nacionalnu sigurnost SAD-a (NSA), nadzornim tijelima u različitim državama članicama i njihovu utjecaju na temeljna prava građana EU-a te o transatlantskoj suradnji u pravosuđu i unutarnjim poslovima (2013/2188(INI))

(2017/C 378/14)

Europski parlament,

— uzimajući u obzir Ugovor o Europskoj uniji (UEU), a posebno njegove članke 2., 3., 4., 5., 6., 7., 10., 11. i 21.,

— uzimajući u obzir Ugovor o funkcioniranju Europske unije (UFEU), a posebno njegove članke 15., 16. i 218. te glavu V.,

— uzimajući u obzir Protokol br. 36 o prijelaznim odredbama i njegov članak 10. te Deklaraciju 50. o tom protokolu,

— uzimajući u obzir Povelju o temeljnim pravima Europske unije, a posebno njezine članke 1., 3., 6., 7., 8., 10., 11., 20., 21., 42., 47., 48. i 52.,

— uzimajući u obzir Europsku konvenciju o ljudskim pravima, a posebno njezine članke 6., 8., 9., 10. i 13. te njezine protokole,

— uzimajući u obzir Opću deklaraciju o ljudskim pravima, a posebno njezine članke 7., 8., 10., 11., 12. i 14. ([1]),

— uzimajući u obzir Međunarodni pakt o građanskim i političkim pravima, a posebno njegove članke 14., 17., 18. i 19.,

— uzimajući u obzir Konvenciju Vijeća Europe o zaštiti podataka (ETS br. 108) i Dodatni protokol od 8. studenog 2001. uz Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi s nadzornim tijelima i prekograničnom protoku podataka (ETS br. 181),

— uzimajući u obzir Bečku konvenciju o diplomatskim odnosima, a posebno njezine članke 24., 27. i 40.,

— uzimajući u obzir Konvenciju Vijeća Europe o kibernetičkom kriminalu (ETS br. 185),

— imajući u obzir izvješće posebnog izvjestitelja UN-a o promicanju i zaštiti ljudskih prava i temeljnih sloboda u borbi protiv terorizma, koje je podneseno 17. svibnja 2010. ([2]),

— uzimajući u obzir komunikaciju Komisije „Internetska politika i upravljanje internetom – uloga Europe u oblikovanju budućnosti upravljanja internetom”(COM(2014)0072);

— uzimajući u obzir izvješće posebnog izvjestitelja UN-a o promicanju i zaštiti prava na slobodu mišljenja i izražavanja, koje je podneseno 17. travnja 2013. ([3]),

— uzimajući u obzir Smjernice o ljudskim pravima i borbi protiv terorizma koje je donio Odbor ministara Vijeća Europe 11. srpnja 2002.,

([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

— uzimajući u obzir Deklaraciju iz Bruxellesa od 1. listopada 2010., donesenu na 6. konferenciji parlamentarnih odbora za nadzor nad radom obavještajno-sigurnosnih službi država članica Europske unije,

— uzimajući u obzir Rezoluciju Parlamentarne skupštine Vijeća Europe br. 1954 (2013) o nacionalnoj sigurnosti i pristupu informacijama,

— uzimajući u obzir izvješće o demokratskom nadzoru sigurnosnih službi koje je donijela Venecijanska komisija 11. lipnja 2007. ([1]) te očekujući s velikim interesom njegovo ažuriranje planirano za proljeće 2014.,

— uzimajući u obzir svjedočenja predstavnika nadzornih odbora za obavještajne službe iz Belgije, Nizozemske, Danske i Norveške,

— uzimajući u obzir postupke pokrenute pred francuskim ([2]), poljskim i britanskim ([3]) sudovima te pred Europskim sudom za ljudska prava ([4]) u vezi sa sustavima masovnog nadzora,

— uzimajući u obzir Konvenciju o uzajamnoj pravnoj pomoći u kaznenim stvarima među državama članicama Europske unije, koju je donijelo Vijeće u skladu s člankom 34. Ugovora o Europskoj uniji ([5]), a posebno njezinu glavu III.

— uzimajući u obzir Odluku Komisije 2000/520/EZ od 26. srpnja 2000. o primjerenosti zaštite koju pružaju načela privatnosti sigurne luke i uz njih vezana često postavljana pitanja koje je izdalo Ministarstvo trgovine SAD-a,

— uzimajući u obzir izvješća Komisije o ocjeni primjene načela privatnosti sigurne luke od 13. veljače 2002. (SEC(2002)0196) i od 20. listopada 2004. (SEC(2004)1323),

— uzimajući u obzir Komunikaciju Komisije od 27. studenog 2013. o funkcioniranju sigurne luke iz perspektive građana EU-a i poduzeća s poslovnim nastanom u Europskoj uniji (COM(2013)0847) i Komunikaciju Komisije od 27. studenog 2013. o ponovnoj uspostavi povjerenja u protok podataka između EU-a i SAD-a (COM(2013)0846),

— uzimajući u obzir svoju Rezoluciju od 5. srpnja 2000. o nacrtu Odluke Komisije o primjerenosti zaštite koju pružaju načela privatnosti sigurne luke i uz njih vezana često postavljana pitanja koje je izdalo Ministarstvo trgovine SAD-a ([6]), u kojoj je zauzeto stajalište da se primjerenost sustava ne može potvrditi, te uzimajući u obzir mišljenja Radne skupine iz članka 29., a posebno Mišljenje 4/2000 od 16. svibnja 2000. ([7]),

— uzimajući u obzir sporazume između Sjedinjenih Američkih Država i Europske unije o korištenju i prijenosu podataka iz evidencije podataka o putnicima (Sporazum o PNR-u) iz 2004., 2007. ([8]) i 2012. ([9]),

— uzimajući u obzir zajedničku reviziju provedbe Sporazuma između EU-a i SAD-a o obradi i prijenosu podataka iz zapisnika imena putnika Ministarstvu domovinske sigurnosti SAD-a ([10]), uz izvješće Komisije Europskom parlamentu i Vijeću o zajedničkoj reviziji (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 and La Ligue française pour la défense des droits de l'Homme et du Citoyen v. X; Tribunal de Grande Instance of Paris.
([3]) Predmeti Privacy Internationala i Libertyja pred Sudom za istražne ovlasti.
([4]) Zajednička tužba u skladu s člankom 34. koji su podnijeli Big Brother Watch, Open Rights Group, English Pen Dr Constanze Kurz (tužitelji) protiv Ujedinjene Kraljevine (tuženik).
([5]) SL C 197, 12.7.2000., str. 1.
([6]) SL C 121, 24.4.2001., str. 152.
([7]) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp32en.pdf
([8]) SL L 204, 4.8.2007., str. 18.
([9]) SL L 215, 11.8.2012., str. 5.
([10]) SEC(2013)0630, 27.11.2013.

Srijeda, 12. ožujka 2014.

— uzimajući u obzir mišljenje nezavisnog odvjetnika Cruza Villalóna u kojem je zaključio da Direktiva 2006/24/EZ o zadržavanju podataka dobivenih ili obrađenih u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža nije u skladu s člankom 52. stavkom 1. Povelje o temeljnim pravima Europske unije i da članak 6. te Direktive nije u skladu s člankom 7. i člankom 52. stavkom 1. Povelje ([1]),

— uzimajući u obzir Odluku Vijeća 2010/412/EU od 13. srpnja 2010. o sklapanju Sporazuma između Europske unije i Sjedinjenih Američkih Država o obradi i slanju podataka o izvješćima u vezi s financijskim plaćanjima iz Europske unije Sjedinjenim Američkim Državama za potrebe Programa za praćenje financiranja terorizma (TFTP) ([2]) te popratne izjave Komisije i Vijeća,

— uzimajući u obzir Sporazum o uzajamnoj pravnoj pomoći između Europske unije i Sjedinjenih Američkih Država ([3]),

— uzimajući u obzir tekuće pregovore o okvirnom sporazumu između EU-a i SAD-a o zaštiti osobnih podataka koji se šalju i obrađuju radi sprečavanja, istraživanja i otkrivanja kaznenih djela te kaznenog gonjenja zbog takvih djela, uključujući terorizam, u okviru policijske i sudske suradnje u kaznenim stvarima („Krovni sporazum”),

— uzimajući u obzir Uredbu Vijeća (EZ) br. 2271/96 od 22. studenog 1996. o zaštiti od učinaka izvanteritorijalne primjene zakonodavstva koje donese treća zemlja i djelovanja koja se temelje na tom zakonodavstvu ili iz njega proizlaze ([4]),

— uzimajući u obzir izjavu predsjednika Savezne Republike Brazil na otvaranju 68. zasjedanja Opće skupštine UN-a 24. rujna 2013. i rad Parlamentarnog odbora za istragu o špijunaži koji je osnovo Savezni senat Brazila,

— uzimajući u obzir Zakon o patriotizmu SAD-a (USA PATRIOT Act) koji je potpisao predsjednik George W. Bush 26. listopada 2001.,

— uzimajući u obzir Zakon o nadzoru stranih obavještajnih službi (FISA) iz 1978. i Zakon o izmjenama FISA-e iz 2008.,

— uzimajući u obzir izvršni nalog br.12333 koji je 1981. izdao Predsjednik SAD-a i koji je izmijenjen 2008.,

— uzimajući u obzir Predsjednički ukaz (PPD-28) o aktivnostima prikupljanja informacija o sredstvima veze koji je predsjednik SAD-a Barack Obama donio 17. siječnja 2014.,

— uzimajući u obzir zakonodavne prijedloge koji se trenutno razmatraju u Kongresu SAD-a, uključujući nacrt Zakona o slobodi SAD-a, nacrt Zakona o kontroli obavještajnog djelovanja i reformi nadzora i druge dokumente,

— uzimajući u obzir revizije koje su proveli Odbor za nadzor privatnosti i građanskih sloboda, Vijeće za nacionalnu sigurnost SAD-a i predsjednikova Skupina za preispitivanje obavještajnih i komunikacijskih tehnologija, a posebno izvješće te skupine od 12. prosinca 2013. pod nazivom „Sloboda i sigurnost u svijetu koji se mijenja”,

— uzimajući u obzir odluku Okružnog suda Sjedinjenih država za Okrug Kolumbija, Klayman i ostali protiv Obame i ostalih, građanski postupak br. 13-0851 od 16. prosinca 2013., i odluku Okružnog suda Sjedinjenih država za Južni okrug New Yorka, ACLU i ostali protiv Jamesa R. Clappera i ostalih, građanski postupak br. 13-3994 od 11. lipnja 2013.,

— uzimajući u obzir izvješće o nalazima supredsjedatelja EU-a ad hoc radnom skupinom između EU-a i SAD-a o zaštiti podataka od 27. studenog 2013. ([5]),

([1]) Mišljenje nezavisnog odvjetnika Cruza Villalóna, 12. prosinca 2013., predmet C- 293/12.
([2]) SL L 195, 27.7.2010., str. 3.
([3]) SL L 181, 19.7.2003., str. 34.
([4]) SL L 309, 29.11.1996., str.1.
([5]) Dokument Vijeća 16987/2013.

— uzimajući u obzir svoje rezolucije od 5. rujna 2001. ([1]) i 7. studenog 2002. ([2]) o postojanju globalnog sustava za presretanje privatnih i poslovnih komunikacija (Sustav za presretanje ECHELON),

— uzimajući u obzir svoju Rezoluciju od 21. svibnja 2013. o Povelji EU-a: utvrđene norme za slobodu medija diljem EU-a ([3]),

— uzimajući u obzir svoju Rezoluciju od 4. srpnja 2013. o programu nadzora Agencije za nacionalnu sigurnost SAD-a, obavještajnim službama u raznim državama članicama i njihovu utjecaju na privatnost građana EU-a ([4]), u kojoj je zatražio od svog Odbora za građanske slobode, pravosuđe i unutarnje poslove da provede detaljnu istragu o tom predmetu,

— uzimajući u obzir radni dokument 1. o programima nadzora SAD-a i EU-a i njihovu utjecaju na temeljna prava građana EU-a,

— uzimajući u obzir radni dokument 3. o odnosu između nadzornih praksi u EU-u i SAD-u te propisima EU-a o zaštiti podataka,

— uzimajući u obzir radni dokument 4. o nadzornim aktivnostima SAD-a u pogledu podataka EU-a te o njihovu mogućem pravnom učinku na transatlantske sporazume i suradnju,

— uzimajući u obzir radni dokument 5. o demokratskom nadzoru obavještajnih službi država članica i obavještajnih tijela EU-a,

— uzimajući u obzir radni dokument Odbora AFET o vanjskopolitičkim aspektima istrage o elektroničkom masovnom nadzoru građana EU-a;

— uzimajući u obzir svoju Rezoluciju od 23. listopada 2013. o organiziranom kriminalu, korupciji i pranju novca: preporuke za radnje i inicijative koje treba poduzeti ([5]),

— uzimajući u obzir svoju Rezoluciju od 23. listopada 2013. o suspenziji Sporazuma o programu za praćenje financiranja terorizma (TFTP) zbog nadzora Agencije za nacionalnu sigurnost SAD-a ([6]),

— uzimajući u obzir svoju Rezoluciju od 10. prosinca 2013. o ostvarivanju potencijala računalstva u oblaku u Europi ([7]),

— uzimajući u obzir međuinstitucionalni sporazum između Europskog parlamenta i Vijeća o slanju Europskom parlamentu klasificiranih podataka Vijeća, a koji se odnose na predmete koji nisu iz područja zajedničke vanjske i sigurnosne politike ([8]),

— uzimajući Prilog VIII. Poslovniku,

— uzimajući u obzir članak 48. Poslovnika,

— uzimajući u obzir izvješće Odbora za građanske slobode, pravosuđe i unutarnje poslove (A7-0139/2014),

Učinak masovnog nadzora

A. budući da su zaštita podataka i privatnost temeljna prava; budući da se stoga sigurnosne mjere, uključujući one protiv terorizma, moraju provoditi kroz vladavinu prava te da moraju biti predmetom obveza povezanih s temeljnim pravima, uključujući one koje se odnose na privatnost i zaštitu podataka;

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

Srijeda, 12. ožujka 2014.

B. budući da je potrebno da protoci informacija i podaci, koji danas prevladavaju u svakodnevnom životu i sastavni su dio integriteta svake osobe, budu sigurni od neovlaštenih ulazaka kao što su to privatni domovi;

C. budući da se veze između Europe i Sjedinjenih Američkih Država temelje na duhu i načelima demokracije, vladavine prava, slobode, pravde i solidarnosti;

D. budući da je suradnja Sjedinjenih Američkih Država i Europske unije te njezinih država članica u borbi protiv terorizma i dalje ključna za zaštitu i sigurnost obaju partnera;

E. budući da su uzajamno povjerenje i razumijevanje ključni čimbenici u transatlantskom dijalogu i partnerstvu;

F. budući da je nakon 11. rujna 2001. borba protiv terorizma postala jedan od najvažnijih prioriteta većine vlada; budući da zbog razotkrivanja utemeljenih na dokumentima koje je objavio bivši suradnik NSA-a Edward Snowden politički čelnici imaju obvezu pozabaviti se izazovima nadzora i kontrole obavještajnih agencija tijekom njihovih aktivnosti nadzora te procjenom utjecaja tih aktivnosti na temeljna prava i vladavinu prava u demokratskom društvu;

G. budući da su razotkrivanja od lipnja 2013. izazvala veliku zabrinutost u EU-u u vezi s:

— opsegom sustava nadzora koji je otkriven u SAD-u i državama članicama EU-a;

— kršenjem zakonskih normi EU-a, temeljnih prava i standarda zaštite podataka;

— stupnjem povjerenja između transatlantskih partnera EU-a i SAD-a;

— stupnjem suradnje i uključenosti određenih država članica EU-a u programe nadzora SAD-a ili istovjetne programe na nacionalnoj razini koje su otkrili mediji;

— nedostatkom kontrole i učinkovitog nadzora političkih tijela SAD-a i određenih država članica EU-a nad svojim obavještajnim zajednicama;

— mogućnošću da se te operacije masovnog nadzora koriste iz razloga koji nisu strogo povezani s nacionalnom sigurnošću i borbom protiv terorizma, primjerice za ekonomsku ili industrijsku špijunažu ili profiliranje na političkoj osnovi;

— dovođenjem u pitanje slobode medija i komunikacije osoba čija zanimanja podrazumijevaju jamčenje povjerljivosti, uključujući odvjetnike i liječnike;

— ulogama i stupnjem uključenosti obavještajnih agencija i privatnih informacijsko-tehnoloških i telekomunikacijskih društava;

— sve nejasnijim granicama između pravosudnih i obavještajnih aktivnosti, što je dovelo do toga da se prema svakom građaninu postupa kao prema osumnjičeniku i da ga se nadzire;

— prijetnjama privatnosti u digitalno doba i učinku masovnog nadzora na građane i društva;

