Trešdiena, 2014. gada 12. marta

P7_TA(2014)0230

ASV Nacionālās drošības aģentūras novērošanas programma, novērošanas struktūras dažādās dalībvalstīs un ietekme uz ES pilsoņu pamattiesībām

Eiropas Parlamenta 2014. gada 12. marta rezolūcija par ASV Nacionālās drošības aģentūras novērošanas programmu, novērošanas struktūrām dažādās dalībvalstīs un ietekmi uz ES pilsoņu pamattiesībām un transatlantisko sadarbību tieslietu un iekšlietu jomā (2013/2188(INI))

(2017/C 378/14)

Eiropas Parlaments,

— ņemot vērā Līgumu par Eiropas Savienību (LES), jo īpaši tā 2., 3., 4., 5., 6., 7., 10., 11. un 21. pantu,

— ņemot vērā Līgumu par Eiropas Savienības darbību (LESD), jo īpaši tā 15., 16. un 218. pantu un V sadaļu,

— ņemot vērā 36. protokolu par pārejas noteikumiem un tā 10. pantu, kā arī 50. deklarāciju attiecībā uz šo protokolu,

— ņemot vērā Eiropas Savienības Pamattiesību hartu, jo īpaši tās 1., 3., 6., 7., 8., 10., 11., 20., 21., 42., 47., 48. un 52. pantu,

— ņemot vērā Eiropas Cilvēktiesību konvenciju, jo īpaši tās 6., 8., 9., 10. un 13. pantu, un tās protokolus,

— ņemot vērā Vispārējo cilvēktiesību deklarāciju, jo īpaši tās 7., 8., 10., 11., 12. un 14. pantu ([1]),

— ņemot vērā Starptautisko paktu par pilsoniskajām un politiskajām tiesībām, jo īpaši tā 14., 17., 18. un 19. pantu,

— ņemot vērā Eiropas Padomes Konvenciju par datu aizsardzību (ELS Nr. 108) un Eiropas Padomes Konvencijas par personu aizsardzību attiecībā uz personas datu automātisko apstrādi 2001. gada 8. novembra Papildu protokolu par uzraudzības institūcijām un pārrobežu datu plūsmām (ELS Nr. 181),

— ņemot vērā Vīnes konvenciju par diplomātiskajiem sakariem, jo īpaši tās 24., 27. un 40. pantu,

— ņemot vērā Eiropas Padomes Konvenciju par kibernoziegumiem (ELS Nr. 185),

— ņemot vērā ziņojumu ([2]), ko 2010. gada 17. maijā iesniedza ANO īpašais referents jautājumos par cilvēktiesību un pamatbrīvību veicināšanu un aizsardzību terorisma apkarošanā,

— ņemot vērā Komisijas paziņojumu "Interneta politika un pārvaldība. Eiropas uzdevumi interneta pārvaldības nākotnes veidošanā" (COM(2014)0072);

— ņemot vērā ziņojumu ([3]), ko 2013. gada 17. aprīlī iesniedza ANO īpašais referents jautājumos par tiesību uz uzskatu un vārda brīvību veicināšanu un aizsardzību,

— ņemot vērā Vadlīnijas par cilvēktiesībām un cīņu pret terorismu, ko 2002. gada 11. jūlijā pieņēma Eiropas Padomes Ministru komiteja,

([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

— ņemot vērā 2010. gada 1. oktobra Briseles deklarāciju, kas tika pieņemta Eiropas Savienības dalībvalstu izlūkošanas un drošības dienestu uzraudzības parlamentāro komiteju 6. konferencē,

— ņemot vērā Eiropas Padomes Parlamentārās asamblejas Rezolūciju Nr. 1954 (2013) par valsts drošību un informācijas pieejamību,

— ņemot vērā ziņojumu par drošības dienestu demokrātisko uzraudzību ([1]), ko 2007. gada 11. jūnijā pieņēma Venēcijas komisija, un ar lielu interesi gaidot atjaunināto ziņojumu, ko paredzēts pieņemt 2014. gada pavasarī,

— ņemot vērā Beļģijas, Nīderlandes, Dānijas un Norvēģijas izlūkošanas uzraudzības komiteju pārstāvju liecības,

— ņemot vērā Francijas ([2]), Polijas un Apvienotās Karalistes ([3]) tiesās, kā arī Eiropas Cilvēktiesību tiesā ([4]) iesniegtās lietas attiecībā uz masveida novērošanas sistēmām,

— ņemot vērā Konvenciju par Eiropas Savienības dalībvalstu savstarpēju palīdzību krimināllietās, ko Padome izstrādājusi saskaņā ar Līguma par Eiropas Savienību 34. pantu ([5]) un jo īpaši tā III sadaļu,

— ņemot vērā Komisijas 2000. gada 26. jūlija Lēmumu Nr. 2000/520/EK par pienācīgu aizsardzību, kas noteikta ar privātuma "drošības zonas" principiem un attiecīgajiem visbiežāk uzdotajiem jautājumiem, kurus izdevusi ASV Tirdzniecības ministrija,

— ņemot vērā Komisijas 2002. gada 13. februāra (SEC(2002)0196) un 2004. gada 20. oktobra (SEC(2004)1323) novērtējuma ziņojumus par privātuma "drošības zonas" principu īstenošanu,

— ņemot vērā Komisijas 2013. gada 27. novembra paziņojumu par "drošības zonas" darbību no ES pilsoņu un uzņēmumu, kas veic uzņēmējdarbību ES, viedokļa (COM(2013)0847) un Komisijas 2013. gada 27. novembra paziņojumu par uzticēšanās atjaunošanu datu plūsmām starp ES un ASV (COM(2013)0846),

— ņemot vērā 2000. gada 5. jūlija rezolūciju par Komisijas lēmuma projektu par pienācīgu aizsardzību, kas noteikta ar privātuma "drošības zonas" principiem un attiecīgajiem visbiežāk uzdotajiem jautājumiem, kurus izdevusi ASV Tirdzniecības ministrija ([6]), un šajā rezolūcijā pausto uzskatu, ka šī sistēma nenodrošina pienācīgu aizsardzību, un 29. panta darba grupas atzinumus, jo īpaši 2000. gada 16. maija Atzinumu Nr. 4/2000 ([7]),

— ņemot vērā 2004., 2007. ([8]) un 2012. gada ([9]) nolīgumus starp Amerikas Savienotajām Valstīm un Eiropas Savienību par pasažieru datu reģistra datu izmantošanu un pārsūtīšanu (PDR nolīgumi),

— ņemot vērā kopīgo pārskatu par Nolīguma starp ES un ASV par pasažieru datu reģistra datu apstrādi un pārsūtīšanu ASV Iekšzemes drošības departamentam īstenošanu ([10]), kas pievienots Komisijas ziņojumam Eiropas Parlamentam un Padomei par kopīgo pārskatu (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 un La Ligue française pour la défense des droits de l'Homme et du Citoyen*/X; *Tribunal de Grande Instance de Paris*.
([3]) Izmeklēšanas pilnvaru tribunālā iesniegtās *Privacy International* un *Liberty* lietas.
([4]) Kopīgs pieteikums saskaņā ar 34. pantu, ko iesniedza *Big Brother Watch, Open Rights Group, English Pen Dr Constanze Kurz* (pieteikuma iesniedzēji)/Apvienotā Karaliste (atbildētājs).
([5]) OV C 197, 12.7.2000., 1. lpp.
([6]) OV C 121, 24.4.2001., 152. lpp.
([7]) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp32en.pdf
([8]) OV L 204, 4.8.2007., 18. lpp.
([9]) OV L 215, 11.8.2012., 5. lpp.
([10]) SEC(2013)0630, 27.11.2013.

Trešdiena, 2014. gada 12. marta

— ņemot vērā ģenerāladvokāta *Cruz Villalón* atzinumu, kurā secināts, ka Direktīva 2006/24/EK par tādu datu saglabāšanu, kurus iegūst vai apstrādā saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu vai publiski pieejamu komunikāciju tīklu nodrošināšanu, kopumā neatbilst Eiropas Savienības Pamattiesību hartas 52. panta 1. punktam un ka tās 6. pants neatbilst Pamattiesību hartas 7. pantam un 52. panta 1. punktam ([1]),

— ņemot vērā Padomes 2010. gada 13. jūlija Lēmumu 2010/412/ES par to, lai noslēgtu Nolīgumu starp Eiropas Savienību un Amerikas Savienotajām Valstīm par tādu finanšu ziņojumapmaiņas datu apstrādi un nodošanu, kurus Eiropas Savienība dara pieejamus ASV, lai īstenotu Teroristu finansēšanas izsekošanas programmu (*TFTP*) ([2]), un šim lēmumam pievienotās Komisijas un Padomes deklarācijas,

— ņemot vērā nolīgumu par savstarpējo juridisko palīdzību starp Eiropas Savienību un Amerikas Savienotajām Valstīm ([3]),

— ņemot vērā notiekošās sarunas par ES un ASV pamatnolīgumu par personas datu aizsardzību, tos pārsūtot un apstrādājot, lai novērstu, izmeklētu un atklātu noziedzīgus nodarījumus, tostarp terorismu, un sauktu pie atbildības par tiem, īstenojot policijas un tiesu iestāžu sadarbību krimināllietās ("jumta nolīgums"),

— ņemot vērā Padomes 1996. gada 22. novembra Regulu (EK) Nr. 2271/96, ar ko paredz aizsardzību pret trešās valsts pieņemtu tiesību aktu eksteritoriālas piemērošanas sekām un no tiem izrietošām vai ar tiem pamatotām darbībām ([4]),

— ņemot vērā Brazīlijas Federatīvās Republikas prezidenta paziņojumu ANO Ģenerālās asamblejas 68. sesijas atklāšanā 2013. gada 24. septembrī un darbu, ko paveikusi Brazīlijas Federālā senāta izveidotā Spiegošanas izmeklēšanas parlamentārā komiteja,

— ņemot vērā ASV "Patriota aktu" (*Patriot Act*), ko 2001. gada 26. oktobrī parakstīja ASV prezidents *George W. Bush*,

— ņemot vērā 1978. gada Ārvalstu izlūkošanas novērošanas aktu (*FISA*) un 2008. gada *FISA* grozījumu aktu,

— ņemot vērā Izpildrīkojumu Nr. 12333, ko ASV prezidents izdeva 1981. gadā un grozīja 2008. gadā,

— ņemot vērā Prezidenta politikas direktīvu (*PPD-28*) par signālu izlūkošanas pasākumiem, ko izdevis ASV prezidents *Barack Obama* 2014. gada 17. janvārī,

— ņemot vērā tiesību aktu priekšlikumus, kurus patlaban izskata ASV Kongress, tostarp ASV Brīvības akta projektu, Izlūkošanas uzraudzības un novērošanas reformu akta projektu un citus,

— ņemot vērā Privātuma un pilsonisko brīvību uzraudzības padomes, ASV Nacionālās drošības padomes un Prezidenta izlūkdatu un komunikāciju tehnoloģiju pārbaudes grupas veiktās pārbaudes, jo īpaši pārbaudes grupas 2013. gada 12. decembra ziņojumu "Brīvība un drošība mainīgā pasaulē",

— ņemot vērā ASV Kolumbijas apgabaltiesas 2013. gada 16. decembra lēmumu par civilprasību Nr. 13-0851 lietā *Klayman* u. c./*Obama* u. c. un ASV Ņujorkas dienvidu rajona apgabaltiesas 2013. gada 11. jūnija lēmumu par civilprasību Nr. 13-3994 lietā *ACLU* u. c./*James R. Clapper* u. c.,

— ņemot vērā 2013. gada 27. novembra ziņojumu par ES un ASV Datu aizsardzības jautājumu *ad hoc* darba grupas ES līdzpriekšsēdētāju konstatējumiem ([5]),

([1]) Ģenerāladvokāta *Cruz Villalón* 2013. gada 12. decembra atzinums lietā C-293/12.
([2]) OV L 195, 27.7.2010., 3. lpp.
([3]) OV L 181, 19.7.2003., 34. lpp.
([4]) OV L 309, 29.11.1996., 1. lpp.
([5]) Padomes dokuments Nr. 16987/2013.