H. budući da dosad neviđen razotkriveni stupanj špijunaže zahtijeva iscrpnu istragu nadležnih tijela SAD-a, europskih institucija i vlada država članica, nacionalnih parlamenata i sudskih tijela;

I. budući da su tijela vlasti SAD-a porekla neke od razotkrivenih informacija, ali većinu njih nisu osporila; budući da se razvila velika javna rasprava u SAD-u i određenim državama članicama EU-a; budući da vlade i parlamenti država članica EU-a često ne daju svoje mišljenje i ne pokreću odgovarajuće istrage;

J. budući da je predsjednik Obama nedavno najavio reformu NSA-a i njegovih nadzornih programa;

K. budući da je u usporedbi s aktivnostima koje su poduzele institucije EU-a i određene države članice Europski parlament vrlo ozbiljno shvatio svoju obvezu da rasvijetli razotkrivanja o sveobuhvatnim praksama masovnog nadzora građana EU-a te budući da je svojom Rezolucijom od 4. srpnja 2013. o programu nadzora Agencije za nacionalnu sigurnost SAD-a, obavještajnim službama u raznim državama članicama i njihovu utjecaju na privatnost građana EU-a naložio svojem Odboru za građanske slobode, pravosuđe i unutarnje poslove da provede detaljnu istragu o tom predmetu;

L. budući da je dužnost europskih institucija osigurati potpunu primjenu prava EU-a na dobrobit europskih građana te osigurati da se pravna snaga Ugovora EU-a ne dovodi u pitanje usputnim prihvaćanjem izvanteritorijalnih učinaka normi ili djelovanja trećih zemalja;

Razvoj događaja u SAD-u na području reforme obavještajne djelatnosti

M. budući da je Okružni sud Okruga Kolumbija u svojoj odluci od 16. prosinca 2013. presudio da NSA masovnim prikupljanjem metapodataka krši Četvrti amandman Ustava SAD-a ([1]); međutim budući da je Okružni sud Južnog okruga New Yorka u svojoj odluci od 27. prosinca 2013. presudio da je to prikupljanje podataka u skladu sa zakonom;

N. budući da je Okružni sud Istočnog okruga Michigana u svojoj Odluci presudio da se u Četvrtom amandmanu zahtijeva razumnost u svim pretragama, prethodni nalozi za sve razumne pretrage, nalozi koji se temelje na prethodno utvrđenoj opravdanoj sumnji, pomnost u odnosu na osobe, mjesta i stvari te posredovanje neutralnog suca između službenika izvršne vlasti i građana ([2]);

O. budući da u svom izvješću od 12. prosinca 2013. predsjednikova Skupina za preispitivanje obavještajnih i komunikacijskih tehnologija predlaže 46 preporuka predsjedniku SAD-a; budući da se u preporukama ističe potreba za istovremenom zaštitom nacionalne sigurnosti i privatnosti i slobode osoba; budući da s tim u vezi poziva Vladu SAD-a da što je prije moguće prekine masovno prikupljanje telefonskih podataka građana SAD-a u skladu s odjeljkom 215. Zakona o patriotizmu (USA PATRIOT Act); da poduzme detaljno preispitivanje pravnog okvira NSA-a i obavještajnih službi SAD-a radi osiguranja poštovanja prava na privatnost; da prekine napore usmjerene na rušenje ili slabljenje komercijalnog softvera (stražnja vrata i štetni programi); da poveća uporabu šifri, posebno za podatke u tranzitu, te da ne ugrožava napore koji se ulažu u stvaranje standarda šifriranja; da osnuje instituciju branitelja javnog interesa koji će zastupati privatnost i građanske slobode pred Sudom za nadzor stranih obavještajnih službi; da na Odbor za nadzor privatnosti i građanskih sloboda prenese ovlast nadzora aktivnosti obavještajne zajednice za potrebe stranih obavještajnih službi, i to ne samo za potrebe borbe protiv terorizma; te da prihvati prigovore zviždača i da se koristi ugovorima o uzajamnoj pravnoj pomoći za pribavljanje elektroničkih komunikacija, a ne da se koristi nadzorom da bi krala industrijske ili trgovačke tajne;

P. budući da, u skladu s otvorenim memorandumom koji su predsjedniku Obami 7. siječnja 2014. ([3]) predali bivši viši izvršni direktori/stariji obavještajni stručnjaci za razumnost (VIPS) NSA-a, masovno prikupljanje podataka ne poboljšava njihovu sposobnost sprečavanja budućih terorističkih napada; budući da autori naglašavaju da masovni nadzor koji provodi NSA nije rezultirao nijednim spriječenim napadom i da su milijarde dolara potrošene na programe koji su manje učinkoviti i u znatno većoj mjeri narušavaju privatnost građana nego interna tehnologija pod nazivom THINTHREAD izrađena 2001.;

Q. budući da se u pogledu obavještajnih aktivnosti usmjerenih na osobe koje nisu državljani SAD-a u skladu s odjeljkom 702. FISA-e u preporukama predsjedniku SAD-a priznaje temeljno načelo poštovanja privatnosti i ljudskog dostojanstva sadržano u članku 12. Opće deklaracije o ljudskim pravima i članku 17. Međunarodnog pakta o građanskim i političkim pravima; budući da ne preporučuju da se osobama koje nisu državljani SAD-a daju ista prava i jednaka zaštita kao državljanima SAD-a;

([1]) Klayman i ostali protiv Obame i ostalih, građanski predmet br. 13-0851, 16. prosinca 2013.
([2]) ACLU protiv NSA-a br. 06-CV-10204, 17. kolovoza 2006.
([3]) http://consortiumnews.com/2014/01/07/nsa-insiders-reveal-what-went-wrong.

Srijeda, 12. ožujka 2014.

R. budući da je u Predsjedničkom ukazu o aktivnostima prikupljanja informacija o sredstvima veze od 17. siječnja 2014. i s njim povezanome govoru predsjednik SAD-a Barack Obama izjavio da je masovni elektronički nadzor i dalje nužan kako bi Sjedinjene Države mogle štititi nacionalnu sigurnost, svoje građane i građane svojih saveznika i partnera te unaprijediti svoje vanjskopolitičke interese; budući da taj ukaz sadrži određena načela koja se odnose na prikupljanje, korištenje i razmjenu informacija o sredstvima veze te da se njime osiguravaju određene zaštitne mjere osobama koje nisu državljani SAD-a, čime im se dijelom osigurava postupanje jednako onome koje je zajamčeno svim državljanima SAD-a, uključujući zaštitu osobnih podataka svih pojedinaca neovisno o njihovoj nacionalnosti ili mjestu boravka; međutim budući da predsjednik Obama nije zatražio nikakve konkretne prijedloge, posebno u pogledu zabrane masovnog nadzora i uvođenja administrativne i sudske zaštite za osobe koje nisu državljani SAD-a;

Pravni okvir

Temeljna prava

S. budući da se u izvješću o nalazima supredsjedatelja EU-a ad hoc radnom skupinom između EU-a i SAD-a o zaštiti podataka daje pregled pravne situacije u SAD-u, ali da se njime ne utvrđuju činjenice o obavještajnim programima nadzora SAD-a; budući da nisu dostupne informacije o takozvanoj radnoj skupini „druge razine" u okviru koje države članice vode bilateralne razgovore s nadležnim tijelima SAD-a o pitanjima koja se odnose na nacionalnu sigurnost;

T. budući da temeljna prava, a posebno sloboda izražavanja, medija, mišljenja, svijesti, vjere i udruživanja, privatni život, zaštita podataka te pravo na učinkovit pravni lijek, pretpostavku nedužnosti i pravo na pošteno suđenje i nediskriminaciju, ugrađena u Povelju o temeljnim pravima Europske unije i Europsku konvenciju o ljudskim pravima, čine temelj demokracije; budući da je masovni nadzor osoba nespojiv s tim temeljem;

U. budući da su u svim državama članicama povjerljive informacije koje se razmjenjuju između odvjetnika i klijenta zakonom zaštićene od razotkrivanja, što je načelo koje je priznao Sud Europske unije ([1]);

V. budući da je u svojoj Rezoluciji od 23. listopada 2013. o organiziranom kriminalu, korupciji i pranju novca Parlament pozvao Komisiju da podnese zakonodavni prijedlog o uspostavi djelotvornog i sveobuhvatnog programa zaštite zviždača u EU-u kako bi se zaštitili financijski interesi te da, osim toga, provede istragu o tome bi li takvo buduće zakonodavstvo trebalo obuhvatiti i druga područja nadležnosti Unije;

Nadležnosti Unije na području sigurnosti

W. budući da će EU u skladu s člankom 67. stavkom 3. UFEU-a „nastojati osigurati visok stupanj sigurnosti"; budući da je u odredbama Ugovora (posebno člankom 4. stavkom 2. UEU-a, člankom 72. UFEU-a i člankom 73. UFEU-a) propisano da EU ima određene nadležnosti u pitanjima zajedničke sigurnosti Unije; budući da EU ima nadležnost u pitanjima unutarnje sigurnosti (članak 4. točka (j) UFEU-a) te da tu nadležnost izvršava donošenjem odluka o nizu zakonodavnih instrumenata i sklapanjem međunarodnih sporazuma (PNR, TFTP) u cilju borbe protiv teškog kriminala i terorizma te uspostavljanjem strategije unutarnje sigurnosti i osnivanjem agencija koje djeluju na tom području;

X. budući da se u Ugovoru o funkcioniranju Europske unije navodi da „države članice mogu među sobom i u okviru svoje odgovornosti uspostaviti oblike suradnje i koordinacije kakve smatraju primjerenima između nadležnih službi svojih uprava koje su odgovorne za zaštitu nacionalne sigurnosti" (članak 73. UFEU-a);

Y. budući da se u članku 276. UFEU-a navodi da „u izvršavanju svojih ovlasti u pogledu odredaba trećeg dijela glave V. poglavlja 4. i 5. koje se odnose na područje slobode, sigurnosti i pravde, Sud Europske unije nije nadležan ispitivati valjanost ili razmjernost operacija koje provodi policija ili druge službe zadužene za izvršavanje zakona države članice ili izvršavanje odgovornosti država članica u pogledu očuvanja javnog poretka i zaštite unutarnje sigurnosti";

([1]) Odluka suda od 18. svibnja 1982. u slučaju C-155/79, AM & S Europe Limited protiv Komisije Europskih zajednica

Z. budući da se pojmovi „nacionalne sigurnosti", „unutarnje sigurnosti", „unutarnje sigurnosti EU-a" i „međunarodne sigurnosti" preklapaju; budući da Bečka konvencija o pravu međunarodnih ugovora, načelo iskrene suradnje među državama članicama EU-a i načelo zakonodavstva o ljudskim pravima o uskom tumačenju svih iznimaka ukazuju na ograničeno tumačenje pojma „nacionalne sigurnosti" te se njima zahtijeva da se države članice suzdrže od zadiranja u područje nadležnosti EU-a;

AA. budući da je u skladu s europskim Ugovorima Europskoj komisiji dodijeljena uloga „čuvara Ugovora" te je stoga pravna odgovornost Komisije istražiti svaki mogući slučaj kršenja prava EU-a;

AB. budući da, u skladu s člankom 6. UEU-a o Povelji EU-a o temeljnim pravima i Europskoj konvenciji o ljudskim pravima, agencije država članica, a čak i privatne stranke koje djeluju na području nacionalne sigurnosti također moraju poštovati prava sadržana u tom članku, bilo u odnosima prema vlastitim državljanima bilo prema državljanima drugih država;

Ekstrateritorijalnost

AC. budući da treća zemlja koja primjenom svojih zakona, propisa i drugih zakonodavnih ili izvršnih instrumenata izvan svog teritorija u situacijama koje su u nadležnosti EU-a ili njezinih država članica može utjecati na uspostavljeni pravni poredak i vladavinu prava, ili čak prekršiti međunarodno pravo ili pravo EU-a, uključujući prava fizičkih i pravnih osoba, uzimajući u obzir opseg i navedeni ili stvarni cilj takve primjene; budući da je u tim okolnostima nužno poduzeti mjere na razini Unije kako bi se u okviru EU-a osiguralo poštovanje vrijednosti EU-a utvrđenih u članku 2. UEU-a, Povelji o temeljnim pravima, Europskoj konvenciji o ljudskim pravima koja se odnosi na temeljna prava, demokraciju i vladavinu prava, te poštovanje prava fizičkih i pravnih osoba utvrđenih u sekundarnom zakonodavstvu u okviru kojega se primjenjuju ta temeljna načela, na primjer uklanjanjem, neutraliziranjem i blokiranjem učinaka dotičnog stranog zakonodavstva ili nekim drugim načinom borbe protiv tih učinaka;

Međunarodni prijenos podataka

AD. budući da bi, u skladu s člankom 340. UFEU-a ili utvrđenom sudskom praksom Suda EU-a ([1]), zbog prijenosa osobnih podataka SAD-u za potrebe provedbe zakona institucije, tijela, uredi ili agencije EU-a ili države članice, u slučaju nepostojanja odgovarajućih zaštitnih mjera i zaštite temeljnih prava građana EU-a, posebno prava na privatnost i zaštitu osobnih podataka, bili odgovorni za kršenje prava EU-a, što uključuje svako kršenje temeljnih prava sadržanih u povelji EU-a;

AE. budući da prijenos podataka nije geografski ograničen i da su, posebno u kontekstu pojačane globalizacije i komunikacije na svjetskoj razini, zakonodavna tijela EU-a suočena s novim izazovima u pogledu zaštite osobnih podataka i komunikacije; budući da je stoga jačanje pravnih okvira za zajedničke standarde od iznimne važnosti;

AF. budući da su masovnim prikupljanjem osobnih podataka u komercijalne svrhe te u svrhu borbe protiv terorizma i ozbiljnog međudržavnog kriminala osobni podaci i pravo na privatnost građana EU-a ugroženi;

Prijenos SAD-u na temelju sigurne luke SAD-a

AG. budući da pravnim okvirom SAD-a za zaštitu podataka nije osigurana odgovarajuća razina zaštite za građane EU-a;

AH. budući da je, kako bi omogućila tijelima za kontrolu podataka EU-a da prenose osobne podatke određenom tijelu SAD-a, Komisija u svojoj Odluci 2000/520/EZ objavila primjerenost zaštite koju pružaju načela privatnosti sigurne luke i s njima povezanih često postavljanih pitanja koje izdaje Ministarstvo trgovine SAD-a za osobne podatke koji se prenose iz Unije organizacijama u Sjedinjenim Državama koje su se pridružile sigurnoj luci;

([1]) Vidi posebno Zajedničke predmete C-6/90 i C-9/90, Francovich i ostali protiv Italije, presuda od 19. studenoga 1991.

Srijeda, 12. ožujka 2014.

AI. budući da je u svojoj Rezoluciji od 5. srpnja 2000. Europski parlament izrazio sumnje i zabrinutost u pogledu primjerenosti sigurne luke te pozvao Komisiju da što je prije moguće preispita odluku u svjetlu iskustva i zakonodavnih trendova;

AJ. budući da su u radnom dokumentu 4. Parlamenta od 12. prosinca 2013. o nadzornim aktivnostima SAD-a u pogledu podataka EU-a te o njihovu mogućem pravnom učinku na transatlantske sporazume i suradnju izvjestitelji izrazili sumnju i zabrinutost u pogledu primjerenosti sigurne luke te pozvali Komisiju da opozove odluku o primjerenosti sigurne luke i nađe nova pravna rješenja;

AK. budući da je u Odluci Komisije 2000/520/EZ utvrđeno da nadležna tijela država članica mogu izvršavati svoje postojeće ovlasti za obustavu protoka podataka organizaciji koja je sama potvrdila poštovanje načela sigurne luke kako bi zaštitila osobe u odnosu na obradu osobnih podataka kad postoji velika vjerojatnost da se krše načela sigurne luke ili da bi nastavak prijenosa predstavljao neizbježan rizik od nanošenja velike štete osobama čiji se podaci obrađuju;

AL. budući da se u Odluci Komisije 2000/520/EZ također navodi da ako postoji dokaz da osoba odgovorna za osiguravanje poštovanja načela ne izvršava učinkovito svoju ulogu, Komisija mora obavijestiti Ministarstvo trgovine SAD-a i po potrebi predstaviti mjere u cilju poništavanja ili obustave primjene navedene Odluke ili ograničavanja njezina područja primjene;

AM. budući da je u prva dva izvješća o provedbi sigurne luke, objavljena 2002. i 2004., Komisija utvrdila nekoliko nedostataka u vezi s ispravnom provedbom sigurne luke i dala više preporuka nadležnim tijelima SAD-a radi ispravljanja tih nedostataka;

AN. budući da je u trećem izvješću o provedbi, od 27. studenog 2013., devet godina nakon drugog izvješća i bez ijednog ispravljenog nedostatka utvrđenog u tom izvješću, Komisija utvrdila daljnje opsežne slabosti i nedostatke sigurne luke i zaključila da se sadašnji način provedbe ne može održati; budući da je Komisija naglasila da širok pristup obavještajnih agencija SAD-a podacima koje u SAD prenose društva potvrđena kao sigurne luke dovodi do dodatnih ozbiljnih pitanja o kontinuitetu zaštite podataka osoba iz EU-a čiji se podaci obrađuju; budući da je Komisija nadležnim tijelima SAD-a uputila 13 preporuka i poduzela korake da do ljeta 2014., zajedno s nadležnim tijelima SAD-a, utvrdi pravna sredstva što je prije moguće, što će činiti osnovu za potpuno preispitivanje funkcioniranja načela sigurne luke;

AO. budući da se od 28. do 31. listopada 2013. izaslanstvo Odbora Europskog parlamenta za građanske slobode, pravosuđe i unutarnje poslove (Odbor LIBE) u Washingtonu sastalo s Ministarstvom trgovine SAD-a i Saveznim povjerenstvom SAD-a za trgovinu; budući da je Ministarstvo trgovine potvrdilo postojanje organizacija koje su same sebi potvrdile poštovanje načela sigurne luke, ali jasno pokazuju neažurirani status, što znači da društvo ne ispunjava zahtjeve sigurne luke iako i dalje prima osobne podatke iz EU-a; budući da je Savezno povjerenstvo za trgovinu priznalo da je potrebno preispitati sigurnu luku kako bi je se poboljšalo, posebno u odnosu na pritužbe i sustave za alternativno rješavanje sporova;

AP. budući da načela sigurne luke mogu biti ograničena „do mjere koja je potrebna da se ispune uvjeti nacionalne sigurnosti, javnog interesa ili provedbe zakona”; budući da se takva iznimka, kao iznimka od temeljnog prava, uvijek mora tumačiti restriktivno i mora biti ograničena na ono što je nužno i razmjerno u demokratskom društvu, te da u zakonu moraju jasno biti utvrđeni uvjeti i zaštitne mjere zahvaljujući kojima će to ograničenje postati legitimno; budući da su SAD i EU, a posebno Komisija, trebali razjasniti okvir primjene takve iznimke kako bi se izbjegla pogrešna tumačenja ili provedba koja u suštini poništava, između ostaloga, temeljna prava privatnosti i zaštite podataka; budući da se prema tome takva iznimka ne bi trebala koristiti na način kojim se ugrožava ili poništava zaštita koja se pruža Poveljom o temeljnim pravima, Europskom konvencijom o ljudskim pravima, zakonodavstvom EU-a o zaštiti podataka i načelima sigurne luke; ustraje u tome da se u slučaju pozivanja na iznimku o nacionalnoj sigurnosti mora navesti u skladu s kojim nacionalnim zakonom je to zatraženo;

AQ. budući da je pristup velikog broja obavještajnih agencija SAD-a ozbiljno narušio transatlantsko povjerenje i da ima negativan utjecaj na povjerenje prema organizacijama SAD-a koje djeluju u EU-u; budući da se to dodatno pogoršalo zbog nedostatka sudskih i administrativnih pravnih lijekova za građane EU-a u zakonodavstvu SAD-a, osobito u slučaju nadzora u obavještajne svrhe;

Prijenos trećim zemljama uz odluku o primjerenosti

AR. budući da su, prema otkrivenim informacijama i nalazima istrage Odbora LIBE, nacionalne sigurnosne agencije Novog Zelanda, Kanade i Australije u velikoj mjeri uključene u masovni nadzor elektroničkih komunikacija i da aktivno surađuju s SAD-om u okviru takozvanoga programa „Pet očiju" te da možda međusobno razmjenjuju osobne podatke građana EU-a prenesene iz EU-a;

AS. budući da se u odlukama Komisije 2013/65/EU ([1]) i 2002/2/EZ ([2]) navodi da je razina zaštite koju pružaju novozelandski Zakon o privatnosti i kanadski Zakon o zaštiti osobnih podataka i elektroničkih dokumenata primjerena; budući da navedena razotkrivanja također ozbiljno utječu na povjerenje u pravne sustave tih zemalja u pogledu kontinuiteta zaštite koja se pruža građanima EU-a; budući da Komisija nije preispitala taj aspekt;

Prijenos utemeljen na ugovornim odredbama i drugim instrumentima

AT. budući da je u Direktivi 95/46/EZ predviđeno da se međunarodni prijenos podataka u treću zemlju može odvijati i posebnim instrumentima, pri čemu tijelo za kontrolu podataka pruža odgovarajuće zaštitne mjere u pogledu privatnosti i temeljnih prava i sloboda pojedinaca te u pogledu ostvarivanja odgovarajućih prava;

AU. budući da takve zaštitne mjere mogu posebno proizlaziti iz odgovarajućih ugovornih odredbi;

AV. budući da na temelju Direktive 95/46/EZ Komisija ima ovlast odlučiti o tome da posebne standardne ugovorne odredbe pružaju dostatne zaštitne mjere propisane tom Direktivom te budući da je na temelju toga Komisija donijela tri modela standardnih ugovornih odredbi za prijenos podataka tijelima za kontrolu i obradu (i tijelima za podobradu) u trećim zemljama;

AW. budući da je u odlukama Komisije kojima se utvrđuju standardne ugovorne odredbe predviđeno da nadležna tijela u državama članicama mogu izvršavati svoje postojeće ovlasti obustave protoka podataka ako se utvrdi da su u zakonu kojem podliježe uvoznik ili tijelo za podobradu podataka utvrđeni zahtjevi o odstupanju od primjenjivog zakona o zaštiti podataka, kojima se prekoračuju ograničenja nužna u demokratskom društvu kako je predviđeno člankom 13. Direktive 95/46/EZ, ako će takvi zahtjevi vjerojatno imati znatan negativan učinak na jamstva propisana primjenjivim zakonom o zaštiti podataka i standardnim ugovornim odredbama ili ako postoji velika vjerojatnost da se standardne ugovorne odredbe u prilogu ne poštuju ili se neće poštovati te da bi nastavak prijenosa predstavljao neposredan rizik od velike štete za osobe čiji se podaci obrađuju;

AX. budući da su nacionalna tijela za zaštitu podataka razvila obvezujuća korporativna pravila radi olakšavanja međunarodnih prijenosa u okviru međunarodne korporacije s odgovarajućim zaštitnim mjerama u pogledu privatnosti i temeljnih prava i sloboda pojedinaca te u pogledu ostvarivanja odgovarajućih prava; budući da obvezujuća korporativna pravila prije primjene moraju odobriti nadležna tijela država članica nakon što su ocijenila njihovu usklađenost sa zakonodavstvom Unije o zaštiti podataka; budući da je Odbor LIBE u svom izvješću o Uredbi o općoj zaštiti podataka odbacio obvezujuća korporativna pravila za tijela koja obrađuju podatke s obzirom na to da bi se njima onemogućilo da tijela za kontrolu podataka i osobe čiji se podaci obrađuju imaju bilo kakvu kontrolu nad područjem nadležnosti u okviru kojega se njihovi podaci obrađuju;

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

Srijeda, 12. ožujka 2014.

AY. budući da Europski parlament, s obzirom na nadležnost utvrđenu člankom 218. UFEU-a, ima odgovornost kontinuirano nadzirati vrijednost međunarodnih sporazuma za koje je dao suglasnost;

Prijenos utemeljen na sporazumima o TFTP-u i PNR-u

AZ. budući da je u svojoj Rezoluciji od 23. listopada 2013. Europski parlament izrazio veliku zabrinutost zbog razotkrivanja aktivnosti NSA-a u vezi s izravnim pristupom porukama o financijskim plaćanjima i s njima povezanim podacima, što bi predstavljalo očito kršenje Sporazuma o programu za praćenje financiranja terorizma, posebno njegova članka 1.;

BA. budući da je praćenje financiranja terorizma ključan alat u borbi protiv financiranja terorizma i teškog kriminala koji protuterorističkim istražiteljima omogućuje otkrivanje poveznica između ciljeva istrage i drugih mogućih osumnjičenika povezanih sa širim terorističkim mrežama za koje se sumnja da financiraju terorizam;

BB. budući da je Europski parlament tražio od Komisije da obustavi Sporazum i zatražio da se sve mjerodavne informacije i dokumenti odmah stave na raspolaganje Parlamentu radi razmatranja; budući da Komisija nije učinila ništa od navedenoga;

BC. budući da je nakon tvrdnji objavljenih u medijima Komisija odlučila započeti savjetovanje s SAD-om u skladu s člankom 19. Sporazuma o TFTP-u; budući da je 27. studenog 2013. povjerenik Malmström obavijestio Odbor LIBE da je, nakon sastanka s vlastima SAD-a i u svjetlu odgovora koje su nadležna tijela SAD-a navela u svojim dopisima i za vrijeme sastanaka, Komisija odlučila da neće nastaviti sa savjetovanjem jer ne postoje elementi koji bi ukazali na to da je Vlada SAD-a djelovala protivno odredbama Sporazuma te da je SAD dostavio pisano uvjerenje da nije bilo izravnog prikupljanja podataka protivno odredbama Sporazuma o TFTP-u; budući da nije jasno jesu li vlasti SAD-a zaobišle Sporazum pristupanjem tim podacima preko drugih sredstava, kako je navedeno u pismu od 18. rujna 2013. koje su poslale vlasti SAD-a ([1]);

BD. budući da se tijekom posjeta Washingtonu od 28. do 31. listopada 2013. izaslanstvo Odbora LIBE sastalo s Ministarstvom financija SAD-a; budući da je Ministarstvo financija SAD-a izjavilo da od stupanja na snagu Sporazuma o TFTP-u nije imalo pristup podacima iz SWIFT-a u EU-u, osim u okviru TFTP-a; budući da je Ministarstvo financija SAD-a odbilo komentirati postoji li mogućnost da je podacima SWIFT-a izvan okvira TFTP-a pristupilo bilo koje drugo državno tijelo SAD-a te je li Vlada SAD-a svjesna aktivnosti masovnog nadzora koje provodi NSA; budući da je 18. prosinca 2013. g. Glenn Greenwald u istrazi koju je proveo Odbor LIBE izjavio da su ciljevi NSA-a i GCHQ-a bile mreže SWIFT;

BE. budući da su belgijska i nizozemska tijela za zaštitu podataka 13. studenog 2013. odlučila da će provesti zajedničku istragu u sigurnost platnih mreža SWIFT-a kako bi utvrdila mogu li treće strane dobiti neovlašten ili nezakonit pristup bankovnim podacima europskih građana ([2]);

BF. budući da je, u skladu sa Zajedničkim izvješćem o Sporazumu o PNR-u između EU-a i SAD-a, Ministarstvo domovinske sigurnosti SAD-a 23 puta otkrilo podatke iz PNR-a NSA-u u pojedinačnim slučajevima u okviru borbe protiv terorizma na način koji je u skladu s posebnim uvjetima iz Sporazuma;

BG. budući da se u Zajedničkom izvješću ne spominje činjenica da u slučaju obrade osobnih podataka u obavještajne svrhe, u skladu sa zakonom SAD-a, osobe koje nisu državljani SAD-a nemaju nikakav sudski ili administrativni način da zaštite svoja prava, a ustavna se zaštita jamči samo državljanima SAD-a; budući da se nepostojanjem sudskih ili administrativnih prava poništava zaštita građana EU-a propisana u postojećem Sporazumu o PNR-u;

([1]) U pismu se navodi da „Vlada SAD-a traži i pribavlja financijske informacije … [koje] se prikupljaju regulatornim, pravosudnim, diplomatskim i obavještajnim kanalima te razmjenom sa stranim partnerima" te da se „Vlada SAD-a koristi TFTP-om kako bi dobila podatke SWIFT koje ne dobivamo iz drugih izvora".

([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

Prijenos utemeljen na Sporazumu o uzajamnoj pravnoj pomoći u kaznenim stvarima između EU-a i SAD-a

BH. budući da je Sporazum o uzajamnoj pravnoj pomoći u kaznenim stvarima između EU-a i SAD-a od 6. lipnja 2003. ([1]) stupio na snagu 1. veljače 2010. i da je njegova svrha olakšavanje suradnje između EU-a i SAD-a u učinkovitijoj borbi protiv kriminala, vodeći računa o pravima pojedinaca i vladavini prava;

Okvirni sporazum o zaštiti podataka u području policijske i pravosudne suradnje („krovni sporazum")

BI. budući da je svrha ovog općeg sporazuma uspostaviti pravni okvir za sve prijenose osobnih podataka između EU-a i SAD-a isključivo u svrhu sprječavanja, istraživanja, otkrivanja ili kaznenog progona kaznenih djela, uključujući terorizam, u okviru policijske i pravosudne suradnje u kaznenim stvarima; budući da je Vijeće 2. prosinca 2010. odobrilo pregovore; budući da je ovaj sporazum iznimno važan te da bi bio osnova za olakšavanje prijenosa podataka u kontekstu policijske i pravosudne suradnje te suradnje u kaznenim stvarima;

BJ. budući da bi ovim sporazumom trebala biti predviđena jasna i precizna pravno obvezujuća načela obrade podataka i da bi se trebalo priznati pravo građana EU-a na pravosudni pristup osobnim podacima u SAD-u i njihovo ispravljanje i brisanje te pravo na učinkovite mehanizme upravnih i sudskih pravnih lijekova za građane EU-a u SAD-u i neovisan nadzor aktivnosti obrade podataka;

BK. budući da je u Komunikaciji od 27. studenog 2013. Komisija navela da bi „krovni sporazum" trebao dovesti do visokog stupnja zaštite za građane s obje strane Atlantika i povećati povjerenje Europljana u razmjenu podataka između EU-a i SAD-a te predstavljati osnovu za daljnji razvoj sigurnosne suradnje i partnerstva između EU-a i SAD-a;

BL. budući da pregovori o sporazumu nisu napredovali zbog upornog stajališta Vlade SAD-a da odbije priznavanje izvršnih prava na upravne i sudske pravne lijekove građanima EU-a i zbog namjere da osigura opsežna odstupanja od načela za zaštitu podataka sadržanih u sporazumu, kao što je ograničenje namjene, zadržavanja podataka ili daljnjeg prijenosa podataka unutar zemlje i u inozemstvo;

Reforma zaštite podataka

BM. budući da se pravni okvir EU-a za zaštitu podataka trenutno preispituje u cilju uspostavljanja sveobuhvatnog, dosljednog, modernog i čvrstog sustava za sve aktivnosti obrade podataka u Uniji; budući da je Komisija u siječnju 2012. predstavila paket zakonodavnih prijedloga: Opću uredbu o zaštiti podataka ([2]), koja će zamijeniti Direktivu 95/46/EZ i uspostaviti ujednačeno zakonodavstvo diljem Unije, i Direktivu ([3]) kojom će se propisati usklađen okvir za sve aktivnosti obrade podataka koje provode pravosudna tijela za potrebe provedbe zakona i smanjiti postojeće razlike među nacionalnim zakonima;

BN. budući da je 21. listopada 2013. Odbor LIBE donio svoja zakonodavna izvješća o dva prijedloga i odluku o otvaranju pregovora s Vijećem u cilju donošenja zakonodavnih instrumenata u ovom zakonodavnom sazivu;

BO. budući da, iako je Europsko vijeće od 24. i 25. listopada 2013. pozvalo na pravovremeno donošenje snažnog općeg okvira za zaštitu podataka u EU-u radi jačanja povjerenja građana i poduzeća u digitalnu ekonomiju, nakon dvije godine rasprave Vijeće još uvijek nije uspjelo doći do općeg pristupa Općoj uredbi o zaštiti podataka i Direktivi ([4]);

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

Sigurnost IT-a i računarstvo u oblaku

BP. budući da se u gorenavedenoj Rezoluciji Parlamenta od 10. prosinca 2013. naglašava gospodarski potencijal „računarstva u oblaku" za rast i zapošljavanje; budući da se ukupna ekonomska vrijednost tržišta računarstva u oblaku procjenjuje na 207 bilijuna USD godišnje do 2016., što je dvostruko od njegove vrijednosti 2012. godine;

BQ. budući da stupanj zaštite podataka u okolini računarstva u oblaku ne smije biti manji od onoga koji se pruža u bilo kojem drugom kontekstu obrade podataka; budući da se zakonodavstvo Unije o zaštiti podataka, s obzirom na to da je tehnološki neutralno, već primjenjuje na usluge računarstva u oblaku unutar EU-a;