— ņemot vērā 2001. gada 5. septembra ([1]) un 2002. gada 7. novembra ([2]) rezolūcijas par tādas globālas sistēmas pastāvēšanu, ar kuru pārtver privātu un komerciāla rakstura saziņu (*Echelon* pārtveršanas sistēma),

— ņemot vērā Parlamenta 2013. gada 21. maija rezolūciju par ES hartu — standartu noteikšanu attiecībā uz plašsaziņas līdzekļu brīvību Eiropas Savienībā ([3]),

— ņemot vērā 2013. gada 4. jūlija rezolūciju par ASV Nacionālās drošības aģentūras novērošanas programmu, novērošanas struktūrām vairākās dalībvalstīs un to ietekmi uz ES pilsoņu privātumu ([4]), ar ko tas uzdeva Pilsoņu brīvību, tieslietu un iekšlietu komitejai veikt padziļinātu izmeklēšana par šo jautājumu,

— ņemot vērā 1. darba dokumentu par ASV un ES novērošanas programmām un to ietekmi uz ES iedzīvotāju pamattiesībām,

— ņemot vērā 3. darba dokumentu par attiecībām starp novērošanas praksi ES un ASV un ES datu aizsardzības noteikumiem,

— ņemot vērā 4. darba dokumentu par ASV novērošanas pasākumiem attiecībā uz ES datiem un to iespējamo ietekmi uz transatlantiskajiem nolīgumiem un sadarbību,

— ņemot vērā 5. darba dokumentu par dalībvalstu izlūkdienestu un ES izlūkošanas struktūru demokrātisku uzraudzību,

— ņemot vērā AFET darba dokumentu par ES pilsoņu masveida elektroniskās novērošanas izmeklēšanas ārpolitikas aspektiem;

— ņemot vērā Parlamenta 2013. gada 23. oktobra rezolūciju par organizēto noziedzību, korupciju un nelikumīgi iegūtu līdzekļu legalizēšanu — ieteicamie pasākumi un iniciatīvas ([5]),

— ņemot vērā 2013. gada 23. oktobra rezolūciju par *TFTP* nolīguma darbības apturēšanu ASV Nacionālās drošības aģentūras veiktās novērošanas dēļ ([6]),

— ņemot vērā 2013. gada 10. decembra rezolūciju par mākoņdatošanas potenciāla atraisīšanu Eiropā ([7]),

— ņemot vērā iestāžu nolīgumu starp Eiropas Parlamentu un Padomi par to, kā Eiropas Parlamentam nosūta un kā tas apstrādā Padomes rīcībā esošo klasificēto informāciju par jautājumiem, kas nav kopējās ārpolitikas un drošības politikas darbības jomā ([8]),

— ņemot vērā Reglamenta VIII pielikumu,

— ņemot vērā Reglamenta 48. pantu,

— ņemot vērā Pilsoņu brīvību, tieslietu un iekšlietu komitejas ziņojumu (A7-0139/2014),

Masveida novērošanas ietekme

A. tā kā datu aizsardzība un privātums ir pamattiesības; tā kā tādēļ drošības pasākumi, tostarp terorisma apkarošanas pasākumi, jāveic, ievērojot tiesiskumu, un tiem ir jāatbilst pienākumam ievērot pamattiesības, tostarp tās, kas saistītas ar privātumu un datu aizsardzību;

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

B. tā kā informācijas plūsmām un datiem, kas mūsdienās ietekmē ikdienas dzīvi un ir daļa no ikvienas personas integritātes, ir jābūt drošībā tāpat kā privātiem mājokļiem;

C. tā kā saites starp Eiropu un Amerikas Savienotajām Valstīm balstās uz demokrātijas, tiesiskuma, brīvības, taisnīguma un solidaritātes garu un principiem;

D. tā kā sadarbība starp ASV un Eiropas Savienību un tās dalībvalstīm terorisma apkarošanas jomā arvien ir ļoti svarīga abu partneru aizsardzībai un drošībai;

E. tā kā savstarpēja uzticēšanās un izpratne ir transatlantiskā dialoga un partnerības galvenie faktori;

F. tā kā pēc 2001. gada 11. septembra vairākumam valdību cīņa pret terorismu kļuva par vienu no galvenajām prioritātēm; tā kā to atklājumu dēļ, kuru pamatā ir ziņotāja un Nacionālās drošības aģentūras (NDA) bijušā līgumdarbinieka *Edward Snowden* nopludinātie dokumenti, politiskajiem vadītājiem ir jārisina problēmas saistībā ar izlūkošanas aģentūru uzraudzību un kontroli novērošanas darbībās un jānovērtē to ietekme uz pamattiesībām un tiesiskumu demokrātiskā sabiedrībā;

G. tā kā šie atklājumi kopš 2013. gada jūnija Eiropas Savienībā ir izraisījuši daudz bažu par:

— gan ASV, gan ES dalībvalstīs atklāto novērošanas sistēmu darbības apmēru,

— to, ka tiek pārkāpti ES tiesību standarti, pamattiesības un datu aizsardzības standarti,

— uzticības pakāpi starp ES un ASV transatlantiskajiem partneriem,

— dažu ES dalībvalstu sadarbības un līdzdalības apmēru ASV novērošanas programmās vai līdzvērtīgās programmās valsts līmenī, kā to atklājuši plašsaziņas līdzekļi,

— politisko iestāžu un dažu ES dalībvalstu kontroles un efektīvas uzraudzības trūkumu attiecībā uz saviem izlūkdienestiem,

— iespēju, ka šie masveida novērošanas pasākumi tiek izmantoti mērķiem, kas nav saistīti ar valsts drošību un cīņu pret terorismu vistiešākajā nozīmē, piemēram, ekonomiskajai un rūpnieciskajai spiegošanai vai profilēšanai politisku iemeslu dēļ,

— to, ka tiek apdraudēta preses brīvība un konfidencialitātes privilēģija komunikācijā ar tādu profesiju pārstāvjiem kā juristi un ārsti,

— izlūkošanas aģentūru un privātu IT un telekomunikāciju uzņēmumu attiecīgajām lomām un līdzdalības apmēru,

— aizvien neskaidrākajām robežām starp tiesībaizsardzības un izlūkošanas darbībām, kā rezultātā pret ikvienu iedzīvotāju izturas kā pret aizdomās turēto un kā pret personu, kas jāuzrauga,

— digitālajā laikmetā apdraudēto privātumu un masveida novērošanas ietekmi uz iedzīvotājiem un sabiedrībām;

H. tā kā, ņemot vērā konstatētās spiegošanas nepieredzēto apmēru, ASV iestādēm, Eiropas iestādēm, dalībvalstu valdībām, valstu parlamentiem un tiesu iestādēm ir jāveic pilna izmeklēšana;

I. tā kā daļu no atklātās informācijas ASV iestādes ir noliegušas, bet lielu tās daļu nav apstrīdējušas; tā kā ASV un noteiktās ES dalībvalstīs ir izvērsušās plašas publiskās debates; tā kā ES valdības un parlamenti pārāk bieži ieņem pasīvu pozīciju un neuzsāk pienācīgu izmeklēšanu;

J. tā kā nesen prezidents *B. Obama* paziņoja par NDA un tās novērošanas programmu reformu;

K. tā kā salīdzinājumā gan ar ES iestāžu, gan ar noteiktu ES dalībvalstu veiktajiem pasākumiem Eiropas Parlaments ir ļoti nopietni uztvēris savu pienākumu informēt par atklājumiem saistībā ar ES iedzīvotāju masveida novērošanas pasākumiem un savā 2013. gada 4. jūlija rezolūcijā par ASV Nacionālās drošības aģentūras novērošanas programmu, novērošanas struktūrām dažādās dalībvalstīs un to ietekmi uz ES iedzīvotājiem tas ir uzdevis Pilsoņu brīvības, tieslietu un iekšlietu komitejai veikt šā jautājuma padziļinātu izpēti;

L. tā kā Eiropas iestāžu pienākums ir nodrošināt, ka ES tiesību akti tiek pilnībā īstenoti Eiropas iedzīvotāju labā un ka ES Līgumu juridisko spēku nemazina trešo valstu standartu vai rīcības eksteritoriālo seku vienaldzīga pieņemšana;

Izlūkošanas politikas reformas norise ASV

M. tā kā saskaņā ar Kolumbijas apgabaltiesas 2013. gada 16. decembra lēmumu NDA, masveidā ievācot metadatus, ir pārkāpusi ASV Konstitūcijas Ceturto grozījumu ([1]); tā kā tomēr Ņujorkas dienvidu rajona apgabaltiesa savā 2013. gada 27. decembra lēmumā atzina, ka šī datu ievākšana bija likumīga;

N. tā kā saskaņā ar Mičiganas austrumu apgabaltiesas lēmumu Ceturtais grozījums paredz, ka meklēšanai vienmēr ir jābūt pamatotai, ka tā jāveic saskaņā ar iepriekšēju pilnvaru, ka pilnvaras pamatā ir jābūt iepriekš konstatētam iespējamam iemeslam, kā arī jābūt konkrētībai attiecībā uz personām, vietu un lietām un ir jānodrošina neitrāla tiesneša starpniecība starp izpildvaras amatpersonām un iedzīvotājiem ([2]);

O. tā kā Prezidenta izlūkdatu un komunikāciju tehnoloģiju pārbaudes grupa savā 2013. gada 12. decembra ziņojumā Amerikas Savienoto Valstu prezidentam sniedza 46 ieteikumus; tā kā šajos ieteikumos ir uzsvērts, ka vienlaikus ir jāaizsargā valsts drošība, kā arī personu privātums un pilsoniskās brīvības; tā kā šajā sakarībā tā aicina ASV valdību pēc iespējas ātrāk izbeigt ASV iedzīvotāju telefonsarunu datu masveida vākšanu saskaņā ar "Patriota akta" 215. sadaļu; sākt rūpīgu NDA un ASV izlūkošanas tiesiskā regulējuma pārskatīšanu, lai nodrošinātu privātuma tiesību ievērošanu; izbeigt centienus uzlauzt vai padarīt neaizsargātu komerciālo programmatūru (izmantojot aizsardzības sistēmu apiešanas ceļus un ļaunprogrammatūru); pastiprināt šifru izmantošanu, jo īpaši datu pārraides gadījumā, un nemazināt centienus ieviest šifrēšanas standartus; izveidot sabiedrības interešu aizstāvības struktūru, kas Ārvalstu izlūkošanas novērošanas tiesā aizstāvētu privātumu un pilsoniskās tiesības; piešķirt Privātuma un pilsonisko brīvību uzraudzības padomei pilnvaras pārraudzīt izlūkdienestu darbību ārvalstu izlūkošanas, nevis tikai terorisma apkarošanas mērķiem un saņemt ziņotāju sūdzības; izmantot savstarpējās tiesiskās palīdzības līgumus, lai saņemtu elektroniskos paziņojumus, un neizmantot novērošanu rūpniecības vai tirdzniecības noslēpumu zagšanas nolūkā;

P. tā kā saskaņā ar atklāto memorandu, ko 2014. gada 7. janvārī prezidentam *B. Obama* iesniedza bijušie NDA vadošie darbinieki/izlūkošanas profesionālie veterāni par veselo saprātu (*Veteran Intelligence Professionals for Sanity — VIPS*) ([3]), masveida datu ievākšana neveicina spēju novērst turpmākos teroristu uzbrukumus; tā kā tā autori uzsver, ka NDA veiktās masveida novērošanas rezultātā nav novērsts neviens uzbrukums un ka ir iztērēti miljardiem dolāru programmās, kuras ir neefektīvākas un daudz plašāk un vairāk iejaucas iedzīvotāju privātumā nekā iekšzemes tehnoloģija *THINTHREAD*, ko izveidoja 2001. gadā;

Q. tā kā attiecībā uz izlūkošanas darbībām, kuras saskaņā ar *FISA* 702. sadaļu piemēro personām, kas nav ASV pilsoņi, ieteikumos ASV prezidentam ir atzīts būtiskais princips par privātuma un cilvēka cieņas ievērošanu, kā noteikts Vispārējās cilvēktiesību deklarācijas 12. pantā un Starptautiskā pakta par pilsoniskajām un politiskajām tiesībām 17. pantā; tā kā saskaņā ar šiem ieteikumiem personām, kas nav ASV pilsoņi, netiek nodrošinātas tādas pašas tiesības un aizsardzība kā ASV pilsoņiem;

([1]) Civilprasība Nr. 13-0851 lietā *Klayman* u. c./*Obama* u. c., 2013. gada 16. decembris.
([2]) *ACLU*/NDA, Nr. 06-CV-10204, 2006. gada 17. augusts.
([3]) http://consortiumnews.com/2014/01/07/nsa-insiders-reveal-what-went-wrong.