BR. budući da aktivnosti masovnog nadzora omogućuju obavještajnim službama pristup osobnim podacima koje pojedinci u EU-u pohranjuju ili na drugi način obrađuju u skladu s ugovorima o uslugama računarstva u oblaku s glavnim pružateljima usluga računarstva u oblaku u SAD-u; budući da su obavještajna tijela SAD-a pristupila osobnim podacima pohranjenim ili na drugi način obrađenim na poslužiteljima na tlu EU-a prisluškivanjem unutarnjih mreža Yahooa i Googlea; budući da te aktivnosti predstavljaju kršenje međunarodnih obveza i normi europskih temeljnih prava, uključujući i pravo na privatnost i obiteljski život, povjerljivost komunikacija, pretpostavku nevinosti, slobodu izražavanja, slobodu informiranja, slobodu okupljanja i udruživanja i slobodu poduzetništva; budući da nije isključeno da su obavještajna tijela pristupila i podacima javnih tijela ili poduzeća i institucija u državama članicama pohranjenim u uslugama oblaka;

BS. budući da američke obavještajne agencije provode politiku sustavnog podrivanja kriptografskih protokola i proizvoda kako bi mogle presretati i šifrirane komunikacije; budući da je Agencija za nacionalnu sigurnost SAD-a prikupila veliku količinu takozvanih „zero-day exploits" – IT-sigurnosnih ranjivosti koje još nisu poznate javnosti ili prodavaču proizvoda; budući da te aktivnosti u velikoj mjeri ugrožavaju globalne napore u poboljšanju informatičke sigurnosti;

BT. budući da je činjenica da su obavještajne agencije imale pristup osobnim podacima korisnika internetskih usluga jako poremetila povjerenje građana u te usluge i da stoga ima negativan učinak na poduzeća koja ulažu u nove usluge koje koriste velike količine podataka („Big Data") i nove aplikacije poput interneta stvari („Internet of Things");

BU. budući da prodavači informatičke tehnologije često dostavljaju proizvode čija informatička sigurnost nije bila provjerena na odgovarajući način ili koji ponekad čak imaju „stražnja vrata" („backdoors") koje je prodavač namjerno ugradio; budući da je nepostojanje pravila o odgovornosti za prodavače softvera dovelo do situacije koju su iskoristile obavještajne agencije, ali da također ostavlja otvorenim rizik da napad izvedu i druga tijela;

BV. budući da je ključno da trgovačka društva koja pružaju takve nove usluge i aplikacije poštuju pravila o zaštiti podataka i privatnost podataka osoba čiji se podaci prikupljaju, obrađuju i analiziraju kako bi se među građanima zadržala visoka razina povjerenja;

Demokratski nadzor obavještajnih službi

BW. budući da su obavještajnim službama u demokratskim društvima dane posebne ovlasti i sposobnosti za zaštitu temeljnih prava, demokracije i vladavine prava, prava građana i države od unutarnjih i vanjskih prijetnji te da one podliježu demokratskoj odgovornosti i pravosudnom nadzoru; budući da one jedino u tu svrhu imaju posebne ovlasti i sposobnosti; budući da bi se tim ovlastima trebalo koristiti u zakonskim okvirima koje postavljaju temeljna prava, demokracija i vladavina zakona te da bi njihovu primjenu trebalo strogo kontrolirati jer one inače gube legitimitet i prijete potkopavanju demokracije;

BX. budući da je činjenica da se izvjestan stupanj tajnosti obavještajnim službama dopušta kako bi se izbjeglo ugrožavanje tekućih operacija, otkrivanje načina rada ili ugrožavanje života agenata, ta tajnost ne može poništiti ili isključiti pravila demokratske i sudske kontrole i preispitivanja aktivnosti tih službi, kao ni pravila transparentnosti, posebno u pogledu poštovanja temeljnih prava i vladavine prava, a sve su to temelji demokratskog društva;

BY. budući da je većina postojećih nacionalnih mehanizama nadzora i tijela osnovana ili preuređena 1990.-ih i nije nužno prilagođena brzom političkom i tehnološkom razvoju u prošlom desetljeću koji je doveo do pojačane međunarodne obavještajne suradnje, između ostalog i velikom količinom razmjene osobnih podataka i često dokidanjem razgraničenja između obavještajnih aktivnosti i aktivnosti provođenja zakona;

BZ. budući da se demokratski nadzor obavještajnih aktivnosti i dalje vrši samo na nacionalnoj razini, unatoč povećanoj razmjeni informacija između država članica EU-a i između država članica i trećih zemalja; budući da postoji sve veći jaz između razine međunarodne suradnje s jedne strane i sposobnosti nadzora koje su ograničene na nacionalnu razinu, s druge strane, što dovodi do nedovoljne i neučinkovite demokratske kontrole;

CA. budući da nacionalna nadzorna tijela često nemaju potpun pristup obavještajnim podacima dobivenim od stranih obavještajnih agencija, što može dovesti do praznina u kojima se međunarodne razmjene informacija mogu odvijati bez odgovarajućeg preispitivanja; budući da je taj problem dodatno pojačan takozvanim „pravilom treće stranke" ili načelom „kontrole pošiljatelja", koje je osmišljeno kako bi se pošiljateljima omogućilo da zadrže kontrolu nad daljnjim širenjem svojih osjetljivih informacija, ali se nažalost često tumači kao da se odnosi i na nadzor službi primatelja.

CB. budući da su privatne i javne inicijative za reformu transparentnosti ključ za osiguravanje povjerenja javnosti u aktivnosti obavještajnih agencija; budući da pravni sustavi ne bi smjeli sprječavati trgovačka društva od objavljivanja javnosti informacija o tome kako postupaju po zahtjevima vlasti i sudskim nalozima za pristup podacima korisnika, uključujući i mogućnost objavljivanja ukupnih informacija o nizu odobrenih i odbijenih zahtjeva i naloga;

Glavni nalazi

1. smatra da su nedavno objavljene priče zviždača i novinara u tisku, zajedno s iskazima vještaka za vrijeme istrage, priznanjima vlasti i nedostatnim odgovorom na te navode doveli do uvjerljivih dokaza o postojanju dalekosežnih, složenih i tehnološki naprednih sustava koje su osmislile obavještajne službe SAD-a i nekih država članica radi prikupljanja pohranjivanja i analize komunikacijskih podataka, uključujući i sadržajnih podataka, te lokacijskih podataka i metapodataka o svim građanima diljem svijeta u neviđenim razmjerima i na nediskriminirajući način koji nije utemeljen na sumnji;

2. ukazuje posebno na obavještajne programe Agencije za nacionalnu sigurnost SAD-a koji omogućuju masovni nadzor građana EU-a putem izravnog pristupa središnjim poslužiteljima glavnih internetskih trgovačkih društava u SAD-u (program PRISM), analize sadržaja metapodataka (program Xkeyscore), zaobilaženja šifriranja na internetu (BULLRUN), pristupa računalnim i telefonskim mrežama i pristupa lokacijskim podacima te sustava obavještajne agencije UK-a, GCHQ, kao što su njezini sustavi nadzora (program Tempora) i program za dešifriranje (Edgehill), ciljanih posredničkih („man-in-the-middle") napada na informatičke sustave (programi Quantumtheory i Foxacid) i prikupljanja i zadržavanja 200 milijuna tekstualnih poruka dnevno (program Dishfire);

3. primjećuje tvrdnje o hakiranju ili prisluškivanju sustava Belgacoma od strane obavještajne agencije UK-a, GCHQ-a; napominje navode Belgacoma da ne može niti potvrditi niti opovrgnuti da su ciljane institucije EU-a ili da su one pogođene, kao i da je korišteni štetni program bio vrlo složen i da bi njegov razvoj i uporaba zahtijevali opsežne financijske i ljudske resurse do kojih privatna tijela ili hakeri ne bi mogli doći;

4. naglašava da je povjerenje značajno narušeno: povjerenje između dvaju transatlantskih partnera, povjerenje između građana i njihovih vlada, povjerenje u funkcioniranje demokratskih institucija na obje strane Atlantika, povjerenje u poštovanje vladavine prava i povjerenje u sigurnost službi IT-a i komunikacije; vjeruje da je za ponovnu izgradnju povjerenja u sve te dimenzije hitno potreban sveobuhvatan plan za odgovor koji obuhvaća niz akcija podložnih javnoj kontroli;

5. primjećuje da neke vlade tvrde da su programi masovnog nadzora nužni za borbu protiv terorizma; snažno osuđuje terorizam, ali čvrsto vjeruje da borba protiv terorizma nikada ne može biti opravdanje za ciljane, tajne ili čak nezakonite programe masovnog nadzora; smatra da nijedan od tih programa nije u skladu s načelom nužnosti i proporcionalnosti u demokratskom društvu;

Srijeda, 12. ožujka 2014.

6. podsjeća na čvrsto uvjerenje EU-a u potrebu da se uspostavi ravnoteža između sigurnosnih mjera i zaštite građanskih sloboda i temeljnih prava uz osiguravanje potpunog poštovanja privatnosti i zaštite podataka;

7. smatra da prikupljanje podataka u takvom opsegu ostavlja velike sumnje pitanju vodi li te aktivnosti samo borba protiv terorizma jer se radi o prikupljanju svih mogućih podataka o svim građanima; stoga ističe moguće postojanje drugih razloga koji uključuju i političku i gospodarsku špijunažu koje treba u cijelosti ukloniti;

8. dovodi u pitanje usklađenost aktivnosti masivne gospodarske špijunaže nekih država članica s unutarnjim tržištem EU-a i pravom tržišnog natjecanja kako je propisano u Glavi I. i Glavi VII. Ugovora o funkcioniranju Europske unije; potvrđuje načelo iskrene suradnje sadržano u članku 4. stavku 3. Ugovora o funkcioniranju Europske unije i načelo da se države članice „suzdržavaju od mjera kojima bi se moglo ugroziti ostvarivanje ciljeva Unije";

9. napominje da ni međunarodni ugovori i zakonodavstvo EU-a i SAD-a ni nacionalni mehanizmi nadzora nisu uspjeli osigurati neophodan sustav uzajamnog nadzora i demokratske odgovornosti;

10. osuđuje opsežno, sustavno, nekritičko prikupljanje osobnih podataka o nedužnim osobama, što često uključuje i intimne osobne podatke; naglašava da sustavi nekritičkog masovnog nadzora obavještajnih službi predstavljaju tešku povredu temeljnih prava građana; naglašava da privatnost nije luksuz već predstavlja temelj slobodnog i demokratskog društva; ističe, nadalje, da masovni nadzor može snažno utjecati na slobodu medija, misli i govora kao i slobode okupljanja i udruživanja te da sa sobom nužno nosi rizik od zlouporabe prikupljenih informacija protiv političkih protivnika; naglašava da te aktivnosti masovnog nadzora obuhvaćaju i nezakonito djelovanje obavještajnih službi i da dovode do pitanja o eksteritorijalnosti nacionalnih zakona;

11. smatra ključnim da se profesionalna tajna odvjetnika, novinara, liječnika i ostalih reguliranih profesija zaštiti od aktivnosti masovnog nadzora; posebno naglašava da bi svaka sumnja u povjerljivost komunikacija između odvjetnika i njihovih klijenata mogla negativno utjecati na pravo građana EU-a na pristup pravnim savjetima i pristup pravdi kao i pravu na pravično suđenje;

12. programe nadzora smatra još jednim korakom prema uspostavi potpune preventivne države, mijenjajući uspostavljenu paradigmu kaznenog zakona u demokratskim društvima u kojima upletanje u temeljna prava osumnjičenika treba odobriti sudac ili tužitelj na osnovi razumne sumnje i ono treba biti regulirano zakonom, promičući umjesto toga mješavinu provedbe zakona i obavještajnih aktivnosti s nejasnom i oslabljenom pravnom zaštitom, što često nije u skladu s načelom demokratske kontrole i temeljnim pravima, posebno s pretpostavkom nedužnosti; podsjeća u tom smislu na odluku njemačkog saveznog Ustavnog suda ([1]) o zabrani uporabe preventivnih koordiniranih mjera („präventive Rasterfahndung") osim ako postoji dokaz o konkretnoj opasnosti za druga važna pravno zaštićena prava, pri čemu opća rizična situacija ili međunarodne napetosti ne opravdavaju takve mjere;

13. uvjeren da se tajnim zakonima i sudovima krši načelo vladavine prava; ističe da se presuda suda i odluka upravnog tijela iz države koja nije članica EU-a, a kojom se izravno ili neizravno odobrava prijenos osobnih podataka ne može priznati ni izvršiti ni na koji način ako ne postoji ugovor o uzajamnoj pravnoj pomoći ili međunarodni sporazum koji je na snazi između treće zemlje koja je podnijela zahtjev i Unije ili države članice i prethodnog odobrenja nadležnog nadzornog tijela; podsjeća da nijedna presuda tajnog suda i nijedna odluka upravnog tijela države koja nije članica EU-a, a kojom se tajno odobravaju, izravno ili neizravno, aktivnosti nadzora neće biti priznate ni izvršive;

([1]) 1 BvR 518/02 od 4. travnja 2006.

14. ističe da navedenu zabrinutost pogoršava brz tehnološki i društveni razvoj jer su internet i mobilni uređaji dio svakodnevnog modernog života („sveprisutna računala"), a poslovni model većine internetskih tvrtki temelji se na obradi osobnih podataka; smatra da se radi o problemu neviđenih razmjera; napominje da to može stvoriti situaciju u kojoj se infrastruktura za masovno prikupljanje i obradu podataka može zloupotrijebiti u slučaju promjene političkog režima;

15. primjećuje da za javne institucije EU-a i za građane nema jamstava da se njihova sigurnost i privatnost mogu zaštititi od napada dobro opremljenih uljeza („nema sto postotne internetske sigurnosti"); primjećuje da, kako bi se postigla maksimalna informatička sigurnost, Europljani moraju biti voljni odvojiti dovoljna financijska sredstva i ljudske potencijale za očuvanje neovisnosti i samostalnosti Europe u području informatičke tehnologije;

16. snažno odbija ideju da su sva pitanja povezana s programima masovnog nadzora pitanja nacionalne sigurnosti i da su stoga ona u isključivoj nadležnosti država članica; ponavlja da države članice moraju u potpunosti poštovati zakonodavstvo EU-a i Europsku konvenciju o ljudskim pravima kad djeluju u svrhu osiguravanja nacionalne sigurnosti; podsjeća na nedavnu presudu Suda Europske unije koja kaže: „iako države članice moraju poduzeti odgovarajuće mjere da osiguraju svoju unutarnju i vanjsku sigurnost, sama činjenica da se odluka odnosi na državnu sigurnost ne može učiniti pravo Europske unije nemjerodavnim" ([1]); podsjeća osim toga da je u pitanju zaštita privatnosti svih građana EU-a, kao i sigurnost i pouzdanost svih komunikacijskih mreža EU-a; vjeruje stoga da rasprava i djelovanje na razini EU-a nije samo legitimno već i pitanje autonomije EU-a;

17. upućuje pohvale institucijama i stručnjacima koji su doprinijeli ovoj istrazi; osuđuje činjenicu da su nadležna tijela nekoliko država članica odbila surađivati u istrazi koju je Europski parlament proveo u ime građana pozdravlja otvorenost nekoliko članova Kongresa i nacionalnih parlamenata;

18. svjestan da je u tako ograničenom vremenskom roku moguće provesti samo preliminarnu istragu svih pitanja aktualnih od srpnja 2013.; prepoznaje opseg predmetnih otkrića i činjenicu da su oni još uvijek aktualni; stoga prihvaća pristup planiranja za budućnost koji se sastoji od niza posebnih prijedloga i mehanizma za praćenje djelovanja u sljedećem sazivu parlamenta osiguravajući da nalazi ostanu među glavnim političkim prioritetima EU-a;

19. namjerava zatražiti da u provedbu prijedloga i preporuka ove istrage budu uključene snažne političke snage iz nove Komisije imenovane nakon europskih izbora u svibnju 2014. s ciljem provedbe prijedloga i preporuka iz ove istrage;

Preporuke

20. poziva vlasti SAD i države članice EU-a da, ako to još nije slučaj, zabrane masovne aktivnosti nadzora;

21. poziva države članice EU-a, a posebno one koje sudjeluju u tzv. programima „devet pari očiju" i „14 pari očiju" ([2]), da sveobuhvatno vrednuju i po potrebi revidiraju svoje nacionalno zakonodavstvo i prakse kojima su uređene aktivnosti obavještajnih službi kako bi osigurale da ove podliježu parlamentarnom i pravosudnom nadzoru i javnoj kontroli, da poštuju načela zakonitosti, nužnosti, proporcionalnosti, valjanog postupka, obavještavanja korisnika i transparentnosti, što uključuje i upućivanje na Kompilacije dobrih praksi UN-a i preporuke Venecijanske komisije, te da su u skladu sa standardima Europske konvencije o ljudskim pravima i da su u skladu s obvezama država članica u pogledu temeljnih prava, posebno u vezi sa zaštitom podataka, privatnošću i pretpostavkom nedužnosti;

([1]) Presuda u predmetu C-300/11, ZZ protiv ministrice unutarnjih poslova, 4. lipnja 2013.