R. tā kā savā 2014. gada 17. janvāra Prezidenta politikas direktīvā par signālu izlūkošanas pasākumiem un saistītajā runā ASV prezidents *Barack Obama* norādīja, ka masveida elektroniskā izlūkošana ir nepieciešama Amerikas Savienotajām Valstīm, lai aizsargātu savas valsts drošību, iedzīvotājus un ASV sabiedroto un partneru iedzīvotāju drošību, kā arī lai veicinātu to ārpolitikas intereses; tā kā politikas direktīvā ir ietverti konkrēti principi par signālu izlūkdatu vākšanu, izmantošanu un apmaiņu ar tiem un ar to tiek paplašināti noteikti tiesiskās aizsardzības līdzekļi personām, kas nav ASV pilsoņi, daļēji nodrošinot attieksmi, kas ir līdzvērtīga tai, kāda ir pret ASV pilsoņiem, tostarp arī aizsargājot visu iedzīvotāju personisko informāciju aizsardzību neatkarīgi no viņu valstspiederības vai dzīvesvietas; tā kā prezidents *B. Obama* tomēr neprasīja iesniegt nekādus konkrētus priekšlikumus, jo īpaši attiecībā uz masu novērošanas pasākumu aizliegšanu un administratīvu un tiesisku aizsardzības mehānismu ieviešanu personām, kas nav ASV pilsoņi;

Tiesiskais regulējums

Pamattiesības

S. tā kā ziņojumā par ES un ASV Datu aizsardzības jautājumu *ad hoc* darba grupas ES līdzpriekšsēdētāju konstatējumiem ir sniegts pārskats par tiesisko situāciju ASV, bet tajā nav noskaidroti fakti par ASV novērošanas programmām; tā kā nav pieejama nekāda informācija par tā dēvēto "rezerves ceļa" darba grupu, kurā dalībvalstis dialogā ar ASV iestādēm pārrunā ar valsts drošību saistītus jautājumus;

T. tā kā pamattiesības, jo īpaši vārda, preses, domas, pārliecības, ticības un biedrošanās brīvība, tiesības uz privāto dzīvi un datu aizsardzību, kā arī tiesības uz efektīvu tiesību aizsardzību, nevainīguma prezumpcija un tiesības uz taisnīgu tiesu un nediskrimināciju, kas paredzētas Eiropas Savienības Pamattiesību hartā un Eiropas Cilvēktiesību konvencijā, ir demokrātijas stūrakmeņi; tā kā cilvēku masveida novērošana ir pretrunā ar šiem pamatprincipiem;

U. tā kā visās dalībvalstīs ar likumu ir aizsargāta tādas informācijas izpaušana, ar ko konfidenciāli apmainās jurists un klients — princips, ko ir atzinusi Eiropas Savienības Tiesa ([1]);

V. tā kā 2013. gada 23. oktobra rezolūcijā par organizēto noziedzību, korupciju un nelikumīgi iegūtu līdzekļu legalizēšanu Parlaments aicināja Komisiju iesniegt tiesību akta priekšlikumu par efektīvas un visaptverošas Eiropas ziņotāju aizsardzības programmas izveidi, lai aizsargātu ES finansiālās intereses un turklāt pārbaudītu, vai šādā turpmākā tiesību aktā būtu jāietver arī citas jomas, kas ir Savienības kompetencē;

Savienības kompetences drošības jomā

W. tā kā saskaņā ar LESD 67. panta 3. punktu ES "cenšas nodrošināt augstu drošības līmeni"; tā kā no Līgumu noteikumiem (jo īpaši LES 4. panta 2. punkta un LESD 72. un 73. panta) izriet, ka ES ir noteiktas kompetences jautājumos par Savienības kolektīvo drošību; tā kā ES ir īstenojusi savu kompetenci iekšējās drošības jautājumos (LESD 4. panta j) apakšpunkts) un ir īstenojusi savu kompetenci, pieņemot lēmumus par vairākiem likumdošanas instrumentiem un noslēdzot starptautiskus nolīgumus (PDR, *TFTP*), kuru mērķis ir cīnīties pret smagiem noziegumiem un terorismu, un izveidojot iekšējās drošības stratēģiju un aģentūras, kas strādā šajā jomā;

X. tā kā Līgumā par Eiropas Savienības darbību ir noteikts "dalībvalstīm ir iespēja uz pašu atbildību izvēlēties tādas savstarpējas sadarbības un koordinācijas formas, kādas tās uzskata par piemērotām sadarbībai starp kompetentajām valsts pārvaldes iestādēm, kas atbild par valsts drošību" (LESD 73. pants);

Y. tā kā LESD 276. pantā ir noteikts, ka "Eiropas Savienības Tiesa, īstenojot tai uzticētās pilnvaras saistībā ar trešās daļas V sadaļas 4. un 5. iedaļas noteikumiem par brīvības, drošības un tiesiskuma telpu, nav kompetenta pārbaudīt kādas dalībvalsts policijas vai citu tiesību aizsardzības dienestu darbības likumību vai samērību, vai tādu dalībvalstu pienākumu izpildi, kas attiecas uz likumības un kārtības uzturēšanu un iekšējas drošības sargāšanu";

([1]) 1982. gada 18. maija spriedums lietā C-155/79, *AM & S Europe Limited*/Eiropas Kopienu Komisija.

Z. tā kā jēdzieni "valsts drošība", "iekšējā drošība", "ES iekšējā drošība" un "starptautiskā drošība" daļēji pārklājas; tā kā Vīnes konvencija par starptautisko līgumu tiesībām, lojālas sadarbības princips starp ES dalībvalstīm un cilvēktiesību princips jebkādu atbrīvojumu interpretēšanā konkrēti norāda uz "valsts drošības" jēdziena šauru interpretāciju un aicina dalībvalstis neiejaukties ES kompetencēs;

AA. tā kā Eiropas Līgumos ir noteikts, ka Eiropas Komisijai jābūt par Līgumu uzraudzītāju, un tāpēc Eiropas Komisija ir juridiski atbildīga par ikviena iespējama ES tiesību aktu pārkāpuma izmeklēšanu;

AB. tā kā saskaņā ar LES 6. pantu, kurā ietverta atsauce uz ES Pamattiesību hartu un ECTK, dalībvalstu aģentūrām un pat privātpersonām, kas darbojas valsts drošības jomā, ir jāievēro tajā paredzētās tiesības neatkarīgi no tā, vai tās ir attiecīgās valsts vai citu valstu pilsoņu tiesības;

Eksteritorialitāte

AC. tā kā trešās valsts normatīvo aktu un citu likumdošanas vai administratīvo instrumentu eksteritoriāla piemērošana situācijās, kas ietilpst ES vai tās dalībvalstu jurisdikcijā, var ietekmēt iedibināto tiesisko kārtību un tiesiskumu vai pat pārkāpt starptautiskās vai ES tiesības, tostarp fizisku un juridisku personu tiesības, ņemot vērā šādas piemērošanas apmēru un norādīto vai faktisko mērķi; tā kā šādos ārkārtas apstākļos ir jārīkojas Savienības līmenī, lai nodrošinātu, ka ES tiek ievērotas LES 2. pantā, Pamattiesību hartā, ECTK un dalībvalstu konstitūcijās ietvertās vērtības, t. i., pamattiesības, demokrātija un tiesiskums, kā arī fizisku un juridisku personu tiesības, kas noteiktas sekundārajos tiesību aktos, ar kuriem šie pamatprincipi tiek piemēroti, piemēram, likvidējot, neitralizējot, aizkavējot vai citādi novēršot attiecīgās ārvalsts tiesību aktu piemērošanas sekas;

Datu starptautiskā pārsūtīšana

AD. tā kā, ja ES iestādes, struktūras, biroji, aģentūras vai dalībvalstis personas datus tiesībaizsardzības nolūkā pārsūta ASV, nenodrošinot atbilstošas garantijas un aizsardzību, lai tiktu ievērotas ES iedzīvotāju pamattiesības, jo īpaši tiesības uz privātumu un personas datu aizsardzību, attiecīgā ES iestāde, struktūra, birojs, aģentūra vai dalībvalsts saskaņā ar LESD 340. pantu vai ES Tiesas iedibināto judikatūru ([1]) ir atbildīga par ES tiesību, tostarp ES Pamattiesību hartā paredzēto pamattiesību, pārkāpšanu;

AE. tā kā datu pārsūtīšana nav ģeogrāfiski ierobežota un jo īpaši pieaugošās globalizācijas un starptautiskās komunikācijas apstākļos ES likumdevējs saskaras ar jaunām problēmām saistībā ar personas datu un komunikācijas aizsardzību; tā kā tādēļ ir ārkārtīgi svarīgi veicināt kopīgu standartu tiesisko regulējumu;

AF. tā kā masveida personas datu ievākšana komerciālos nolūkos un cīņā pret terorismu un smagiem transnacionāliem noziegumiem apdraud ES iedzīvotāju personas datus un tiesības uz privātumu;

Datu pārsūtīšana uz ASV, balstoties uz ASV "drošības zonas" principiem

AG. tā kā ASV tiesiskais regulējums datu aizsardzības jomā nenodrošina pienācīgu ES iedzīvotāju aizsardzības līmeni;

AH. tā kā, lai ES datu kontrolieri varētu pārsūtīt personas datus kādai ASV organizācijai, Komisija savā Lēmumā 2000/520/EK ir paziņojusi par pienācīgu aizsardzību, kas noteikta ar privātuma "drošības zonas" principiem un attiecīgajiem visbiežāk uzdotajiem jautājumiem, kurus izdevusi ASV Tirdzniecības ministrija, attiecībā uz personas datiem, kas no Savienības tiek pārsūtīti ASV dibinātām organizācijām, kuras ir pievienojušās "drošības zonai";

([1]) Skat. jo īpaši 1991. gada 19. novembra spriedumu apvienotajās lietās C-6/90 un C-9/90, *Francovich* u. c./Itālija.

AI. tā kā Parlaments savā 2000. gada 5. jūlija rezolūcijā izteica šaubas un bažas par to, vai "drošības zona" nodrošina pienācīgu aizsardzību, un aicināja Komisiju savu lēmumu savlaicīgi pārskatīt, ņemot vērā pieredzi un izmaiņas tiesību aktos;

AJ. tā kā Parlaments savā 2013. gada 12. decembra 4. darba dokumentā par ASV novērošanas pasākumiem attiecībā uz ES datiem un to iespējamo ietekmi uz transatlantiskajiem nolīgumiem un sadarbību referenti izteica šaubas un bažas par "drošības zonas" atbilstību un aicināja Komisiju atcelt lēmumu par "drošības zonas" atbilstību un rast jaunus tiesiskus risinājumus;

AK. tā kā Komisijas Lēmumā 2000/520/EK ir noteikts, ka dalībvalstu kompetentās iestādes var īstenot savas pašreizējās pilnvaras, lai pārtrauktu datu plūsmu uz organizāciju, kura pati ir apliecinājusi, ka tā stingri ievēro "drošības zonas" principus, lai nodrošinātu aizsardzību attiecībā uz personas datu apstrādi, ja ir liela iespējamība, ka "drošības zonas" principi tiek pārkāpti vai pārsūtīšanas turpināšana datu subjektiem radītu būtiska kaitējuma draudus;

AL. tā kā Komisijas Lēmumā 2000/520/EK ir arī noteikts, ka, ja ir sniegti pierādījumi, ka jebkurš, kas ir atbildīgs par šo principu ievērošanu, savu uzdevumu pilda neefektīvi, Komisija informē ASV Tirdzniecības ministriju un vajadzības gadījumā iesniedz pasākumus, kuru mērķis ir atcelt vai apturēt šo lēmumu vai ierobežot tā darbības jomu;

AM. tā kā Komisija savos pirmajos divos ziņojumos par "drošības zonas" īstenošanu (publicēti 2002. un 2004. gadā) konstatēja vairākas nepilnības "drošības zonas" pareizā īstenošanā un sniedza vairākus ieteikumus ASV iestādēm, kā šīs nepilnības novērst;

AN. tā kā Komisija savā trešajā īstenošanas ziņojumā (2013. gada 27. novembris), deviņus gadus pēc otrā ziņojuma, kurā minētās nepilnības netika novērstas, konstatēja vēl citas plaša spektra nepilnības un trūkumus "drošības zonas" īstenošanā un secināja, ka pašreizējo īstenošanu nevar turpināt; tā kā Komisija ir uzsvērusi, ka ASV izlūkošanas aģentūru plašā piekļuve datiem, kas pārsūtīti tām ASV organizācijām, kuras pievienojušās "drošības zonai", rada nopietnas šaubas par ES datu subjektu datu aizsardzības nepārtrauktību; tā kā Komisija ASV iestādēm sniedza 13 ieteikumus un uzņēmās līdz 2014. gada vasarai kopā ar ASV iestādēm noteikt novēršanas pasākumus, kas jāveic pēc iespējas ātrāk, nodrošinot pamatu "drošības zonas" principu darbības pilnīgai pārskatīšanai;

AO. tā kā 2013. gada 28.–31. oktobrī Eiropas Parlamenta Pilsoņu brīvību, tieslietu un iekšlietu komitejas (LIBE komiteja) delegācija Vašingtonā tikās ar ASV Tirdzniecības ministriju un ASV Federālo tirdzniecības komisiju; tā kā Tirdzniecības ministrija atzina tādu organizāciju esamību, kuras pašas ir apliecinājušas, ka stingri ievēro "drošības zonas" principus, lai gan ir skaidri redzams to "neaktuālais statuss", kas nozīmē to, ka uzņēmums nepilda "drošības zonas" prasības, turpinot saņemt personas datus no ES; tā kā Federālā tirdzniecības komisija atzina, ka "drošības zonu" vajadzētu pārskatīt, lai to uzlabotu, jo īpaši attiecībā uz sūdzībām un alternatīvas strīdu izšķiršanas sistēmām;

AP. tā kā "drošības zonas" principu piemērošana var būt ierobežota "ciktāl tas ir nepieciešams, lai izpildītu valsts drošības, sabiedrības interešu vai tiesībaizsardzības prasības"; tā kā šāds pamattiesību izņēmums vienmēr ir jāinterpretē šauri un attiecībā tikai uz to, kas ir vajadzīgs un samērīgs demokrātiskā sabiedrībā, un tiesību aktos ir skaidri jāparedz nosacījumi un garantijas, lai šo ierobežojumu padarītu likumīgu; tā kā šāda izņēmuma piemērošanas joma būtu jāprecizē ASV un ES, konkrēti, Komisijai, lai izvairītos no jebkādas interpretācijas vai īstenošanas, kas būtībā anulē citu starpā pamattiesības uz privātumu un datu aizsardzību; tā kā līdz ar to šādu izņēmumu nedrīkst izmantot tādā veidā, ka tiek vājināta vai anulēta aizsardzība, ko nodrošina Pamattiesību harta, ECTK, ES tiesību akti datu aizsardzības jomā un "drošības zonas" principi; uzstāj, ka valsts drošības izņēmuma piemērošanas gadījumā ir jānorāda attiecīgie valsts tiesību akti, ar kuriem saskaņā tas tiek darīts;

AQ. tā kā ASV izlūkošanas aģentūru plašā piekļuve ir nopietni mazinājusi transatlantisko uzticību un negatīvi ietekmējusi uzticēšanos ASV organizācijām, kas darbojas ES; tā kā šo situāciju vēl vairāk saasina tiesiskās un administratīvās aizsardzības trūkums ES iedzīvotājiem saskaņā ar ASV tiesību aktiem, jo īpaši tādu novērošanas darbību gadījumā, kas tiek veiktas izlūkošanas nolūkā;

Datu pārsūtīšana trešām valstīm ar lēmumu par pienācīgu aizsardzību

AR. tā kā saskaņā ar atklāto informāciju un LIBE komitejas veiktās izmeklēšanas rezultātiem Jaunzēlandes, Kanādas un Austrālijas valsts drošības aģentūras ir plaši iesaistītas elektronisko komunikāciju masveida novērošanā un ir aktīvi sadarbojušās ar ASV, īstenojot tā dēvēto "piecu acu" programmu, un, iespējams, ir savstarpēji apmainījušās ar ES iedzīvotāju personas datiem, kas tām pārsūtīti no ES;

AS. tā kā Komisijas Lēmumā 2013/65/ES ([1]) un Lēmumā Nr. 2002/2/EK ([2]) ir atzīts pienācīgs aizsardzības līmenis, ko nodrošina Jaunzēlande un Kanādas likums par personas datu aizsardzību un elektroniskajiem dokumentiem; tā kā iepriekš minētie atklājumi nopietni ietekmē uzticēšanos šo valstu tiesību sistēmām attiecībā uz ES iedzīvotājiem nodrošinātās aizsardzības nepārtrauktību; tā kā Komisija šo aspektu nav izpētījusi;

Datu pārsūtīšana saskaņā ar līguma klauzulām un citiem instrumentiem

AT. tā kā Direktīvā 95/46/EK ir noteikts, ka datu starptautiskā pārsūtīšana uz trešo valsti var notikt arī tad, ja tiek izmantoti īpaši instrumenti, ar kuriem datu kontrolieris sniedz atbilstošas garantijas attiecībā uz personu privātuma un pamattiesību un brīvību aizsardzību un attiecībā uz atbilstošo tiesību izmantošanu;

AU. tā kā šādas garantijas jo īpaši var izrietēt no attiecīgajām līguma klauzulām;

AV. tā kā saskaņā ar Direktīvu 95/46/EK Komisijai ir tiesības nolemt, ka konkrētas līguma standartklauzulas sniedz pietiekamas garantijas, kas paredzētas šajā direktīvā, un tā kā, pamatojoties uz to, Komisija ir pieņēmusi trīs līguma standartklauzulu modeļus datu pārsūtīšanai kontrolieriem un apstrādātājiem (un apakšapstrādātājiem) trešās valstīs;

AW. tā kā Komisijas lēmumos, ar ko izveido līguma standartklauzulas, ir noteikts, ka dalībvalstu kompetentās iestādes var īstenot savas pašreizējās pilnvaras, lai pārtrauktu datu plūsmu, ja tiek konstatēts, ka tiesību akti, kuri datu saņēmējam vai apakšapstrādātājam ir jāievēro, uzliek tam pienākumu atkāpties no piemērojamiem tiesību aktiem datu aizsardzības jomā, kas pārsniedz ierobežojumus, kuri ir vajadzīgi demokrātiskā sabiedrībā, kā paredzēts Direktīvas 95/46/EK 13. pantā, ja ir iespējamība, ka šis pienākums var ļoti negatīvi ietekmēt garantijas, kas ir paredzētas piemērojamos tiesību aktos datu aizsardzības jomā un līguma standartklauzulās, vai ir liela iespējamība, ka nav ievērotas vai netiks ievērotas pielikumā minētās līguma standartklauzulas, un pārsūtīšanas turpināšana datu subjektiem radītu būtiska kaitējuma draudus;

AX. tā kā valstu datu aizsardzības iestādes ir izstrādājušas saistošos uzņēmumu noteikumus, lai veicinātu datu starptautisko pārsūtīšanu daudznacionālā uzņēmumā ar atbilstošām garantijām attiecībā uz personu privātuma un pamattiesību un brīvību aizsardzību un attiecībā uz atbilstošo tiesību izmantošanu; tā kā pirms to izmantošanas saistošie uzņēmumu noteikumi ir jāapstiprina dalībvalstu kompetentajām iestādēm pēc tam, kad tās ir novērtējušas atbilstību Savienības tiesību aktiem datu aizsardzības jomā; tā kā LIBE komitejas ziņojumā par Vispārīgo datu aizsardzības regulu ir noraidīti saistošie uzņēmumu noteikumi attiecībā uz datu apstrādātājiem, jo datu kontrolieri un datu subjekti tiktu atstāti bez jebkādas kontroles jurisdikcijā, kurā tiek apstrādāti to dati;

([1]) OV L 28, 30.1.2013., 12. lpp.
([2]) OV L 2, 4.1.2002., 13. lpp.