([2]) „Program devet pari očiju" obuhvaća SAD, UK, Kanadu, Australiju, Novi Zeland, Dansku, Francusku, Norvešku i Nizozemsku, a „program 14 pari očiju" obuhvaća navedene zemlje, ali i Njemačku, Belgiju, Italiju, Španjolsku i Švedsku.

22. poziva države članice EU-a, a u vezi sa svojom Rezolucijom od 4. srpnja 2013. i saslušanjem povezanim s istragom posebno Ujedinjeno Kraljevstvo, Francusku, Njemačku, Švedsku, Nizozemsku i Poljsku, da osiguraju da njihov aktualni i budući zakonodavni okvir i mehanizmi nadzora aktivnosti obavještajnih službi budu u skladu sa standardima Europske konvencije o ljudskim pravima i zakonodavstvom Europske unije o zaštiti podataka; poziva te države članice da pojasne navode o aktivnostima masovnog nadzora uključujući masovni nadzor prekograničnih telekomunikacija, neselektivni nadzor kabelskih komunikacija, potencijalne sporazume obavještajnih službi i telekomunikacijskih društava o pristupu i razmjeni osobnih podataka i pristupu transatlantskim kabelima, osoblje i opremu obavještajnih službi SAD-a na teritoriju EU-a bez kontrole operacija nadzora i njihovu kompatibilnost sa zakonodavstvom EU-a; poziva nacionalne parlamente tih zemalja da pojačaju suradnju svojih tijela za nadzor obavještajnih aktivnosti na europskoj razini;

23. poziva Ujedinjenu Kraljevinu, posebno s obzirom na opsežna medijska izvješća o masovnom nadzoru koje provodi obavještajna služba GCHQ, da revidira svoj postojeći pravni okvir koji se sastoji od „složene interakcije" između triju odvojenih zakona – Zakona o ljudskim pravima iz 1998., Zakona o obavještajnim službama iz 1994. i Zakona o regulaciji istražnih ovlasti iz 2000.;

24. prima na znanje pregled nizozemskog Zakona o obavještajnim aktivnostima i sigurnosti iz 2002. (izvješće „Dessensove komisije" od 2. prosinca 2013.); podupire one preporuke komisije za pregled kojima se nastoji ojačati transparentnost, kontrola i nadzor nizozemskih obavještajnih službi; poziva Nizozemsku da se suzdrži od proširenja ovlasti obavještajnih službi na način koji omogućava neselektivni i masovni nadzor kabelske komunikacije nedužnih građana, posebno s obzirom na činjenicu da se jedno od najvećih središta za razmjenu internetskog prometa na svijetu nalazi u Amsterdamu (AMS-IX); poziva na oprez prilikom definiranja ovlasti i kapaciteta nove Zajedničke kibernetičke jedinice za obavještajne podatke o sredstvima veze, kao i na oprez glede prisustva i djelovanja obavještajnog osoblja SAD-a na nizozemskom teritoriju;

25. poziva države članice, uključujući slučajeve u kojima ih predstavljaju njihove obavještajne agencije, da se suzdrže od prihvaćanja nezakonito prikupljenih podataka iz trećih zemalja i od dopuštanja aktivnosti nadzora od strane vlada trećih zemalja ili agencija na svom državnom području, koje su nezakonite u skladu s nacionalnim pravom ili ne zadovoljavaju pravne zaštitne mjere sadržane u međunarodnim instrumentima ili instrumentima EU-a, uključujući zaštitu ljudskih prava u okviru UEU-a, Europske konvencije o ljudskim pravima -a i Povelje EU-a o temeljnim pravima;

26. poziva na prekid masovnog presretanja i obrade slika s internetskih kamera koje vrši bilo koja tajna služba; poziva države članice da u potpunosti istraže na koji su način i u kojem opsegu njihove tajne službe uključene u prikupljanje i obradu slika s internetskih kamera te da izbrišu sve pohranjene slike prikupljene u okviru takvih programa masovnog nadzora;

27. poziva države članice da odmah ispune svoje pozitivne obaveze iz Europske konvencije o ljudskim pravima u vezi sa zaštitom svojih građana od nadzora protivnog zahtjevima te konvencije koje provode treće zemlje ili njihove vlastite obavještajne službe, uključujući slučajeve u kojima je cilj takvog nadzora zaštita nacionalne sigurnosti, i da osiguraju da vladavina prava ne bude oslabljena kao rezultat primjene zakona treće zemlje izvan njezinog državnog područja;

28. poziva glavnog tajnika Vijeća Europe da pokrene postupak iz članka 52. u skladu s kojim „na zahtjev glavnog tajnika Vijeća Europe svaka visoka ugovorna stranka mora dostaviti objašnjenje načina na koji njezino nacionalno zakonodavstvo osigurava učinkovitu provedbu odredbi Konvencije";

29. poziva države članice da odmah poduzmu odgovarajuće mjere, uključujući sudske postupke, protiv povrede svojeg suvereniteta i općeg javnog međunarodnog prava kao rezultat programa masovnog nadzora; nadalje, poziva države članice da iskoriste dostupne međunarodne mjere za obranu temeljnih prava građana EU-a, u prvom redu pokretanjem žalbenog postupka između država u skladu s člankom 41. Međunarodnog pakta o građanskim i političkim pravima (ICCPR);

30. poziva države članice da uspostave učinkovite mehanizme kako bi osobe odgovorne za programe (masovnog) nadzora kojima se krše vladavina prava i temeljna prava građana odgovarale za ovu zlouporabu ovlasti;

31. poziva SAD da bez odgode revidira svoje zakonodavstvo kako bi ga uskladio s međunarodnim pravom, da prizna pravo na privatnost i druga prava građana EU-a, da osigura sudsku zaštitu građana EU-a, da izjednači prava građana EU-a s pravima državljana SAD-a i da potpiše Fakultativni protokol kojim će se omogućiti žalbe pojedinaca u skladu s ICCPR-om;

32. u tom smislu pozdravlja primjedbe predsjednika SAD-a Obame i njegov predsjednički ukaz od 17. siječnja 2014. kao korak naprijed u procesu ograničavanja odobrenja za korištenje nadzorom i obradom podataka u svrhe nacionalne sigurnosti i jednakog postupanja obavještajne zajednice SAD-a prema osobnim informacijama svih pojedinaca, bez obzira na njihovo državljanstvo ili boravište; međutim, u kontekstu odnosa EU-a i SAD-a očekuje dodatne konkretne korake kojima će se, što je najvažnije, ojačati povjerenje prema transatlantski prijenos podataka i kojima će se osigurati obvezujuća jamstva za izvršiva prava građana EU-a na privatnost, kako je detaljno izloženo u ovom izvješću;

33. naglašava svoju ozbiljnu zabrinutost zbog rada Odbora za konvenciju o kibernetičkom kriminalu Vijeća Europe na tumačenju članka 32. Konvencije o kibernetičkom kriminalu od 23. studenog 2001. (Konvencija iz Budimpešte) o prekograničnom pristupu pohranjenim računalnim podacima uz suglasnost ili u slučaju javne dostupnosti i protivi se svakom zaključenju dodatnog protokola ili smjernica kojima bi se nastojalo proširiti područje primjene te odredbe u odnosu na trenutačni režim uspostavljen tom Konvencijom, koji već ionako predstavlja veliku iznimku od načela teritorijalnosti zbog toga što bi to moglo dovesti do nesmetanog daljinskog pristupa pravosudnih tijela poslužiteljima i računalima u drugim državama bez pribjegavanja sporazumima o uzajamnoj pravnoj pomoći i drugim instrumentima pravosudne suradnje kojima bi se jamčila temeljna prava pojedinca, uključujući pravo na zaštitu podataka i pravično suđenje, a posebno Konvenciju 108 Vijeća Europe;

34. poziva Komisiju da prije srpnja 2014. provede ocjenu mogućnosti primjene Uredbe (EZ) br. 2271/96 na slučajeve sukoba zakona o prijenosu osobnih podataka;

35. poziva Agenciju za temeljna prava da provede detaljno istraživanje zaštite temeljnih prava u kontekstu nadzora, a osobito aktualnog pravnog položaja građana EU-a u odnosu na mogućnosti pravne zaštite koja im u vezi s tom praksom stoji na raspolaganju;

Međunarodni prijenos podataka

Pravni okvir SAD-a za zaštitu podataka i sigurna luka SAD-a

36. napominje da su trgovačka društva koja su prema medijskim navodima uključena u masovni nadzor Agencije za nacionalnu sigurnost SAD-a nad osobama u EU-u čiji se podaci obrađuju društva koja su sama potvrdila svoju privrženost sigurnoj luci i napominje da je sigurna luka pravni instrument koji se upotrebljava za prijenos osobnih podataka iz EU-a u SAD (npr. Google, Microsoft, Yahoo!, Facebook, Apple i LinkedIn); izražava svoju zabrinutost zbog toga što te organizacije nisu šifrirale podatke i komunikacije između podatkovnih centara, čime obavještajnim službama omogućuju presretanje podataka; pozdravlja naknadne izjave nekih trgovačkih društava SAD-a da će ubrzati planove za šifriranje protoka podataka među svojim globalnim podatkovnim centrima;

37. smatra da sveobuhvatan pristup obavještajnih službi SAD-a osobnim podacima iz EU-a koji se obrađuju kroz sigurnu luku sam po sebi ne zadovoljava kriterije za izuzeće na temelju „nacionalne sigurnosti”;

38. smatra da se, budući da u postojećim okolnostima načela sigurne luke ne osiguravaju odgovarajuću zaštitu građanima EU-a, ti prijenosi trebaju odvijati u okviru drugih instrumenata, kao što su ugovorne odredbe ili obvezujuća korporativna pravila, pod uvjetom da se tim instrumentima utvrde posebne zaštitne mjere ili zaštita i da ih ne bude moguće zaobići drugim pravnim okvirima;

39. smatra da Komisija nije djelovala u cilju ispravljanja dobro poznatih nedostataka trenutačne provedbe sigurne luke;

40. poziva Komisiju da predstavi mjere kojima se osigurava hitna obustava primjene Odluke Komisije 2000/520/EZ, u kojoj je objavljena primjerenost načela privatnosti sigurne luke i povezanih često postavljanih pitanja koja objavljuje Ministarstvo trgovine SAD-a; poziva stoga vlasti SAD-a da iznesu prijedlog za novi okviri za prijenos osobnih podataka iz EU-a u SAD koji je u skladu s odredbama Europske unije o zaštiti podataka i koji pruža traženu odgovarajuću razinu zaštite;

41. poziva nadležna tijela država članica, u prvom redu tijela za zaštitu podataka, da iskoriste postojeće ovlasti i odmah obustave protok podataka prema bilo kojoj organizaciji koja je potvrdila poštovanje načela sigurne luke SAD-a i da zatraže da se takav protok podataka odvija samo u okviru drugih instrumenata, pod uvjetom da sadrže odgovarajuće mjere zaštite i jamstva za zaštitu privatnosti i temeljnih prava i sloboda pojedinaca;

42. poziva Komisiju da do prosinca 2014. predstavi sveobuhvatnu ocjenu okvira SAD-a za zaštitu privatnosti, uključujući trgovinske, policijske i obavještajne aktivnosti te da predstavi konkretne preporuke utemeljene na nedostatku općeg zakona o zaštiti podataka u SAD-u; potiče Komisiju na angažman s vlastima SAD-a kako bi se uspostavio pravni okvir koji će osigurati visoku razinu zaštite pojedinaca odnosno njihovih osobnih podataka prenesenih u SAD i osigurati jednakost okvira za privatnost EU-a i SAD-a;

Prijenos trećim zemljama uz odluku o primjerenosti

43. podsjeća da je u Direktivi 95/46/EZ predviđeno da se prijenos osobnih podataka u treću zemlju može odvijati samo ako, ne dovodeći u pitanje usklađenost s nacionalnim odredbama donesenim u skladu s drugim odredbama Direktive, predmetna treća zemlja osigura odgovarajući stupanj zaštite, s tim da je svrha ove odredbe osigurati kontinuitet zaštite koja se osigurava zakonodavstvom EU-a o zaštiti podataka u slučaju prijenosa podataka izvan EU-a;

44. podsjeća da je u Direktivi 95/46/EZ također predviđeno da se odgovarajuća razina zaštite koju osiguravaju treće zemlje ocjenjuje ovisno o svim okolnostima u vezi s prijenosom podataka ili skupom tih prijenosa; također podsjeća da se Direktivom Komisiji dodjeljuju provedbene ovlasti da izjavi da treća zemlja osigurava odgovarajući stupanj zaštite u svjetlu kriterija propisanih u Direktivi 95/46/EZ; podsjeća da se Direktivom 95/46/EZ Komisiji daju ovlasti da izjavi da treća zemlja ne osigurava odgovarajući stupanj zaštite;

45. podsjeća da u tom slučaju države članice moraju poduzeti nužne mjere za sprječavanje prijenosa podataka iste vrste u predmetnu treću zemlju i da bi Komisija trebala pokrenuti pregovore u cilju ispravljanja te situacije;

46. poziva Komisiju i države članice da bez odlaganja ocijene je li uključenost obavještajnih službi Novog Zelanda i Kanade u masovni nadzor građana EU-a utjecala na odgovarajući stupanj zaštite novozelandskog Zakona o privatnosti i kanadskog Zakona o zaštiti osobnih podataka i elektroničkih dokumenata, kako je navedeno u Odlukama Komisije 2013/65/EU i 2002/2/EZ i da, ako je potrebno, poduzmu odgovarajuće mjere kako bi odgodile ili preinačile odluke o primjerenosti; također poziva Komisiju da ocijeni stanje za druge države koje su dobile ocjenu o primjerenosti; očekuje od Komisije da Parlament izvijesti o svojim nalazima o navedenim zemljama najkasnije do prosinca 2014.;

Prijenosi utemeljeni na ugovornim odredbama i drugim instrumentima

47. podsjeća da su nacionalna tijela za zaštitu podataka istaknula da standardne ugovorne obveze ni obvezujuća korporativna pravila nisu formulirani imajući na umu situacije pristupa podacima za potrebe masovnog nadzora i da takav pristup nije u skladu s odredbama o odstupanju od ugovornih odredbi ili obvezujućih korporativnih pravila koji se odnose na iznimna odstupanja u slučaju legitimnog interesa u demokratskom društvu ili kada je to nužno i razmjerno;

48. poziva države članice da zabrane ili obustave protok podataka u treće zemlje na temelju standardnih ugovornih odredbi, ugovornih odredbi ili obvezujućih korporativnih pravila koje su odobrila nacionalna nadležna tijela kada je vjerojatno da se zakonom koji se primjenjuje na primatelje podataka ovima nameću zahtjevi koji nadilaze ograničenja koja su nužno potrebna, primjerena i proporcionalna u demokratskom društvu i koji će vjerojatno imati negativan učinak na jamstva predviđena mjerodavnim zakonodavstvom o zaštiti podataka i standardnim ugovornim odredbama ili zato što bi nastavak prijenosa osobe čiji se podaci obrađuju izložio velikom riziku od štete;

49. pozva radnu skupinu iz članka 29. da donese preporuke i smjernice o zaštitnim mjerama koje bi trebali sadržavati ugovorni instrumenti za međunarodni prijenos osobnih podataka iz EU-a kako bi se osigurala zaštita privatnosti, temeljnih prava i sloboda pojedinaca, posebno vodeći računa o zakonima treće zemlje o obavještajnim podacima i nacionalnoj sigurnosti i o sudjelovanju trgovačkih društava koja u trećoj zemlji primaju podatke u aktivnostima masovnog nadzora koje provode obavještajne službe treće zemlje;

50. poziva Komisiju da hitno preispita postojeće standardne ugovorne odredbe koje je utvrdila kako bi ocijenila pružaju li nužnu zaštitu u vezi s pristupom osobnim podacima koji se prenose u okviru odredbi za obavještajne svrhe i, ako je potrebno, da ih revidira;

Prijenosi utemeljeni na Sporazumu o uzajamnoj pravnoj pomoći

51. poziva Komisiju da prije kraja 2014. provede dubinsku ocjenu postojećeg Sporazuma o uzajamnoj pravnoj pomoći, u skladu s njegovim člankom 17., kako bi provjerila njegovu provedbu u praksi, a posebno primjenjuje li doista SAD taj sporazum za dobivanje informacija ili dokaza u EU-u te dolazi li do zaobilaženja Sporazuma kako bi se informacije dobile izravno u EU-u, te da ocijeni učinak na temeljna prava pojedinaca; ta se ocjena ne bi smjela temeljiti samo na službenim izjavama SAD-a već na posebnim evaluacijama EU-a; ova bi se dubinska analiza trebala baviti i posljedicama primjene ustavne arhitekture Unije na taj instrument radi usklađivanja sa zakonodavstvom Unije, uzimajući posebno u obzir Protokol 36. i njegov članak 10. i Izjavu br. 50. uz taj Protokol; također traži od Vijeća i Komisije da ocijene bilateralne sporazume između država članica i SAD-a s ciljem osiguravanja usklađenosti između navedenih sporazuma i sporazuma koje EU ima ili planira sklopiti sa SAD-om;

Uzajamna pravna pomoć EU-a u kaznenim stvarima

52. traži od Vijeća i Komisije da obavijeste Parlament o stvarnoj primjeni Konvencije o uzajamnoj pravnoj pomoći u kaznenim stvarima između država članica, posebno Glave III. o presretanju telekomunikacijskog prometa; poziva Komisiju da, u skladu sa zatraženim, prije kraja 2014. dostavi prijedlog u skladu s Izjavom br. 50. uz Protokol 36. kako bi se on mogao uskladiti s okvirom Ugovora iz Lisabona;

Prijenosi utemeljeni na sporazumima o TFTP-u i PNR-u

53. smatra da informacije koje su dali Europska komisija i Ministarstvo financija SAD-a ne pojašnjavaju činjenicu imaju li obavještajne službe SAD-a pristup financijskim porukama iz SWIFT-a u EU-u presretanjem mreža SWIFT-a ili bankovnih operativnih sustava ili komunikacijskih mreža, odvojeno ili u suradnji s nacionalnim obavještajnim agencijama i izbjegavajući postojeće bilateralne kanale za uzajamnu pravnu pomoć i pravosudnu suradnju;

Srijeda, 12. ožujka 2014.