Trešdiena, 2014. gada 12. marta

AY. tā kā Eiropas Parlamentam, ņemot vērā tā kompetenci, kas noteikta LESD 218. pantā, ir pienākums pastāvīgi uzraudzīt tādu starptautisko nolīgumu vērtību, kuriem tas ir devis savu piekrišanu;

Datu pārsūtīšana, kas balstās uz TFTP *un PDR nolīgumiem*

AZ. tā kā Parlaments savā 2013. gada 23. oktobra rezolūcijā pauda nopietnas bažas par atklājumiem saistībā ar NDA darbībām attiecībā uz tiešu piekļuvi finanšu maksājumu ziņojumiem un ar tiem saistītiem datiem, kas ir uzskatāms par skaidru *TFTP* nolīguma un jo īpaši tā 1. panta pārkāpumu;

BA. tā kā teroristu finansēšanas izsekošana ir ļoti svarīgs rīks cīņā pret terorisma un smagu noziegumu finansēšanu, kas ļauj izmeklētājiem terorisma apkarošanas jomā atklāt saiknes starp izmeklēšanas objektiem un citiem potenciālajiem aizdomās turamajiem, kuri ir saistīti ar plašākiem teroristu tīkliem, kurus tur aizdomās par teroristu finansēšanu;

BB. tā kā Parlaments aicināja Komisiju Nolīguma darbību apturēt un pieprasīja, lai visa attiecīgā informācija un dokumenti tiktu nekavējoties iesniegti tam apspriešanai; tā kā Komisija nav veikusi neko no iepriekš minētā;

BC. tā kā pēc plašsaziņas līdzekļos publicētajiem apgalvojumiem Komisija nolēma uzsākt apspriešanos ar ASV saskaņā ar *TFTP* nolīguma 19. pantu; tā kā 2013. gada 27. novembrī komisāre *C. Malmström* informēja LIBE komiteju, ka pēc tikšanās ar ASV iestādēm un ņemot vērā atbildes, ko ASV iestādes sniedza vēstulēs un tikšanās laikā, Komisija nolēma apspriešanos neturpināt, jo nebija nekādu pierādījumu, ka ASV valdība būtu rīkojusies pretēji Nolīguma noteikumiem, un ASV sniedza rakstisku apgalvojumu, ka nav notikusi tieša datu vākšana, kas būtu pretrunā *TFTP* nolīguma noteikumiem; tā kā nav skaidrs, vai ASV iestādes ir apgājušas Nolīgumu, piekļūstot šādiem datiem, izmantojot citus paņēmienus, kā 2013. gada 18. septembra vēstulē ir norādījušas ASV iestādes ([1]);

BD. tā kā savas vizītes laikā 2013. gada 28.–31. oktobrī LIBE delegācija Vašingtonā tikās ar ASV Finanšu ministriju; tā kā ASV Finanšu ministrija paziņoja, ka kopš *TFTP* nolīguma stāšanās spēkā tai nav bijusi piekļuve *SWIFT* datiem ES, izņemot to, kas paredzēta *TFTP*; tā kā ASV Finanšu ministrija attiecās komentēt, vai *SWIFT* datiem ārpus *TFTP* varētu būt piekļuvusi kāda cita ASV valdības iestāde vai ministrija un vai ASV administrācija bija informēta par NDA veiktajām masveida novērošanas darbībām; tā kā 2013. gada 18. decembrī *Glenn Greenwald* paziņoja LIBE izmeklēšanas komitejai, ka NDA un *GCHQ* darbība bija vērsta uz *SWIFT* tīkliem;

BE. tā kā 2013. gada 13. novembrī Beļģijas un Nīderlandes datu aizsardzības iestādes nolēma veikt kopīgu izmeklēšanu par *SWIFT* maksājumu tīklu drošību, lai noskaidrotu, vai trešās puses varēja iegūt nesankcionētu vai nelikumīgu piekļuvi Eiropas iedzīvotāju bankas datiem ([2]);

BF. tā kā saskaņā ar kopīgo pārskatu par ES un ASV PDR nolīgumu ASV Iekšzemes drošības departaments 23 reizes atklāja PDR datus Nacionālajai drošības aģentūrai, katru gadījumu izskatot atsevišķi, lai palīdzētu terorisma apkarošanas lietās, ievērojot Nolīguma īpašos noteikumus;

BG. tā kā kopīgajā pārskatā nav minēts tas, ka saskaņā ar ASV tiesību aktiem personām, kas nav ASV pilsoņi, nav nekādu tiesisku vai administratīvu iespēju aizsargāt savas tiesības, kad to personas dati tiek apstrādāti izlūkošanas vajadzībām, un ka konstitucionālā aizsardzība ir pieejama tikai ASV pilsoņiem; tā kā, ņemot vērā šo tiesisko un administratīvo tiesību trūkumu, spēkā esošajā PDR nolīgumā paredzētā ES iedzīvotāju aizsardzība netiek nodrošināta;

([1]) Vēstulē ir teikts, ka "ASV valdība meklē un iegūst finanšu informāciju […], (ko) ievāc pa normatīviem, likumdošanas, tiesībaizsardzības, diplomātiskiem un izlūkošanas kanāliem, kā arī apmainoties ar ārvalstu partneriem […], ASV valdība izmanto *TFTP*, lai iegūtu *SWIFT* datus, ko mēs neiegūstam no citiem avotiem";

([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

Datu pārsūtīšana, kas balstās uz ES un ASV nolīgumu par savstarpēju tiesisko palīdzību krimināllietās

BH. tā kā ES un ASV 2003. gada 6. jūnija nolīgums par savstarpēju tiesisko palīdzību krimināllietās ([1]) stājās spēkā 2010. gada 1. februārī un tā mērķis ir veicināt sadarbību starp ES un ASV, lai efektīvāk apkarotu noziedzību, pienācīgi ievērojot personu tiesības un tiesiskumu;

Pamatnolīgums par datu aizsardzību policijas un tiesu iestāžu sadarbības jomā ("jumta nolīgums")

BI. tā kā šā vispārējā nolīguma mērķis ir izveidot tiesisko regulējumu jebkurai personas datu pārsūtīšanai starp ES un ASV tikai tādēļ, lai novērstu, izmeklētu un atklātu noziedzīgus nodarījumus, tostarp terorismu, un sauktu pie atbildības par tiem, īstenojot policijas un tiesu iestāžu sadarbību krimināllietās; tā kā 2010. gada 2. decembrī Padome deva atļauju uzsākt sarunas; tā kā šis nolīgums ir ārkārtīgi svarīgs un tas būtu pamats, lai veicinātu datu pārsūtīšanu saistībā ar policijas un tiesu iestāžu sadarbību, kā arī krimināllietās;

BJ. tā kā ar šo nolīgumu būtu jānodrošina skaidri, precīzi un juridiski saistoši datu apstrādes principi un jo īpaši būtu jāatzīst ES iedzīvotāju tiesības tiesiskā ceļā piekļūt saviem personas datiem ASV, tos labot un dzēst, kā arī ES iedzīvotāju tiesības izmantot efektīvu administratīvās un tiesiskās aizsardzības mehānismu ASV un tiesības veikt datu apstrādes darbību neatkarīgu uzraudzību;

BK. tā kā Komisija savā 2013. gada 27. novembra paziņojumā norādīja, ka, īstenojot "jumta nolīgumu", iedzīvotājiem abās Atlantijas okeāna pusēs būtu jānodrošina augsts aizsardzības līmenis un būtu jānostiprina eiropiešu uzticēšanās datu apmaiņai starp ES un ASV, nodrošinot pamatu, uz kura tālāk veidot ES un ASV sadarbību drošības jomā un to partnerattiecības;

BL. tā kā sarunās par nolīgumu nav gūti panākumi, jo ASV valdība ir ieņēmusi nelokāmu nostāju, atsakoties atzīt ES pilsoņu faktiskās tiesības uz administratīvo un tiesisko aizsardzību, un ir iecerējusi noteikt plašas atkāpes no nolīgumā paredzētajiem datu aizsardzības principiem, piemēram, mērķa ierobežošanu, datu saglabāšanu vai tālāku pārsūtīšanu valsts teritorijā vai uz ārzemēm;

Datu aizsardzības reforma

BM. tā kā ES tiesiskais regulējums datu aizsardzības jomā patlaban tiek pārskatīts, lai izveidotu visaptverošu, konsekventu, modernu un stabilu sistēmu visām datu apstrādes darbībām Savienībā; tā kā 2012. gada janvārī Komisija iesniedza priekšlikumus šādiem tiesību aktiem: Vispārīgā datu aizsardzības regula ([2]), ar ko aizstās Direktīvu 95/46/EK un ieviesīs vienotu regulējumu visā ES, un direktīva ([3]), ar ko noteiks saskaņotu regulējumu visām datu apstrādes darbībām, ko tiesībaizsardzības nolūkā veic tiesībaizsardzības iestādes, un samazinās pašreizējās atšķirības valstu tiesību aktos;

BN. tā kā 2013. gada 21. oktobrī LIBE komiteja pieņēma normatīvus ziņojumus par abiem priekšlikumiem un lēmumu par sarunu sākšanu ar Padomi, lai tiesību aktus pieņemtu šā sasaukuma laikā;

BO. tā kā, lai gan 2013. gada 24.–25. oktobrī Eiropadome aicināja savlaicīgi pieņemt stingru vispārīgo ES datu aizsardzības regulējumu, lai veicinātu iedzīvotāju un uzņēmumu uzticēšanos digitālajai ekonomikai, pēc divu gadu ilgām pārdomām Padome vēl aizvien nav spējusi atrast vispārēju pieeju Vispārīgajai datu aizsardzības regulai un direktīvai ([4]);

([1]) OV L 181, 19.7.2003., 25. lpp.
([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

IT drošība un mākoņdatošana

BP. tā kā Parlamenta 2013. gada 10. decembra rezolūcijā ir uzsvērts mākoņdatošanas ekonomiskais potenciāls izaugsmes un nodarbinātības nodrošināšanai; tā kā ir sagaidāms, ka vispārējā mākoņdatošanas ekonomiskā vērtība gadā būs USD 207 miljardi līdz 2016. gadam jeb divreiz lielāka vērtība nekā 2012. gadā;

BQ. tā kā datu aizsardzības līmenis mākoņdatošanas vidē nedrīkst būt zemāks par to, kāds noteikts jebkurā citā datu apstrādes kontekstā; tā kā Savienības tiesību akti datu aizsardzības jomā ir tehnoloģiski neitrāli, tāpēc tie jau pilnībā attiecas uz mākoņdatošanas pakalpojumiem, kas tiek sniegti ES;

BR. tā kā saskaņā ar mākoņdatošanas pakalpojumu līgumiem, kas noslēgti ar ASV lielākajiem mākoņdatošanas pakalpojumu sniedzējiem, masveida novērošanas darbības izlūkošanas aģentūrām nodrošina piekļuvi ES iedzīvotāju glabātajiem vai citādi apstrādātajiem personas datiem; tā kā ASV izlūkošanas iestādes ir piekļuvušas personas datiem, kas tiek glabāti vai citādi apstrādāti serveros, kuri atrodas ES, pieslēdzoties *Yahoo* un *Google* iekšējiem tīkliem; tā kā šādas darbības ir starptautisko saistību un Eiropas pamattiesību standartu, tostarp pamattiesību uz privātumu un datu aizsardzību, kā arī tiesību uz privāto un ģimenes dzīvi, sakaru konfidencialitāti, nevainīguma prezumpciju, vārda brīvību, informācijas brīvību un darījumu veikšanas brīvību, pārkāpums; tā kā nav izslēgts, ka izlūkošanas iestādes ir piekļuvušas informācijai, ko, izmantojot mākoņdatošanas pakalpojumus, glabā dalībvalstu valsts sektora iestādes vai uzņēmumi;

BS. tā kā ASV izlūkdienestu politika ir sistemātiski ignorēt kriptogrāfiskos protokolus un produktus, lai varētu pārtvert pat šifrētu komunikāciju; tā kā ASV Nacionālās drošības aģentūra ir ievākusi lielu skaitu datu par tā dēvētajiem "nulles dienas uzbrukumiem" — IT drošības ievainojamību, par ko vēl nezina ne sabiedrība, ne produkta pārdevējs; tā kā šādas darbības masveidā grauj starptautiskos pūliņus uzlabot IT drošību;

BT. tā kā tas, ka izlūkošanas aģentūras ir piekļuvušas tiešsaistes pakalpojumu lietotāju personas datiem, ir būtiski mazinājis iedzīvotāju uzticību šādiem dienestiem, un tāpēc tas ir negatīvi ietekmējis uzņēmumus, kuri veic ieguldījumus tādu jaunu pakalpojumu attīstībā, kuros izmanto "lielos datus" un jaunas lietojumprogrammas, piemēram, "lietu internetu" (*Internet of Things*);

BU. tā kā IT pārdevēji bieži piegādā produktus, kuru IT drošība nav pienācīgi pārbaudīta vai kuros pārdevējs dažkārt pat mērķtiecīgi iekļauj aizsardzības sistēmu apiešanas ceļus; tā kā noteikumu trūkums par programmatūras pārdevēju atbildību ir izraisījis šādu situāciju, ko savukārt izmanto izlūkošanas aģentūras, kā arī tā rada citu struktūru uzbrukumu risku;

BV. tā kā ir svarīgi, lai uzņēmumi, kuri sniedz šādus jaunus pakalpojumus un lietojumprogrammatūras, ievērotu datu aizsardzības noteikumus un to datu subjektu privātumu, kuru dati ir ievākti, apstrādāti un analizēti, lai nodrošinātu augstu iedzīvotāju uzticības līmeni;

Izlūkošanas dienestu demokrātiskā uzraudzība

BW. tā kā demokrātiskā sabiedrībā izlūkdienestiem ir īpašas pilnvaras un spējas aizsargāt pamattiesības, demokrātiju un tiesiskumu, pilsoņu tiesības un valsti pret nopietniem iekšējiem un ārējiem draudiem un uz tiem attiecas demokrātiskās pārskatatbildības un tiesiskās uzraudzības principi; tā kā tikai šim nolūkam tiem ir piešķirtas īpašas pilnvaras un spējas; tā kā šīs pilnvaras būtu jāizmanto, ievērojot tiesiskos ierobežojumus, ko paredz pamattiesības, demokrātija un tiesiskums, un to izmantošana būtu rūpīgi jāpārbauda, pretējā gadījumā tās zaudē leģitimitāti un riskē apdraudēt demokrātiju;

BX. tā kā tas, ka izlūkdienestiem ir pieļaujams noteikts slepenības līmenis (lai netiktu apdraudētas notiekošās operācijas, atklāti modi operandi vai pakļauta riskam aģentu dzīvība), nedrīkst būt iemesls, lai ignorētu vai izslēgtu noteikumus par to veikto darbību demokrātisku un tiesisku uzraudzību un pārbaudi, kā arī par pārredzamību, jo īpaši attiecībā uz pamattiesību un tiesiskuma ievērošanu, kas ir pamatprincipi demokrātiskā sabiedrībā;

BY. tā kā lielākā daļa valstu pašreizējo uzraudzības mehānismu un struktūru tika izveidoti vai atjaunoti pagājušā gadsimta 90. gados un pēdējo desmit gadu laikā tie ne vienmēr ir tikuši pielāgoti straujajai politikas un tehnoloģiju attīstībai, kā rezultātā ir tikusi veicināta starptautiskā sadarbība izlūkošanas jomā, tostarp arī lielā apjomā apmainoties ar personas datiem un bieži vien mazinot atšķirības starp izlūkošanas un tiesībaizsardzības darbībām;

BZ. tā kā izlūkošanas darbību demokrātiskā uzraudzība joprojām tiek veikta vienīgi valstu līmenī, neraugoties uz pieaugošo informācijas apmaiņu starp ES dalībvalstīm un starp dalībvalstīm un trešām valstīm; tā kā palielinās atšķirība starp starptautiskās sadarbības līmeni, no vienas puses, un valstu līmenī ierobežotajām uzraudzības iespējām, no otras puses, kā rezultātā demokrātiskā kontrole ir nepietiekama un neefektīva;

CA. tā kā valstu uzraudzības struktūrām bieži nav pilnīgas pieejas izlūkdatiem, kuri ir saņemti no ārvalstu izlūkošanas aģentūras, tas var izraisīt situācijas, kurās starptautiska informācijas apmaiņa notiek bez pienācīgas pārbaudes; tā kā šo problēmu vēl vairāk pastiprina tā dēvētais "trešās puses noteikums" jeb "iniciatora kontroles" princips, kas ir paredzēts, lai iniciators varētu kontrolēt tā sensitīvās informācijas tālāku izplatīšanu, taču bieži to interpretē arī kā piemērojamu saņēmēja pakalpojumu uzraudzībai;

CB. tā kā privātās un publiskās pārredzamības reformas iniciatīvas ir svarīgas, lai nodrošinātu sabiedrības uzticību izlūkošanas aģentūru darbībām; tā kā tiesību sistēmas nedrīkstētu atturēt uzņēmumus no tā, lai atklātu sabiedrībai informāciju par to, kā tie apstrādā visu veidu valdības pieprasījumus un tiesu rīkojumus attiecībā uz piekļuvi lietotāju datiem, tostarp iespēju atklāt apkopotu informāciju par vairākiem apstiprinātajiem un noraidītajiem pieprasījumiem un rīkojumiem,

Galvenie konstatējumi

1. uzskata, ka ziņotāju un žurnālistu nesenie atklājumi presē, kā arī šīs izmeklēšanas laikā sniegtās ekspertu liecības, iestāžu atzīšanās un šo pieņēmumu nepietiekama atspēkošana ir neapstrīdams pierādījums tam, ka pastāv vērienīgas, sarežģītas un tehnoloģiskā ziņā ļoti progresīvas sistēmas, kuras izstrādājuši ASV un dažu dalībvalstu izlūkdienesti, lai vēl nepieredzētā apmērā, nešķirojot un nepamatojoties uz aizdomām vāktu, glabātu un analizētu komunikācijas datus, tostarp saturu, atrašanās vietas datus un metadatus par visiem pasaules iedzīvotājiem;

2. īpaši uzsver ASV NDA novērošanas programmas, kas paredz ES iedzīvotāju masveida novērošanu, izmantojot tiešu piekļuvi lielāko ASV interneta uzņēmumu centrālajiem serveriem (programma *PRISM*), analizējot saturu un metadatus (programma *Xkeyscore*), apejot tiešsaistes šifrēšanu (*BULLRUN*) un piekļūstot datoru un telefonu tīkliem un atrašanās vietas datiem, kā arī Apvienotās Karalistes izlūkošanas aģentūras *GCHQ* sistēmām, piemēram, augšupplūsmas novērošanas darbībai (programma *Tempora*) un atšifrēšanas programmai (*Edgehill*), kā arī veicot mērķtiecīgus "cilvēks centrā" uzbrukumus informācijas sistēmām (programmas *Quantumtheory* un *Foxacid*), vācot un saglabājot 200 miljonu SMS ziņu dienā (programma *Dishfire*);

3. norāda uz apgalvojumiem, ka Apvienotās Karalistes izlūkošanas aģentūra *GCHQ* ir nelikumīgi piekļuvusi vai pieslēgusies *Belgacom* sistēmām; norāda uz *Belgacom* paziņojumiem, ka tas nevar ne apstiprināt, ne noliegt, ka uzbrukums bija vērsts uz ES iestādēm vai tika ietekmēta to darbība, kā arī atzīmē, ka izmantotā ļaunprogrammatūra bija ārkārtīgi sarežģīta un, lai to izstrādātu un izmantotu, bija vajadzīgi lieli finanšu un darbaspēka resursi, kas privātām struktūrām vai datorpirātiem nav pieejami;

4. uzsver, ka ir būtiski iedragāta uzticība — uzticība starp iedzīvotājiem un valdībām, uzticība demokrātisku iestāžu darbībai abās Atlantijas okeāna pusēs, uzticība attiecībā uz tiesiskuma ievērošanu un uzticība attiecībā uz IT pakalpojumu un komunikācijas drošību; uzskata, ka, lai atjaunotu uzticību visos šajos aspektos, ir steidzami vajadzīgs visaptverošs reaģēšanas plāns, kas sastāvētu no vairākiem pasākumiem, uz kuriem attiektos sabiedrības uzraudzība;

5. atzīmē, ka vairākas valdības apgalvo, ka šīs masveida novērošanas programmas ir vajadzīgas terorisma apkarošanai; stingri nosoda terorismu, tomēr pauž stingru pārliecību, ka cīņa pret terorismu pati par sevi nekad nevar būt attaisnojums nemērķtiecīgām, slepenām vai pat nelikumīgām masveida novērošanas programmām; uzskata, kā šādas programmas nav savienojamas ar nepieciešamības un samērīguma principiem demokrātiskā sabiedrībā;

6. atgādina ES stingro pārliecību par to, ka ir jāatrod pareizs līdzsvars starp drošības pasākumiem un pilsonisko brīvību un pamattiesību aizsardzību, vienlaikus pilnībā nodrošinot privātuma un datu aizsardzību;

7. uzskata, ka datu vākšana šādā apmērā rada ievērojamas šaubas par to, vai šo pasākumu pamatā ir tikai cīņa pret terorismu, jo tiek vākti visi iespējamie dati par visiem iedzīvotājiem; tāpēc norāda, ka, iespējams, pastāv arī citi mērķi, tostarp politiskā vai ekonomiskā spiegošana, kas pilnībā jāizskaužˇ;

8. apšauba dažu dalībvalstu masveida ekonomiskās spiegošanas darbību atbilstību ES tiesību aktiem iekšējā tirgus un konkurences jomā, kā paredzēts Līguma par Eiropas Savienības darbību I un VII sadaļā; atkārtoti apliecina lojālas sadarbības principu, kas paredzēts Līguma par Eiropas Savienību 4. panta 3. punktā, kā arī principu, ka dalībvalstis "atturas no jebkādiem pasākumiem, kuri varētu apdraudēt Savienības mērķu sasniegšanu";

9. norāda, ka starptautiskie līgumi un ES un ASV tiesību akti, kā arī valstu uzraudzības mehānismi nav nodrošinājuši nepieciešamās pārbaudes un līdzsvaru, vai demokrātisko pārskatatbildību;

10. nosoda plašo, sistēmisko un visaptverošo nevainīgu cilvēku personas datu vākšanu, kas bieži vien ietver ļoti personisku informāciju; uzsver, ka izlūkdienestu izmantotās nediferencētās masveida novērošanas sistēmas ir nopietna iejaukšanās iedzīvotāju pamattiesībās; uzsver, ka privātums nav luksusa tiesības, bet gan brīvas un demokrātiskas sabiedrības stūrakmens; turklāt norāda, ka masveida novērošana var būtiski ietekmēt preses, domas un vārda brīvību, un pulcēšanās un biedrošanās brīvību, kā arī pastāv liela iespēja, ka informācija, kas savākta par politiskajiem pretiniekiem, var tikt izmantota ļaunprātīgi; uzsver, ka šie masveida novērošanas pasākumi ietver arī izlūkdienestu nelikumīgas darbības un radīt šaubas par valstu tiesību aktu eksteritorialitāti;

11. uzskata, ka profesionālās konfidencialitātes saglabāšanas nolūkā ir svarīgi nodrošināt juristiem, žurnālistiem, ārstiem un citu reglamentētu profesiju pārstāvjiem tiesisku aizsardzību pret masveida novērošanas pasākumiem; jo īpaši uzsver, ka jebkāda neskaidrība par saziņas konfidencialitāti starp juristiem un viņu klientiem varētu negatīvi ietekmēt ES pilsoņu tiesības saņemt juridiskās konsultācijas un tiesības uz taisnīgu tiesu;

12. uzskata, ka novērošanas programmas ir vēl viens solis ceļā uz pilnīgi preventīvas valsts izveidi, mainot demokrātiskā sabiedrībā iedibināto krimināltiesību paradigmu, saskaņā ar kuru, lai jebkādā veidā iejauktos aizdomās turamo personu pamattiesībās, ir jāsaņem tiesneša vai prokurora atļauja, ko izsniedz, ņemot vērā pamatotas aizdomas, un tas jāreglamentē ar likumu, taču tā vietā tiek veicinātas dažādas tiesībaizsardzības un izlūkošanas darbības ar neskaidrām un pavājinātām tiesiskām garantijām, kas bieži vien ir pretrunā ar demokrātisku pārbaužu un samērīguma sistēmu un pamattiesībām, jo īpaši nevainīguma prezumpcijai; šajā saistībā atgādina par Vācijas Konstitucionālās tiesas lēmumu ([1]) aizliegt izmantot preventīvus izsekošanas tīklus (*präventive Rasterfahndung*), ja vien nav pierādījumu par konkrētiem draudiem citām prioritārām un juridiski aizsargātām tiesībām; saskaņā ar šo lēmumu ar vispārēju draudu situāciju vai starptautisku saspīlējumu vien nepietiek, lai attaisnotu šādus pasākumus;

13. pauž pārliecību, ka slepeni tiesību akti un tiesas pārkāpj tiesiskumu; norāda, ka neviens ārpussavienības valsts tiesas vai tribunāla spriedums vai administratīvas iestādes lēmums, ar ko tieši vai netieši atļauj veikt personas datu pārsūtīšanu, nevar nekādā veidā tikt atzīts vai izpildīts, ja vien nav spēkā savstarpējās tiesiskās palīdzības nolīgums vai starptautisks līgums, kas ir spēkā starp trešo valsti, kura pieprasa šo pārsūtīšanu, un Savienību vai dalībvalsti, vai kompetentās uzraudzības iestādes iepriekšējo atļauju; atgādina, ka nedrīkst atzīt vai izpildīt nevienu slepenas tiesas vai tribunāla spriedumu vai lēmumu, ko ir pieņēmusi ārpus ES esoša valsts, ar ko tieši vai netieši slepeni atļauj veikt novērošanas darbības;

([1]) Nr. 1 *BvR* 518/02, 2006. gada 4. aprīlis.