54. ponavlja svoju Rezoluciju od 23. listopada 2013. i poziva Komisiju da obustavi primjenu Sporazuma o TFTP-u;

55. poziva Komisiju da reagira na zabrinutost zbog toga što se tri najveća računalna rezervacijska sustava koja koriste zrakoplovne tvrtke u svijetu nalaze u SAD-u i što se PNR-podaci pohranjuju u sustave oblaka koji djeluju na tlu SAD-a u skladu s američkim zakonima, zbog čega ne postoji usklađenost zaštite podataka;

Okvirni sporazum o zaštiti podataka u području policijske i pravosudne suradnje („krovni sporazum")

56. smatra da je zadovoljavajuće rješenje u okviru „krovnog sporazuma" preduvjet za potpunu obnovu povjerenja između transatlantskih partnera;

57. traži trenutačnu obnovu pregovora s SAD-om o „krovnom sporazumu" kojim bi se prava građana EU-a trebala dovesti u istu razinu s pravima građana SAD-a; ističe, osim toga, da bi taj sporazum trebao pružiti učinkovitu i izvršivu upravnu i pravosudnu zaštitu svim građanima EU-a u SAD-u bez ikakvog oblika diskriminacije;

58. traži od Komisije i Vijeća da s SAD-om ne pokreću nikakve nove sektorske sporazume ili dogovore o prijenosu osobnih podataka u svrhu provedbe zakona sve dok ne stupi na snagu „krovni sporazum";

59. poziva Komisiju da detaljno izvijesti o različitim točkama pregovora i stanju do travnja 2014.;

Reforma zaštite podataka

60. poziva Predsjedništvo Vijeća i države članice da ubrzaju rad na cijelom paketu o zaštiti podataka kako bi omogućile njegovo donošenje u 2014. godini da građani EU-a mogu uživati bolju zaštitu u vrlo bliskoj budućnosti; ističe da su snažan angažman i puna potpora Vijeća neophodan uvjet da se trećim zemljama pokaže vjerodostojnost i odlučnost;

61. naglašava da su i Uredba o zaštiti podataka i Direktiva o zaštiti podataka nužne za zaštitu temeljnih prava pojedinaca i da se one stoga moraju promatrati u paketu i donijeti istovremeno kako bi se osiguralo da sve aktivnosti obrade podataka na razini EU-a osiguravaju visoku razinu zaštite u svim okolnostima; naglašava da će daljnje mjere za suradnju u provedbi zakona donijeti tek kada Vijeće započne pregovore s Parlamentom i Komisijom o paketu o zaštiti podataka;

62. podsjeća da koncepti „tehničke privatnosti" i „integrirane privatnosti" predstavljaju jačanje zaštite podataka te da bi trebali predstavljati smjernice za sve proizvode, usluge i sustave koji se pružaju na internetu;

63. veću transparentnost i više sigurnosne standarde za internet i telekomunikaciju smatra nužnim načelom za ostvarenje boljeg sustava zaštite podataka te stoga poziva Komisiju da iznese zakonski prijedlog za standardizirane opće uvjete za internet i telekomunikacije te da ovlasti nadzorno tijelo da nadzire usklađenost s općim uvjetima;

Računarstvo u oblaku

64. primjećuje da su navedene prakse negativno utjecale na povjerenje u računarstvo u oblaku i pružatelje tih usluga u SAD-u; ističe, stoga, razvoj europskih oblaka i IT rješenja kao nužnog elementa za rast i zapošljavanje i povjerenje u usluge računarstva u oblaku i pružatelje tih usluga te za osiguranje visoke razine zaštite podatka;

65. poziva sva javna tijela u Uniji da ne upotrebljavaju usluge računarstva u oblaku u slučajevima kada bi se mogli primjenjivati zakoni koji nisu iz EU-a;

66. ponovno naglašava ozbiljnu zabrinutost zbog toga što pružatelji usluga, koji podliježu zakonodavstvu trećih zemalja ili upotrebljavaju poslužitelje koji su smješteni u trećim zemljama, imaju obvezu izravno otkriti osobne podatke i informacije obrađene u skladu sa sporazumima računarstva u oblaku iz EU-a vlastima trećih zemalja te zbog izravnog pristupa na daljinu osobnim podacima i informacijama koje obrađuju tijela za provođenje zakona i obavještajne službe trećih zemalja;

67. osuđuje činjenicu što vlasti trećih zemalja izravnom provedbom zakonskih pravila pristupaju podacima, a ne upotrebljavaju se međunarodni instrumenti utvrđeni za pravnu suradnju kao što su uzajamna pravna pomoć ili drugi oblici pravosudne suradnje;

68. poziva Komisiju i države članice da ubrzaju svoje aktivnosti na uspostavljanju Europskog partnerstva za računarstvo u oblaku uz potpuno uključivanje civilnog društva i tehničke zajednice, primjerice Radne skupine za internetski inženjering (IETF), i aspekata zaštite podataka;

69. poziva Komisiju da, dok pregovara o međunarodnim sporazumima koji uključuju obradu osobnih podataka, obrati posebnu pozornost na rizike i izazove povezane s računarstvom u oblaku, u vezi s temeljni pravima, a posebno, ali ne i isključivo, na pravo na privatnost i zaštitu osobnih podataka, kako je navedeno u člancima 7. i 8. Povelje o temeljnim pravima Europske unije; nadalje, poziva Komisiju da obrati pozornost na nacionalna pravila partnera s kojim pregovara, kojima se utvrđuje pristup policijskih i obavještajnih službi osobnim podacima obrađenima u okviru usluga računarstva u oblaku, posebno tako što će zahtijevati da se policijskim i obavještajnih službama dopusti pristup samo uz puno poštovanje zakonskog postupka na nedvosmislenoj pravnoj osnovi i tako što će postaviti zahtjev za utvrđivanjem točnih uvjeta za pristup, utvrđivanje svrhe tog pristupa, postavljenih sigurnosnih mjera prilikom predaje podataka, prava pojedinaca te pravila za nadzor i mehanizme učinkovite pravne zaštite;

70. podsjeća da sva poduzeća koja se bave djelatnošću pružanja usluga u EU-u moraju bez iznimke poštovati zakonodavstvo EU-a i da su odgovorni za eventualne prekršaje te naglašava važnost raspolaganja učinkovitim, razmjernim i odvraćajućim administrativnim sankcijama koje se može nametnuti onim pružateljima usluga računarstva u oblaku koji se ne pridržavaju standarda EU-a u vezi sa zaštitom podataka;

71. poziva Komisiju i nadležna tijela država članica da procijene razmjer kršenja propisa EU-a o privatnosti i zaštiti podataka u okviru suradnje pravnih subjekata EU-a s tajnim službama ili odobravanja sudskih naloga vlasti trećih zemalja putem kojih su te vlasti tražile osobne podatke građana EU-a protivno zakonodavstvu EU-a o zaštiti podataka;

72. poziva poduzeća koja pružaju nove usluge primjenom „Velikih količina podataka" i novih aplikacija, primjerice aplikacije „Internet stvari" da već u razvojnoj fazi uključe mjere za zaštitu podataka kako bi održali visoku razinu povjerenja među građanima;

Sporazum o partnerstvu za transatlantsku trgovinu i ulaganja (TTIP)

73. prepoznaje da EU i SAD pregovaraju o partnerstvu za transatlantsku trgovinu i ulaganja, koje je od velike strateške važnosti za stvaranje daljnjeg gospodarskog rasta;

74. snažno naglašava, s obzirom na važnost digitalnog gospodarstva za međusobne odnose i za ponovnu izgradnju povjerenja između EU-a i SAD-a, da bi suglasnost Europskog parlamenta na konačni sporazum TTIP mogla biti u pitanju sve dok se potpuno ne obustave masovne aktivnosti nadzora i presretanja komunikacija u institucijama EU-a i diplomatskim predstavništvima i dok se ne nađe odgovarajuće rješenje za prava na privatnost podataka građana EU-a, uključujući administrativni i sudski pravni lijek; naglašava da će Parlament pristati na konačni sporazum TTIP samo ako se

njime u potpunosti poštuju, između ostalog, temeljna prava priznata u Povelji EU-a i pod uvjetom da se na zaštitu privatnosti osoba u vezi s obradom i širenjem osobnih podataka i dalje primjenjuje članak XIV. Općeg sporazuma o trgovini uslugama (GATS); naglašava da se zakonodavstvo EU-a o zaštiti podataka ne smije smatrati „proizvoljnom ili neopravdanom diskriminacijom" u okviru primjene članka XIV. Općeg sporazuma o trgovini uslugama (GATS);

Demokratski nadzor obavještajnih službi

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

76. poziva, kao što je učinio i u slučaju Echelona, sve nacionalne parlamente koji to još nisu učinili da uspostave smisleni sustav nadzora obavještajnih aktivnosti koji će vršiti zastupnici u parlamentu ili stručna tijela s pravnim ovlastima za provedbu istrage; poziva nacionalne parlamente da osiguraju da takvi odbori/tijela za nadzor imaju dovoljno financijskih sredstava, tehničke stručnosti i pravnih sredstava, uključujući ovlast za provođenje terenskih posjeta, za učinkovitu kontrolu obavještajnih službi;

77. poziva na osnivanje skupine zastupnika i stručnjaka koja će na transparentan način i u suradnji s nacionalnim parlamentima ispitati preporuke za bolji demokratski nadzor nad obavještajnim službama, uključujući parlamentarni, te veću suradnju u području nadzora u EU-u, posebice u pogledu njegove prekogranične dimenzije; smatra da bi skupina posebice trebala istražiti mogućnost uvođenja minimalnih europskih standarda ili smjernica za nadzor nad obavještajnim službama (ex ante i ex post) na temelju najboljih postojećih praksi i preporuka međunarodnih tijela (UN, Vijeće Europe), uključujući pitanje nadzornih tijela koje se smatra trećim strankama u skladu s „pravilom o trećoj stranci" ili načelom „kontrole pošiljatelja", te o nadzoru nad obavještajnim službama iz stranih zemalja i njihovoj odgovornosti, o kriterijima povećane transparentnosti koji bi se nadovezali na opće načelo pristupa informacijama i takozvanim „načelima iz Tshwane" ([1]), kao i načelima o ograničenjima trajanja i opsega svakog nadzora kojim se osigurava njegova razmjernost i ograničenost na svrhu;

78. poziva tu skupinu da pripremi izvješće i pomogne u pripremama za konferenciju koju treba održati Parlament s nacionalnim nadzornim tijelima, bilo da su ona parlamentarna ili neovisna, do početka 2015.;

79. poziva države članice da primjene najbolju praksu kako bi poboljšale pristup svojih nadzornih tijela informacijama o obavještajnim aktivnostima (uključujući povjerljive informacije i informacije iz drugih službi) i uspostavile ovlasti za provedbu posjeta na terenu, opsežan niz ovlasti ispitivanja, prikladne resurse i tehničku stručnost, strogu neovisnost o svojim vladama i obvezu izvješćivanja nacionalnih parlamenata;

80. poziva države članice da razviju suradnju među nadzornim tijelima, posebno u okviru Europske mreže nacionalnih tijela za reviziju obavještajnih službi (ENNIR);

81. potiče Visoku predstavnicu/potpredsjednicu Europske komisije da redovito izvještava nadležna tijela Parlamenta o aktivnostima Centra EU-a za obradu obavještajnih podataka (IntCen), koji je dio Europske službe za vanjsko djelovanje, uključujući o njegovom potpunom poštovanju temeljnih ljudskih prava i važećih pravila EU-a o privatnosti podataka, što će omogućiti poboljšani nadzor Parlamenta nad vanjskom dimenzijom politika EU-a; potiče Komisiju i Visoku predstavnicu/potpredsjednicu Komisije da iznesu prijedloge pravne osnove za aktivnosti IntCen-a u slučaju planiranja bilo kakvih operacija ili budućih nadležnosti na području obavještajnog djelovanja ili samostalnih sredstava za prikupljanje podataka koji bi mogli imati utjecaja na strategiju unutarnje sigurnosti EU-a;

([1]) Globalna načela o nacionalnoj sigurnost i pravu na informacije, lipanj 2013.

82. poziva Komisiju da do prosinca 2014. predstavi prijedlog postupka za sigurnosnu provjeru svih dužnosnika u EU-u jer postojeći sustav koji se oslanja na sigurnosnu provjeru u državi članici državljanstva uključuje različite zahtjeve i trajanje postupaka u nacionalnim sustavima, što dovodi do različitog postupanja prema zastupnicima u parlamentu i njihovom osoblju, ovisno o državljanstvu;

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

Agencije EU-a

84. poziva Zajedničko nadzorno tijelo Europola da provede, zajedno s nacionalnim tijelima za zaštitu podataka, zajedničku inspekciju prije kraja 2014. radi provjere jesu li nacionalna tijela zakonski prikupila informacije i osobne podatke koji se dijele s Europolom, posebno ako su informacije i podatke izvorno stekle obavještajne službe EU-a ili treće zemlje te postoje li odgovarajuće mjere za sprječavanje uporabe i daljnjeg širenja takvih informacija ili podataka; smatra da Europol ne bi trebao obrađivati bilo koje informacije ili podatke stečene kršenjem temeljnih prava koja bi bila zaštićena u skladu s Poveljom o temeljnim pravima;

85. poziva Europol da u skladu sa svojim mandatom zatraži od nadležnih tijela država članica da pokrenu kriminalističke istrage većih kibernetičkih napada i povreda IT sustava s mogućim prekograničnim učinkom; smatra da bi se Europolov mandat trebao proširiti kako bi mu se omogućilo da pokreće vlastite istrage na temelju sumnje u zlonamjerni napad na mrežu i informacijske sustave dvije ili više države članice ili tijela Unije ([1]); poziva Komisiju da preispita aktivnosti Europskog centra za kibernetički kriminal i da po potrebi iznese prijedlog o sveobuhvatnom okviru za jačanje njegovih nadležnosti;

Sloboda izražavanja

86. izražava duboku zabrinutost zbog sve većih prijetnji slobodi medija i zastrašivanja novinara koje vrše državna tijela, posebno u vezi sa zaštitom povjerljivosti novinarskih izvora; ponavlja pozive iznesene u svojoj rezoluciji od 21. svibnja 2013. o Povelji EU-a: utvrđene norme za slobodu medija diljem EU-a";

87. prima na znanje pritvaranje g. Mirande i oduzimanje materijala koje je imao kod sebe od strane britanskih vlasti u skladu sa 7. dijelom Zakona o terorizmu iz 2000. (te zahtjev upućen novinskom listu *The Guardian* da uništi ili preda sav materijal) i izražava zabrinutost da to predstavlja ozbiljno kršenje prava na slobodu izražavanja i medijsku slobodu, koje je priznato u članku 10. EKLJP-a i članku 11. Povelje EU-a, te da bi zakonodavstvo namijenjeno borbi protiv terorizma moglo biti u takvim slučajevima zloupotrijebljeno;

88. skreće pozornost na nevolju zviždača i osoba koje ih podupiru, uključujući novinare koji prate njihova otkrića; poziva Komisiju da provede istragu o tome bi li budući zakonodavni prijedlog kojim se uspostavlja djelotvorni i sveobuhvatni program za zaštitu zviždača u EU-u, koji je Parlament već zatražio u svojoj rezoluciji od 23. listopada 2013., također trebao uključivati druga područja nadležnosti Unije, s posebnim naglaskom na složenost zviždačke prakse u području obavještajnih službi; poziva države članice da iscrpno ispitaju mogućnost da se zviždačima odobrava međunarodna zaštita od kaznenog progona;

([1]) Stajalište Europskog parlamenta od 25. veljače 2014. o prijedlogu Uredbe Europskog parlamenta i Vijeća o Agenciji Europske unije za suradnju i osposobljavanje tijela za provedbu zakona (Europol) (Usvojeni tekstovi, P7_TA(2014)0121).