14. norāda, ka iepriekš minētās bažas pastiprina straujā tehnoloģiju un sabiedrības attīstība, jo internetu un mobilās ierīces ikdienas dzīvē mūsdienās izmanto visur (visuresoša datorika) un lielākās daļas interneta uzņēmumu uzņēmējdarbības modeļi balstās uz personas datu apstrādi; uzskata, ka šī problēma ir vēl nebijušā apmērā; norāda, ka var izveidoties situācija, kad datu masveida vākšanas un apstrādes infrastruktūra tiek izmantota ļaunprātīgi, ja mainās politiskais režīms;

15. norāda, ka ne ES publiskajām iestādēm, ne arī iedzīvotājiem nav nekādu garantiju, ka to IT drošība vai privātums varētu tikt pasargāts no labi aprīkotiem uzbrucējiem ("nepilnīga IT drošība"); norāda, ka, lai sasniegtu maksimālu IT drošību, eiropiešiem ir jāgrib atvēlēt pietiekamus resursus — gan finanšu, gan cilvēkresursus —, lai saglabātu Eiropas neatkarību un pašpaļāvību IT jomā;

16. stingri noraida uzskatu, ka visas ar masveida novērošanas programmām saistītās problēmas ir tikai valsts drošības jautājums un līdz ar to tikai dalībvalstu kompetencē; atkārtoti norāda, ka dalībvalstīm, veicot pasākumus valsts drošības garantēšanai, pilnībā jāievēro ES tiesību akti un ECTK; atgādina Tiesas neseno nolēmumu, saskaņā ar kuru "lai arī dalībvalstīm ir kompetence noteikt pienācīgus pasākumus, lai nodrošinātu to iekšējo un ārējo drošību, tikai tas apstāklis vien, ka lēmums attiecas uz valsts drošību, nevar izraisīt Savienības tiesību nepiemērojamību" ([1]); turklāt atgādina, ka ir apdraudēta visu ES iedzīvotāju privātuma aizsardzība, kā arī visu ES komunikāciju tīklu drošība un uzticamība; tāpēc uzskata, ka diskusijas un rīcība ES līmenī ir ne tikai leģitimitātes, bet arī ES autonomijas jautājums;

17. izsaka atzinību iestādēm un ekspertiem, kuri ir snieguši ieguldījumu šajā izmeklēšanā; pauž nožēlu, ka vairākas dalībvalstu iestādes ir atteikušās sadarboties izmeklēšanā, ko Eiropas Parlaments veic iedzīvotāju interesēs; atzinīgi vērtē vairāku Kongresa locekļu un valstu parlamentu deputātu atklātību;

18. apzinās, ka tik ierobežotā termiņā bija iespējams veikt tikai sākotnēju izmeklēšanu par visiem kopš 2013. gada jūlija aktuālajiem jautājumiem; atzīst gan attiecīgo atklājumu mērogu, gan arī to nepārtrauktību; tāpēc pieņem perspektīvās plānošanas pieeju, kas sastāv no vairākiem konkrētiem priekšlikumiem un izpildes pārbaudes mehānisma, ko izmantos Parlamenta nākamajā sasaukumā, nodrošinot konstatējumu saglabāšanos ES politiskās darba kārtības augšgalā;

19. paredz pieprasīt stingru politisko apņemšanos no jaunās Eiropas Komisijas, kas tiks izveidota pēc 2014. gada maija Eiropas Parlamenta vēlēšanām, lai īstenotu šīs izmeklēšanas priekšlikumus un ieteikumus;

Ieteikumi

20. aicina ASV iestādes un ES dalībvalstis aizliegt vispārējās masveida novērošanas darbības, ja tās to vēl nav izdarījušas;

21. aicina ES dalībvalstis, jo īpaši tās, kas piedalās tā dēvētajās programmās "9 acis" un "14 acis" ([2]), vispārīgi izvērtēt un vajadzības gadījumā pārskatīt valsts tiesību aktus un praksi, kas regulē izlūkdienestu darbību, lai nodrošinātu, ka uz tiem attiecas parlamentārā, tiesiskā un sabiedrības veikta uzraudzība un ka tie ievēro likumības, nepieciešamības, samērīguma, pienācīga procesa, lietotāja informēšanas un pārredzamības principus, tostarp ņemt vērā ANO apkopoto paraugpraksi un Venēcijas komisijas ieteikumus, kā arī to, ka tie atbilst Eiropas Cilvēktiesību konvencijas standartiem un ievēro dalībvalstu saistības attiecībā uz pamattiesībām, jo īpaši datu aizsardzību, privātumu un nevainības prezumpciju;

([1]) 2013. gada 4. jūnija spriedums lietā C-300/11, ZZ/Iekšlietu ministrijas valsts sekretārs.

([2]) Programmā "9 acis" piedalās ASV, Apvienotā Karaliste, Austrālija, Jaunzēlande, Dānija, Francija, Norvēģija un Nīderlande; programmā "14 acis" piedalās jau minētās valstis, kā arī Vācija, Beļģija, Itālija, Spānija un Zviedrija.

22. aicina visas ES dalībvalstis un, ņemot vērā 2013. gada 4. jūlija rezolūciju un ar izmeklēšanu saistītās uzklausīšanas, jo īpaši Apvienoto Karalisti, Franciju, Vāciju, Zviedriju, Nīderlandi un Poliju nodrošināt, lai to pašreizējais vai turpmākais tiesiskais regulējums un pārraudzības mehānismi, ar kuriem tiek reglamentēta izlūkošanas aģentūru darbība, būtu saskaņā ar standartiem, kas noteikti Eiropas Cilvēktiesību konvencijā un Eiropas Savienības tiesību aktos par datu aizsardzību; aicina minētās dalībvalstis ieviest skaidrību jautājumā par iespējamiem pārrobežu telekomunikāciju masveida novērošanas pasākumiem (tostarp nemērķtiecīgu novērošanu attiecībā uz saziņu pa kabeļiem, iespējamu vienošanos starp izlūkdienestiem un telekomunikāciju uzņēmumiem par personas datu pieejamību un apmaiņu ar tiem un piekļuvi transatlantiskajiem kabeļiem, kā arī par ASV izlūku un izlūkošanas aprīkojuma atrašanos ES teritorijā), kuri tiek veikti bez uzraudzības, un par to, vai šie pasākumi atbilst ES tiesību aktiem; aicina minēto valstu nacionālos parlamentus pastiprināt sadarbību ar izlūkdienestu uzraudzības iestādēm Eiropas līmenī;

23. aicina Apvienoto Karalisti, jo īpaši ņemot vērā daudzos plašsaziņas līdzekļu ziņojumus par izlūkdienesta *GCHQ* veikto masveida novērošanu, pārskatīt tās pašreizējo tiesisko regulējumu, ko veido "kompleksa mijiedarbība" starp trim dažādiem tiesību aktiem — 1998. gada Cilvēktiesību aktu, 1994. gada Izlūkdienestu aktu un 2000. gada Aktu par izmeklēšanas pilnvaru regulēšanu;

24. atzīmē, ka ir pārskatīts Nīderlandes 2002. gada Izlūkošanas un drošības akts (*Dessens* komisijas 2013. gada 2. decembra ziņojums); atbalsta tos pārskatīšanas komisijas ieteikumus, kuru mērķis ir stiprināt Nīderlandes izlūkdienestu pārredzamību, kontroli un uzraudzību; aicina Nīderlandi atturēties no izlūkdienestu pilnvaru paplašināšanas tādā veidā, kas ļauj veikt nevainīgu iedzīvotāju komunikācijas pa kabeļiem nemērķtiecīgu novērošanu lielā apmērā, jo īpaši ņemot vērā to, ka viens no lielākajiem interneta plūsmu apmaiņas punktiem pasaulē atrodas Amsterdamā (*AMS-IX*); prasa uzmanīgi noteikt jaunās Kopīgās *Sigint* kibervienības pilnvaras un spējas, kā arī uzmanīgi attiekties pret ASV izlūkošanas personāla uzturēšanos un darbībām Nīderlandes teritorijā;

25. aicina dalībvalstis, tostarp, ja tās pārstāv to izlūkošanas aģentūras, nepieņemt datus no trešām valstīm, kas savākti nelikumīgi, un neļaut trešo valstu valdībām vai aģentūrām savā teritorijā veikt novērošanas darbības, kuras saskaņā ar valstu tiesību aktiem ir nelikumīgas vai neatbilst starptautiskajos vai ES instrumentos paredzētajām tiesiskajām garantijām, tostarp attiecībā uz cilvēktiesību aizsardzību saskaņā ar LES, ECTK un ES Pamattiesību hartu;

26. prasa visiem slepenajiem dienestiem pārtraukt masveida noklausīšanos un ar tīmekļa kameru uzņemtu attēlu apstrādi; aicina dalībvalstis pilnībā izmeklēt, vai, kā un kādā mērā to attiecīgie slepenie dienesti ir bijuši iesaistīti ar tīmekļa kameru uzņemtu attēlu apstrādē, un iznīcināt visus glabātos attēlus, kuri savākti, izmantojot šādas masveida novērošanas programmas;

27. aicina dalībvalstis nekavējoties izpildīt savu pienākumu rīkoties, kā noteikts Eiropas Cilvēktiesību konvencijā, lai aizsargātu savus iedzīvotājus no trešo valstu vai pašu izlūkdienestu veiktas novērošanas, kas ir pretrunā šīs konvencijas prasībām, tostarp gadījumos, kad novērošanas mērķis ir aizsargāt valsts drošību, un nodrošināt, ka trešās valsts tiesību aktu eksteritoriālas piemērošanas rezultātā netiek vājināts tiesiskums;

28. aicina Eiropas Padomes ģenerālsekretāru uzsākt ECTK 52. pantā paredzēto procedūru, saskaņā ar kuru "saņemot pieprasījumu no Eiropas Padomes Ģenerālsekretāra, jebkura Augstā Līgumslēdzēja Puse sniedz paskaidrojumus par veidu, kādā tās iekšējie tiesību akti nodrošina efektīvu jebkura šīs Konvencijas nosacījuma īstenošanu";