89. poziva države članice da osiguraju da njihovo zakonodavstvo, prije svega ono na području nacionalne sigurnosti, pruža sigurnu alternativu tišini za otkrivanje i prijavu prijestupa, uključujući korupciju, kaznena djela, kršenja pravne obveze, pogrešnih presuda i zlouporabu ovlasti, što je također u skladu s odredbama različitih međunarodnih (UN i Vijeće Europe) instrumenata za suzbijanje korupcije, načelima iz Rezolucije br. 1729 (2010) Parlamentarne skupštine Vijeća Europe (PACE), načelima iz Tshwane itd.;

IT sigurnost u EU-u

90. ističe da su nedavni događaji jasno pokazali veliku ranjivost EU-a, posebno institucija EU-a, nacionalnih vlada i parlamenata, velikih europskih poduzeća, europskih IT infrastruktura i mreža, na sofisticirane napade uz pomoć složenog softvera i štetnih programa; napominje da takvi napadi zahtijevaju financijske i ljudske resurse kojima vjerojatno raspolažu državna tijela koja rade za strane vlade; u tom kontekstu spominje slučaj hakiranja ili prisluškivanja telekomunikacijskog poduzeća Belgacom kao zabrinjavajući primjer napada na IT sposobnost EU-a; ističe da se povećanjem IT kapaciteta i sigurnosti EU-a također smanjuje ranjivost EU-a na ozbiljne računalne napade za koje su odgovorne velike zločinačke organizacije ili terorističke skupine;

91. smatra da se otkrića o masovnom nadzoru koja su pokrenula ovu krizu mogu iskoristiti kao prilika za Europu da preuzme inicijativu i izgradi, kao prioritetnu stratešku mjeru, snažnu i neovisnu IT sposobnost; ističe da bi se radi pridobivanja povjerenja takva europska informatička sposobnost morala temeljiti na otvorenim standardima i softveru, i po mogućnosti, hardveru otvorenog izvora, pri čemu cjelokupni opskrbni lanac od dizajna procesora do aplikacijskog sloja postaje transparentan i podložan pregledu; ističe da je radi ponovnog stjecanja konkurentnosti u strateškom sektoru informatičkih usluga potreban „digitalni novi deal”, koji uključuje zajedničke i sveobuhvatne napore institucija EU-a, država članica, istraživačkih institucija, industrije i civilnog društva; poziva Komisiju i države članice da koriste javnu nabavu kao sredstvo za podržavanje razvoja sposobnosti u EU-u na način da standarde sigurnosti i privatnosti u EU-u učini ključnim uvjetom u postupcima javne nabave informatičkih proizvoda i usluga; potiče stoga Komisiju da preispita sadašnje prakse javne nabave u pogledu obrade podataka kako bi se razmislilo o tome da se postupci nadmetanja ograniče na certificirana poduzeća i po mogućnosti na poduzeća iz EU-a ako su u pitanju sigurnosni ili drugi ključni interesi;

92. snažno osuđuje činjenicu da su strane obavještajne službe nastojale smanjiti informatičku sigurnost i postaviti stražnja vrata u velikom broju IT sustava; traži Komisiju da predstavi nacrt zakonodavstva o zabrani korištenja stražnjim vratima od strane policijskih službi; stoga preporučuje korištenje softvera otvorenog izvora u svim okruženjima u kojima informatička sigurnost predstavlja problem;

93. poziva sve države članice, Komisiju, Vijeće i Europsko vijeće da pruže najveću potporu, uključujući financijskim sredstvima za istraživanje i razvoj, razvoju europske inovativne i tehnološke sposobnosti na području IT alata, poduzeća i pružatelja (hardvera, softvera, usluga i mreža), uključujući u svrhe internetske sigurnosti kao i sposobnosti šifriranja i kriptografije; poziva sve nadležne institucije i države članice EU-a na ulaganja u lokalne i nezavisne tehnologije EU-a i da masovno razvijaju i povećavaju mogućnosti otkrivanja;

94. poziva Komisiju, normizacijska tijela i ENISA-u da do prosinca 2014. razviju minimalne sigurnosne standarde i standarde privatnosti te smjernice za IT sustave, mreže i usluge, uključujući usluge računarstva u oblaku, u cilju bolje zaštite osobnih podataka građana EU-a i integriteta svih IT sustava; vjeruje da bi takvi standardi mogli postati mjerilo za nove globalne standarde i da bi se trebali utvrditi u okviru otvorenog i demokratskog procesa, umjesto da njihovo utvrđivanje predvodi jedna zemlja, tijelo ili multinacionalna kompanija; smatra da, iako je potrebno uzeti u obzir legitimne policijske i obavještajne aktivnosti kao pomoć u borbi protiv terorizma, one ne bi trebale dovesti do narušavanja pouzdanosti svih IT sustava; izražava potporu najnovijim odlukama Radne skupine za internetski inženjering (IETF) o uključivanju vlada u izradi modela prijetnji internetskoj sigurnosti;

95. ističe da su EU i nacionalni regulatori za telekomunikacije, a u određenim slučajevima i telekomunikacijska poduzeća, jasno zanemarili IT sigurnost svojih korisnika i klijenata; poziva Komisiju da u potpunosti iskoristi svoje postojeće ovlasti u okviru Direktive o e-privatnosti i Okvirne direktive o telekomunikacijama za jačanje zaštite povjerljivosti komunikacija donošenjem mjera kojima će se osigurati usklađenost terminalne opreme s pravom korisnika na kontrolu i zaštitu njihovih osobnih podataka i da osigura visok stupanj sigurnosti telekomunikacijskih mreža i usluga, uključujući zahtijevanjem vrhunskog šifriranja komunikacija s kraja na kraj;

96. podržava kibernetičku strategiju EU-a, ali smatra da njome nisu obuhvaćene sve moguće prijetnje i da ju je potrebno proširiti na zlonamjerno djelovanje država; ističe potrebu za većom IT sigurnosti i otpornosti IT sustava;

97. poziva Komisiju da najkasnije do siječnja 2015. predstavi Akcijski plan za razvoj veće neovisnosti IT sustava EU-a, uključujući dosljedniji pristup jačanju europskih tehnoloških sposobnosti u području IT-a (uključujući IT sustave, opremu, usluge, računarstvo u oblaku, šifriranje i anonimizaciju) i zaštiti ključne IT infrastrukture (uključujući uvjete vlasništva i ranjivost);

98. poziva Komisiju da u okviru sljedećeg radnog programa za Obzor 2020. usmjeri više resursa na jačanje europskog istraživanja, razvoja, inovacija i osposobljavanja u području informacijskih tehnologija, posebno tehnologija i infrastruktura za jačanje privatnosti, kriptologije, sigurnog računarstva, najboljih sigurnosnih rješenja otvorenog izvora i drugih usluga informacijskog društva, te da također promiče unutarnje tržište za europski softver i hardver te šifrirane načine komunikacije i komunikacijske infrastrukture, uključujući razvojem sveobuhvatne industrijske strategije EU-a za IT industriju; smatra da mala i srednja poduzeća imaju posebnu ulogu u istraživanju; naglašava da se financijska sredstva EU-a ne bi smjela dodjeljivati projektima čiji je jedini cilj razvoj alata za nezakonit upad u IT sustave;

99. traži od Komisije da napravi pregled postojećih odgovornosti i da najkasnije do prosinca 2014. preispita potrebu za širim mandatom, boljom koordinacijom i/ili dodatnim resursima i tehničkim sposobnostima za ENISA-u, Europolov centar za kibernetički kriminal i druge specijalizirane centre Unije, CERT-EU i EDPS kako bi im se omogućilo da imaju ključnu ulogu u zaštiti europskih komunikacijskih sustava, da budu učinkovitiji u prevenciji i istrazi većih povreda IT sustava u EU-u i provedbi (ili pomoći državama članicama i tijelima EU-a u provedbi) tehničkih istraga na terenu u vezi s velikim povredama IT-a; posebno poziva Komisiju da razmisli o jačanju uloge ENISA-a u obrani unutarnjih sustava institucija EU-a i o uspostavi tima za hitne računalne intervencije (CERT) za EU i njegove države članice u okviru njezine strukture;

100. traži od Komisije da procijeni potrebu za Akademijom EU-a za IT koja okuplja najbolje europske i međunarodne neovisne stručnjake u svim povezanim područjima i čija bi zadaća bila pružiti svim mjerodavnim institucijama i tijelima EU-a znanstvene savjete o informacijskim tehnologijama, uključujući sigurnosne strategije;

101. poziva nadležne službe Tajništva Europskog parlamenta da na odgovornost predsjednika EP-a provedu, najkasnije do lipnja 2015., uz srednjoročno izvješće do prosinca 2014., detaljnu reviziju i ocjenjivanje sigurnosne pouzdanosti IT sustava Europskog parlamenta s naglaskom na: proračunska sredstva, osoblje, tehničke sposobnosti, internu organizaciju i sve mjerodavne elemente, u cilju ostvarivanja visokog stupnja sigurnosti IT sustava Parlamenta; vjeruje da bi se takvom ocjenom trebale osigurati informacije, analiza i preporuke barem o:

— potrebi za redovnim, strogim, neovisnim sigurnosnim revizijama i testovima mogućnosti prodora, uz pomoć vanjskih stručnjaka osiguravajući transparentnost i jamstvo za njihove kvalifikacije u odnosu na treće zemlje kao i bilo koji oblik interesa;

— uključivanju posebnih zahtjeva za IT sigurnost/privatnost koji se temelje na najboljim praksama u postupke javne nabave za nove IT sustave, uključujući mogućnost zahtjeva za softver otvorenog izvora kao uvjet za kupnju ili zahtjeva da pouzdana europska poduzeća sudjeluju u javnoj nabavi ako je riječ o osjetljivom području povezanom sa sigurnošću;

— popisu poduzeća koja imaju ugovor s Parlamentom u području IT-a i telekomunikacija, uzimajući u obzir informacije koje su otkrivene o njihovoj suradnji s obavještajnim agencijama (poput otkrića o ugovorima Agencije za nacionalnu sigurnost SAD-a s poduzećem kao što je RSA, čije proizvode Parlament koristi za navodnu zaštitu daljinskog pristupa podataka od strane zastupnika i osoblja), uključujući i izvedivost toga da te iste usluge pružaju druga, po mogućnosti europska, poduzeća;

— pouzdanosti i otpornosti softvera, osobito gotovih komercijalnih softvera, koji koriste institucije EU-a u svojim IT sustavima na prodor i pristup pravosudnih i obavještajnih tijela EU-a ili treće zemlje, uzimajući u obzir odgovarajuće međunarodne standarde, načela upravljanja sigurnosnim rizicima zasnovana na najboljim praksama i pridržavanje normi EU-a za sigurnost mreže i podataka u vezi s povredama sigurnosti;

— uporabi više sustava otvorenog izvora;

— koracima i mjerama koje treba poduzeti kako bi se riješilo pitanje sve veće uporabe mobilnih alata (pametnih telefona, tableta, za osobne ili poslovne potrebe) i njihovog utjecaja na informatičku sigurnost sustava;

— sigurnost komunikacija između različitih radnih mjesta Parlamenta i IT sustava koje koristi Parlament;

— uporabi i pronalaženju poslužitelja i IT centara za IT sustave Parlamenta i utjecaju na sigurnost i integritet sustava;

— provedbu u stvarnosti postojećih pravila o povredama sigurnosti i brzom obavještavanja nadležnih tijela od strane pružatelja javno dostupnih komunikacijskih mreža;

— uporabi računarstva i pohrane u oblaku u Parlamentu, uključujući o vrsti podataka koji se pohranjuju u oblaku, načinima zaštite tih podataka i lokaciji servera tog oblaka, pojašnjavajući primjenjivi pravni režim za zaštitu podataka i obavještajne službe te ocjenjujući mogućnosti da se koriste samo serveri u oblaku koji se nalaze na teritoriju EU-a;

— planu koji omogućuje uporabu kriptografskih tehnologija, posebno šifriranja s kraja na kraj za sve IT i komunikacijske usluge kao što su računarstvo u oblaku, e-pošta, instant poruke i telefonija;

— uporabi elektroničkih potpisa u e-pošti;

— planu uporabe standarda šifriranja za e-poštu kao što je zaštita privatnosti GNU-a, koji bi istovremeno dopustio korištenje digitalnih potpisa;

— mogućnosti uspostavljanja sigurne usluge slanja instant poruka u Parlamentu koja omogućuje sigurnu komunikaciju, dok se na poslužitelju prikazuje samo šifrirani sadržaj;

102. poziva sve institucije i agencije EU-a da u suradnji s ENISA-om, Europolom i CERT-ovima do lipnja 2015. provedu slične postupke, posebno Europsko vijeće, Vijeće, Europsku službu za vanjsko djelovanje (uključujući delegacije EU-a), Komisiju, Sud EU-a i Europsku središnju banku te da do prosinca 2014. podnesu srednjoročno izvješće; poziva države članice da provedu slične ocjene;

103. naglašava da bi se, u odnosu na vanjsko djelovanje EU-a, trebale provesti ocjene povezanih proračunskih potreba i odmah poduzeti prve mjere u slučaju Europske službe za vanjsko djelovanje (EEAS) te da je potrebno osigurati odgovarajuća sredstva u okviru nacrta proračuna za 2015.;

104. smatra da bi se trebali razvijati veliki IT sustavi koji se koriste u području slobode, sigurnosti i pravde, kao što je Schengenski informacijski sustav II, Vizni informacijski sustav, Eurodac i mogući budući sustavi kao što je EU-ESTA, i da bi se njima trebalo upravljati na način kojim će se osigurati da ne dolazi do kompromitiranja podataka kao rezultat zahtjeva vlasti trećih zemalja; traži od eu-LISA-e da izvješćuje Parlament o pouzdanosti uspostavljenih sustava do kraja 2014.;

105. poziva Komisiju i EEAS da djeluju na međunarodnoj razini, posebno u okviru UN-a, i u suradnji sa zainteresiranim partnerima provode strategiju EU-a za demokratsko upravljanje internetom radi sprječavanja neželjenog utjecaja bilo koje osobe, poduzeća ili zemlje na aktivnosti ICANN-a i IANA-e osiguravanjem odgovarajuće zastupljenosti svih zainteresiranih strana u tim tijelima, istovremeno izbjegavajući omogućavanje državnog nadzora ili cenzure ili balkanizacije i fragmentacije interneta;

106. poziva EU da preuzme vodstvo u preoblikovanju arhitekture interneta i upravljanju internetom suočavajući se s rizicima povezanim s protokom podataka i pohranom, u cilju veće minimizacije podataka i transparentnosti te manje centralizirane masovne pohrane sirovih podataka, kao i potpunog šifriranja s kraja na kraj za cijeli internetski promet tako da se izbjegnu trenutačni rizici koje podrazumijeva nepotrebno preusmjeravanje prometa kroz državna područja zemalja koje ne ispunjavaju osnovne standarde o temeljnim pravima, zaštiti podataka i privatnosti;

107. poziva na promicanje:

— internetskih tražilica i društvenih mreža EU-a kao važan korak na putu prema neovisnosti IT-a u EU-u;

— europskih pružatelja IT usluga;

— općenitog šifriranja komunikacije, uključujući komunikaciju putem elektroničke pošte i sms-ova;

— ključnih elemenata europskog IT-ja, primjerice rješenja za operacijske sustave klijent-server, korištenje standarda otvorenog izvora, razvoj europskih elemenata za povezivanje mreža, npr. usmjerivača (engl. *router*);

108. poziva Komisiju da predstavi pravni prijedlog za sustav EU-a za usmjeravanje, uključujući obradu evidencije podataka o pozivima (CDR), na razini Europske unije koji će biti podstruktura postojećeg interneta i neće izlaziti izvan granica EU-a; napominje da bi podatke za usmjeravanje i CDR-ove trebalo obrađivati u skladu s pravnim okvirom EU-a;

109. poziva države članice da, u suradnji s ENISA-om, Europolovim centrom za kibernetički kriminal, CERT-ovima i nacionalnim tijelima za zaštitu podataka i jedinicama za borbu protiv kibernetičkog kriminala, razvijaju kulturu sigurnosti i pokrenu kampanje obrazovanja i podizanja svijesti kako bi se građanima omogućilo da donose informirane odluke o tome koje će osobne podatke stavljati na internet i kako će ih bolje zaštititi, uključujući uz pomoć šifriranja i sigurnog računarstva u oblaku, uz potpuno iskorištavanje platforme s informacijama od javnog interesa predviđene u Direktivi o univerzalnoj usluzi;

110. poziva Komisiju da do prosinca 2014. predstavi nacrt zakona o poticanju proizvođača softvera i hardvera da uvedu bolje značajke tehničke i integrirane sigurnosti i privatnosti u svoje proizvode uvođenjem kažnjavanja za nedozvoljeno i nerazmjerno prikupljanje masovnih osobnih podataka i pravne odgovornosti proizvođača za nepopravljanje poznatih ranjivosti, neispravnih ili nesigurnih proizvoda ili postavljanje tajnih stražnjih prolaza koja omogućuju neovlašteni pristup podacima i njihovu obradu; s time u vezi poziva Komisiju da ocijeni mogućnost uspostave programa za certificiranje ili validaciju IT hardvera, uključujući postupke ispitivanja na razini EU-a radi osiguravanja integriteta i sigurnosti proizvoda;

Ponovna izgradnja povjerenja

111. vjeruje da je istraga pokazala ne samo da je potrebna zakonodavna promjena, nego da SAD mora obnoviti povjerenje svojih partnera jer su u protivnom ugrožene aktivnosti američkih obavještajnih službi;

112. ističe da se nastala kriza nepovjerenja proširuje na:

— duh suradnje unutar EU-a jer neke nacionalne obavještajne aktivnosti mogu ugroziti ostvarivanje ciljeva Unije;

— građane, koji shvaćaju da ih možda špijuniraju ne samo treće zemlje ili multinacionalna poduzeća, već i njihova vlada;

— poštovanje temeljnih prava, demokracije i vladavine prava te vjerodostojnost demokratske, pravosudne i parlamentarne zaštite i nadzora u digitalnom društvu;

Između EU-a i SAD-a

113. podsjeća na važno povijesno i strateško partnerstvo između država članica EU-a i SAD-a, koje se temelji na zajedničkoj vjeri u demokraciju, vladavinu prava i temeljna prava;

114. vjeruje da je masovno nadziranje građana i špijuniranje političkih vođa koje je provodio SAD ozbiljno naštetilo odnosima između EU-a i SAD-a i imalo negativan utjecaj na povjerenje u organizacije SAD-a koje djeluju u EU-u; sve je to pogoršano nedostatkom sudskih i upravnih pravnih lijekova za građane EU-a u zakonima SAD-a, osobito u slučajevima nadzornih aktivnosti radi u obavještajne svrhe;

115. prepoznaje, u svjetlu globalnih izazova s kojima se suočavaju EU i SAD, da je potrebno dalje jačati transatlantsko partnerstvo i da je od ključne važnosti nastaviti s transatlantskom suradnjom na području borbe protiv terorizma na temelju novog povjerenja koje se zasniva na istinskom uzajamnom poštovanju vladavine prava i odbacivanju svih praksi općeg masovnog nadzora; stoga ustraje da SAD mora poduzeti jasne mjere za ponovnu uspostavu povjerenja i ponovno naglasiti zajedničke osnovne vrijednosti koje su temelj partnerstva;

116. spreman je aktivno sudjelovati u dijalogu s partnerima iz SAD-a, tako da se u okviru postojeće američke javne rasprave i rasprave u Kongresu o reformi nadzora i preispitivanju nadzora obavještajnih službi, građanima EU-a, osobama koje u njemu borave i drugim osobama koje se zaštićene pravom EU-a jamče pravo na privatnost, jednaka prava ina informiranje i zaštita privatnosti na sudovima u SAD-u primjerice revizijom Zakona o privatnosti i Zakona o privatnosti u području elektroničkih komunikacija te ratifikacijom Prvog fakultativnog protokola Međunarodnog pakta o građanskim i političkim pravima (ICCPR), tako da se postojeća diskriminacija ne nastavi;

117. ustraje na tome da je potrebno provesti odgovarajuće reforme i Europljanima pružiti učinkovita jamstva da će nadzor i obrada podataka za potrebe stranih obavještajnih službi biti razmjerni i ograničeni u skladu s jasno definiranim uvjetima i na slučajeve utemeljene ili opravdane sumnje u terorističke aktivnosti; ističe da ta svrha mora biti podložna transparentnoj sudskoj kontroli;

118. smatra da su potrebni jasni politički signali naših američkih partnera iz kojih će se vidjeti da SAD razlikuje između saveznika i suparnika;

119. potiče Komisiju i vladu SAD-a da, u kontekstu tekućih pregovora o krovnom sporazumu između EU-a i SAD-a o prijenosu podataka u svrhe provedbe zakona, riješi problem informiranja i sudskih pravnih lijekova za građane EU-a i da završi te pregovore, u skladu s obvezama koje su EU i SAD preuzele na ministarskom sastanku za pravosuđe i unutarnje poslove od 18. studenog 2013., prije ljeta 2014.;

120. potiče SAD da pristupi Konvenciji Vijeća Europe o zaštiti osoba glede automatske obrade osobnih podataka (Konvencija 108), kao što je pristupila Konvenciji o kibernetičkom kriminalu iz 2001., na taj način jačajući zajedničku pravnu osnovu među transatlantskim saveznicima;

121. poziva institucije EU-a da istraže mogućnosti za uspostavu kodeksa ponašanja sa SAD-om kojim bi se jamčilo da SAD ne može vršiti špijuniranje protiv institucija i tijela EU-a;

U Europskoj uniji

122. također vjeruje da su uključenost i aktivnosti država članica EU-a dovele do gubitka povjerenja, uključujući među državama članicama te između građana i vlasti njihovih država članica; smatra da će se samo na temelju potpune otvorenosti o svrsi i sredstvima nadzora, javnom raspravom i revizijom zakonodavstva te praksama za okončanje aktivnosti masovnog nadzora i jačanje sustava sudskog i parlamentarnog nadzora, omogućiti ponovna uspostava izgubljenog povjerenja; ponavlja da je teško razviti sveobuhvatne politike EU-a o sigurnosti dokle god se provode aktivnosti masovnog nadzora i naglašava da načelo EU-a iskrene suradnje nalaže državama članicama da se suzdrže od provođenja obavještajnih aktivnosti na državnom području drugih država članica;

123. primjećuje da neke države članice održavaju bilateralnu komunikaciju s vlastima SAD-a o navodima o špijunaži i da su neke od njih sklopile (Ujedinjena Kraljevina) ili su u postupku sklapanja (Njemačka, Francuska) takozvanih sporazuma o „nešpijuniranju"; ističe da te države članice moraju u potpunosti voditi računa o interesima i zakonodavnom okviru EU-a u cjelini; smatra da su takvi bilateralni sporazumi kontraproduktivni i nevažni jer je za taj problem potrebno europsko rješenje; traži od Vijeća da obavijesti Parlament o potezima država članica u vezi sa zajedničkim sporazumom o nešpijuniranju na razini EU-a;

124. smatra da takvi sporazumi ne bi smjeli biti protivni Europskim ugovorima, posebno u odnosu na načelo iskrene suradnje (Članak 4. stavak 3. UEU-a) ili narušavati politike EU-a općenito, a posebno politike unutarnjeg tržišta, poštenog tržišnog natjecanja i gospodarskog, industrijskog i društvenog razvoja; odlučio je pregledati sve takve sporazume u smislu njihove sukladnosti s europskim pravom i zadržava pravo aktivirati postupke iz Ugovora u slučaju da su takvi sporazumi protivni koheziji Unije ili temeljnim načelima na kojima se ona zasniva;

125. poziva države članice da poduzmu sve što je u njihovoj moći da poboljšaju suradnju s ciljem pružanju jamstava o nepostojanju špijuniranja u suradnji s nadležnim tijelima i agencijama EU-a kako bi se zaštitili građani i institucije EU-a, europska poduzeća, industrija EU-a, informatička infrastruktura i mreže te europsko istraživanje; smatra da je aktivno sudjelovanje dionika EU-a preduvjet za djelotvornu razmjenu informacija; ističe da su sigurnosne prijetnje postale sve internacionalnije, raznovrsnije i složenije, što nalaže pojačanu europsku suradnju; vjeruje da bi Ugovori trebali bolje održavati takvu situaciju i stoga poziva na reviziju Ugovora kako bi se osnažila ideja iskrene suradnje između država članica i Unije u pogledu cilja postizanja prostora sigurnosti i sprečavanja uzajamnog špijuniranja među državama članicama unutar Unije;

126. smatra da su u svim relevantnim institucijama EU-a i delegacijama EU-a krajnje potrebne komunikacijske strukture otporne na prisluškivanje (e-pošta i telekomunikacije, uključujući fiksni i mobilni telefon) i dvorane za sastanke otporne na prisluškivanje; stoga poziva na uspostavu šifriranog internog sustava elektroničke pošte EU-a;

127. poziva Vijeće i Komisiju da bez daljnjeg odlaganja daju svoj pristanak prijedlogu Uredbe Europskog parlamenta o detaljnim odredbama o izvršavanju prava Europskog parlamenta na istragu i stavljanju izvan snage Odluke 95/167/EZ, Euratom, EZUČ Europskog parlamenta, Vijeća i Komisije predstavljene na temelju članka 226. UFEU-a, koji je Europski parlament usvojio 23. svibnja 2012.; poziva na reviziju Ugovora s ciljem proširenja istražnih ovlasti tako da obuhvaćaju, bez ograničenja ili iznimki, sva područja nadležnosti ili aktivnosti Unije i mogućnost saslušanja pod prisegom;

Međunarodno

128. poziva Komisiju da najkasnije do siječnja 2015. predstavi strategiju EU-a za demokratsko upravljanje internetom;

129. poziva države članice da se odazovu na poziv na 35. međunarodnu konferenciju povjerenika za zaštitu podataka i privatnost „radi zagovaranja donošenja dodatnog protokola uz članak 17. Međunarodnog pakta o građanskim i političkim pravima (ICCPR), koji bi se trebao temeljiti na načelima koje je razvila i potvrdila Međunarodna konferencija i odredbama Opće napomene br. 16. Odbora za ljudska prava uz Pakt radi stvaranja globalno primjenjivih standarda zaštite podataka i zaštite privatnosti u skladu s vladavinom prava"; poziva države članice da u taj postupak uključe poziv da međunarodna agencija UN-a bude nadležna osobito za praćenje pojave alata za nadziranje te za regulaciju i istragu njihove upotrebe; poziva Visoku predstavnicu/Potpredsjednicu Komisije i Europske službe za vanjsko djelovanje da zauzme proaktivan stav;

130. poziva države članice da razviju dosljednu i snažnu strategiju u okviru Ujedinjenih naroda, kojom će posebno podržati rezoluciju o „pravu na privatnost u digitalnom dobu", koju su pokrenuli Brazil i Njemačka, i koja je usvojena 27. studenog 2013. na trećem Odboru Opće skupštine UN-a (Odbor za ljudska prava), te da nastave s mjerama za zaštitu privatnosti i zaštitu podataka na međunarodnoj razini istovremeno izbjegavajući omogućavanje državnog nadzora ili cenzure ili fragmentacije interneta, uključujući inicijativu za međunarodni sporazum kojim bi se zabranile aktivnosti masovnog nadzora i za osnivanje agencije za nadzor tog sporazuma;

Plan prioriteta: Europski digitalni Habeas Corpus – zaštita temeljnih prava u digitalnom dobu

131. odlučuje dostaviti građanima EU-a, institucijama i državama članicama gore navedene preporuke u obliku Plana prioriteta za sljedeći parlamentarni saziv; poziva Komisiju i ostale institucije, tijela, urede i agencije EU-a navedene u ovoj Rezoluciji da u skladu s člankom 265. UFEU-a postupaju u skladu s preporukama i pozivima iz ove Rezolucije;

132. odlučuje pokrenuti program „Europski digitalni Habeas Corpus – zaštita temeljnih prava u digitalnom dobu" sa sljedećih osam aktivnosti, čiju će provedbu nadzirati:

— Aktivnost 1.: donijeti Paket za zaštitu podataka u 2014.;

— Aktivnost 2.: sklopiti Krovni sporazum između EU-a i SAD-a kojim će se građanima EU-a jamčiti temeljno pravo na privatnost i zaštitu podataka te osigurati odgovarajući pravni lijekovi, uključujući u slučaju prijenosa podataka iz EU-a u SAD za potrebe provedbe zakona;

— Aktivnost 3.: obustaviti Sigurnu luku do provedbe potpunog preispitivanja i popravka trenutnih nedostataka, osiguravajući pritom da se prijenos osobnih podataka za komercijalne potrebe iz Unije u SAD može izvršavati samo u skladu s najvišim standardima EU-a;

— Aktivnost 4.: obustaviti primjenu sporazuma FTP do: (i) okončanja pregovora o Krovnom sporazumu; (ii) okončanja detaljne istrage na temelju analize EU-a i odgovarajućeg rješenja svih pitanja koje je Parlament postavio u svojoj rezoluciji od 23. listopada 2013.;

— Aktivnost 5.: ocijeniti svaki sporazum, mehanizam ili razmjenu podataka s trećim zemljama koji uključuju osobne podatke kako bi se osiguralo da pravo na privatnost i zaštitu osobnih podataka nije prekršeno uslijed aktivnosti nadzora te kako bi se poduzele potrebne naknadne mjere;

— Aktivnost 6.: zaštititi vladavinu prava i temeljna prava građana EU-a (uključujući od prijetnji slobodi medija), pravo javnosti na nepristranu informaciju i odnos povjerljivosti (uključujući odnose između odvjetnika i klijenta) uz pojačanu zaštitu zviždača;

— Aktivnost 7.: razviti Europsku strategiju za neovisnost IT sustava (digitalni „novi deal" uključujući dodjelu odgovarajućih financijskih sredstava na nacionalnoj razini i razini EU-a) kako bi se unaprijedila industrija IT-a i omogućilo europskim poduzećima da iskoriste konkurentsku prednost EU-a u pogledu privatnosti;

— Aktivnost 8.: razviti EU kao referentni model za demokratsko i neutralno upravljanje internetom;

133. poziva institucije EU-a i države članice da promiču program „Europski digitalni Habeas Corpus" za zaštitu temeljnih prava u digitalnom dobu; preuzima obvezu zastupanja građanskih prava građana EU-a, uz sljedeći raspored za praćenje provedbe;

— travanj 2014. – ožujak 2015. skupina za praćenje utemeljena na istražnom timu LIBE koji je odgovoran za praćenje svih novih otkrića o mandatu istrage i za strogo praćenje provedbe ove Rezolucije;

— od srpnja 2014. na dalje: stalni mehanizam nadzora za prijenos podataka i sudske lijekove u okviru nadležnog odbora;

— proljeće 2014.: službeni poziv Europskom vijeću da uključi „Europski digitalni Habeas Corpus – zaštita temeljnih prava u digitalnom dobu" u smjernice koje će biti donesene u skladu s člankom 68. UFEU-a;

— jesen 2014.: obveza da će „Europski digitalni Habeas Corpus – zaštita temeljnih prava u digitalnom dobu" i povezane preporuke služiti kao ključan kriterij za odobrenje sljedeće Komisije;

— 2014.: konferencija na kojoj će se okupiti europski stručnjaci na visokoj razini u različitim područjima koja doprinose IT sigurnosti (uključujući matematiku, kriptografiju i tehnologije za jačanje privatnosti) i pomoći u stvaranju strategije EU-a za IT za sljedeći sastav zakonodavnog tijela;

— 2014. – 2015.: redovno sazivanje skupine za povjerenje/podatke i građanska prava između Europskog parlamenta i američkog Kongresa te s drugim relevantnim parlamentima trećih zemalja, uključujući Brazil;

— 2014. – 2015.: konferencija s nadzornim tijelima za obavještajne službe europskih nacionalnih parlamenata;

o

o o

134. nalaže svom Predsjedniku da proslijedi ovu rezoluciju Europskom Vijeću, Vijeću, Komisiji, parlamentima i vladama država članica, nacionalnim tijelima za zaštitu podataka, EDPS-u, eu-LISA-i, ENISA-i, Agenciji za temeljna prava, radnoj skupini na temelju članka 29., Vijeću Europe, Kongresu Sjedinjenih Američkih Država, Vladi SAD-a, Predsjedniku, Vladi i parlamentu Savezne Republike Brazil i Glavnom tajniku Ujedinjenih naroda.

135. nalaže svom Odboru za građanske slobode, pravosuđe i unutarnje poslove da se o tom pitanju očituje Parlamentu na plenarnoj sjednici godinu dana nakon donošenja ove Rezolucije; smatra da je neophodno ocijeniti u kojem se opsegu poštuje preporuke koje je Parlament usvojio i analizirati sve slučajeve u kojima se *takve preporuke ne poštuje;*