29. aicina dalībvalstis nekavējoties veikt atbilstošus pasākumus, tostarp sākt tiesvedību par suverenitātes un līdz ar to arī vispārējo starptautisko tiesību pārkāpšanu, īstenojot masveida novērošanas programmas; turklāt aicina dalībvalstis izmantot arī visus pieejamos starptautiskos līdzekļus, lai aizsargātu ES iedzīvotāju pamattiesības, jo īpaši uzsākot starpvalstu sūdzību procedūru saskaņā ar Starptautiskā pakta par pilsoniskajām un politiskajām tiesībām (*ICCPR*) 41. pantu;

30. aicina dalībvalstis izveidot efektīvus mehānismus, kas ļautu par varas ļaunprātīgu izmantošanu saukt pie atbildības tās personas, kuras ir atbildīgas par (masveida) novērošanas programmām, kas neievēro tiesiskumu un pilsoņu pamattiesības;

31. aicina ASV nekavējoties pārskatīt savus tiesību aktus, lai panāktu to atbilstību starptautiskajām tiesībām, atzīt ES iedzīvotāju privātumu un citas tiesības, nodrošināt ES iedzīvotājiem tiesisko aizsardzību, nodrošināt ES iedzīvotājiem līdzvērtīgas tiesības tām, kas ir ASV iedzīvotājiem, un parakstīt Fakultatīvo protokolu, ļaujot privātpersonām izmantot *ICCPR* paredzēto sūdzību procedūru;

32. atzinīgi vērtē šajā saistībā ASV prezidenta *B. Obama* 2014. gada 17. janvārī izteiktās piezīmes un izdoto Prezidenta politikas direktīvu, kas ir solis ceļā uz to, lai ierobežotu pilnvaras izmantot novērošanu un datu apstrādi valsts drošības nolūkos un lai ASV izlūkošanas kopienai būtu vienāda attieksme pret visu cilvēku personas informāciju neatkarīgi no viņu tautības vai dzīvesvietas; tomēr sagaida ES un ASV attiecībās turpmākus konkrētus soļus, lai stiprinātu uzticību transatlantiskajās datu plūsmās un nodrošinātu saistošas garantijas ES privātuma tiesību īstenošanai, kas ir sīki izklāstīta šajā ziņojumā;

33. uzsver savas nopietnās bažas par darbu Eiropas Padomes Konvencijas par kibernoziegumiem komitejā, interpretējot 2001. gada 23. novembra Konvencijas par kibernoziegumiem 32. pantu (Budapeštas konvencija) par pārrobežu piekļuvi datorā uzglabātiem datiem ar piekrišanu vai ja tie ir publiski pieejami, un iebilst pret to, ka tiek noslēgts papildu protokols vai norādījumi, kuru mērķis ir paplašināt šā noteikuma piemērošanas jomu, kas ir noteikta atbilstoši pašreizējam šajā konvencijā paredzētajam režīmam, kas jau tā ir nozīmīgs teritorialitātes principa izņēmums, jo tas varētu izraisīt situāciju, ka tiesībaizsardzības iestādes var brīvi attālināti piekļūt serveriem un datoriem, kuri atrodas citās jurisdikcijās, neatsaucoties uz savstarpējās tiesiskās palīdzības nolīgumiem un citiem tiesiskās sadarbības instrumentiem, kas ir paredzēti, lai garantētu, ka tiek ievērotas cilvēka pamattiesības, tostarp tiesības uz datu aizsardzību un tiesību aktos paredzētās kārtības ievērošanu un jo īpaši Eiropas Padomes 108. konvencija;

34. aicina Komisiju līdz 2014. gada jūlijam novērtēt Regulas (EK) Nr. 2271/96 piemērojamību gadījumiem, kad pastāv pretruna starp tiesību aktiem attiecībā uz personas datu pārsūtīšanu;

35. aicina Pamattiesību aģentūru veikt padziļinātu izpēti par pamattiesību aizsardzību novērošanas kontekstā un jo īpaši par ES pilsoņu pašreizējo stāvokli attiecībā uz viņiem pieejamiem tiesiskās aizsardzības līdzekļiem saistībā ar minēto praksi;

Datu starptautiskā pārsūtīšana

ASV tiesiskais regulējums datu aizsardzības jomā un ASV "drošības zona"

36. norāda, ka uzņēmumi, par kuriem plašsaziņas līdzekļos ir atklāts, ka tie ir iesaistīti ASV NDA plašā mērogā veiktajā ES datu subjektu masveida novērošanā, ir uzņēmumi, kas paši ir apliecinājuši, ka tie stingri ievēro "drošības zonas" principus, un ka "drošības zona" ir juridisks instruments, kuru izmanto ES personas datu pārsūtīšanai uz ASV (piemēram, *Google*, *Microsoft*, *Yahoo!*, *Facebook*, *Apple* un *LinkedIn*); pauž bažas par to, ka šīs organizācijas nav šifrējušas informācijas un komunikācijas plūsmu starp saviem datu centriem, tādējādi ļaujot izlūkdienestiem šo informāciju pārtvert; atzinīgi vērtē dažu ASV uzņēmumu sniegtos paziņojumus par to, ka tie paātrināti īstenos plānus par datu plūsmu šifrēšanu starp to datu centriem pasaulē;

37. uzskata, ka ES izlūkošanas aģentūru plašā piekļuve "drošības zonas" apstrādātajiem ES personas datiem neatbilst kritērijiem attiecībā uz atkāpi saistībā ar valsts drošību;

38. uzskata, ka, tā kā pašreizējos apstākļos "drošības zonas" principi nenodrošina ES iedzīvotāju pienācīgu aizsardzību, datu pārsūtīšana būtu jāveic, izmantojot citus instrumentus, piemēram, līguma klauzulas vai saistošos uzņēmumu noteikumus, ja vien tajos ir noteiktas īpašas garantijas un tiesiskās aizsardzības līdzekļi un ja tos nevar apiet, izmantojot citus tiesiskos regulējumus;

39. uzskata, ka Komisija ir rīkojusies nesekmīgi, lai novērstu labi zināmās nepilnības "drošības zonas" pašreizējā īstenošanā;

40. aicina Komisiju piedāvāt pasākumus, kas paredz nekavējoties apturēt Komisijas Lēmumu 2000/520/EK, kurā ir paziņots par pienācīgu aizsardzību, ko nodrošina privātuma "drošības zonas" principi, un attiecīgajiem visbiežāk uzdotajiem jautājumiem, kurus izdevusi ASV Tirdzniecības ministrija; tādēļ aicina ASV iestādes nākt klajā ar priekšlikumu par jaunu sistēmu, kā pārsūtīt personas datus no ES uz ASV tā, lai tiktu ievērotas Savienības tiesību aktu prasības par datu aizsardzību un nodrošināts nepieciešamais attiecīgais aizsardzības līmenis;

41. aicina dalībvalstu kompetentās iestādes, jo īpaši datu aizsardzības iestādes, īstenot savas pašreizējās pilnvaras un nekavējoties pārtraukt datu plūsmu uz visām organizācijām, kuras pašas ir apliecinājušas, ka tās stingri ievēro ASV "drošības zonas" principus, un pieprasīt, lai šāda datu pārsūtīšana notiktu tikai tādā gadījumā, ja tiek izmantoti citi instrumenti ar nosacījumu, ka tie nodrošina nepieciešamos tiesiskās aizsardzības līdzekļus un garantijas attiecībā uz personu privātuma un pamattiesību un brīvību aizsardzību;

42. aicina Komisiju līdz 2014. gada decembrim sniegt visaptverošu novērtējumu par ASV privātuma regulējumu, aptverot komerciālās, tiesībaizsardzības un izlūkošanas darbības un konkrētus ieteikumus, ņemot vērā to, ka ASV nav vispārīga datu aizsardzības tiesību akta; mudina Komisiju sadarboties ar ASV valdību, lai izveidotu tiesisko regulējumu, kas iedzīvotājiem nodrošina augstu aizsardzības līmeni attiecībā uz viņu personas datu aizsardzību tad, kad tie tiek nosūtīti ASV, un nodrošināt ES un ASV privātuma regulējuma saderību;

Datu pārsūtīšana uz citām trešām valstīm ar lēmumu par pienācīgu aizsardzību

43. atgādina, ka Direktīvā 95/46/EK ir noteikts, ka personas datu pārsūtīšana uz trešo valsti var notikt tikai tādā gadījumā, ja, neierobežojot atbilstību valsts noteikumiem, kas pieņemti saskaņā ar šīs direktīvas pārējiem noteikumiem, attiecīgā trešā valsts nodrošina pienācīgu aizsardzības līmeni, un šā noteikuma mērķis ir nodrošināt ES datu aizsardzības tiesību aktos paredzētās aizsardzības nepārtrauktību gadījumā, kad personas dati tiek pārsūtīti ārpus ES;

44. atgādina, ka Direktīvā 95/46/EK ir arī noteikts, ka, novērtējot, vai trešās valsts nodrošinātā aizsardzība ir pienācīga, ir jāņem vērā visi ar datu pārsūtīšanas darbību vai šādu darbību kopumu saistītie apstākļi; tāpat atgādina, ka saskaņā ar minēto direktīvu Komisijai ir piešķirtas īstenošanas pilnvaras paziņot, ka, ņemot vērā Direktīvā 95/46/EK noteiktos kritērijus, trešā valsts nodrošina pienācīgu aizsardzības līmeni; atgādina, ka saskaņā ar Direktīvu 95/46/EK Komisija ir arī pilnvarota paziņot, ka trešā valsts nenodrošina pienācīgu aizsardzības līmeni;

45. atgādina, ka pēdējā gadījumā dalībvalstīm ir jāveic vajadzīgie pasākumi, lai nepieļautu tāda paša tipa datu pārsūtīšanu uz attiecīgo trešo valsti, un Komisijai būtu jāsāk sarunas, lai šo situāciju labotu;

46. aicina Komisiju un dalībvalstis nekavējoties novērtēt, vai pienācīgo aizsardzības līmeni, ko nodrošina Jaunzēlandes likums par privātumu un Kanādas likums par personas datu aizsardzību un elektroniskajiem dokumentiem un kas ir atzīts Komisijas Lēmumā 2013/65/ES un Lēmumā Nr. 2002/2/EK, nav ietekmējusi šo valstu izlūkošanas aģentūru iesaistīšanās ES iedzīvotāju masveida novērošanā, un vajadzības gadījumā veikt atbilstošus pasākumus, lai apturētu vai atceltu lēmumu par pienācīgu aizsardzību; aicina Komisiju arī izvērtēt situāciju attiecībā uz citām valstīm, kuras ir saņēmušas atbilstības novērtējumu; gaida, ka vēlākais līdz 2014. gada decembrim Komisija ziņos Parlamentam par novērtēšanas rezultātiem iepriekš minētajās valstīs;

Datu pārsūtīšana saskaņā ar līguma klauzulām un citiem instrumentiem

47. atgādina, ka valstu datu aizsardzības iestādes ir norādījušas, ka ne līguma standartklauzulās, ne saistošajos uzņēmumu noteikumos nav formulētas situācijas par piekļuvi personas datiem masveida novērošanas nolūkā un ka šāda piekļuve neatbilstu līguma klauzulu vai saistošo uzņēmumu noteikumu atkāpēm, kuras ārkārtas apstākļos piemēro demokrātiskas sabiedrības interešu vārdā un tikai tad, ja tas ir nepieciešami un samērīgi;

48. aicina dalībvalstis aizliegt vai apturēt datu plūsmas uz trešām valstīm, ko pārsūta saskaņā ar līguma standartklauzulām, līgumu klauzulām vai saistošiem uzņēmumu noteikumiem, ko apstiprinājušas valstu kompetentās iestādes, ja ir iespējams, ka saskaņā ar tiesību aktu, ko piemēro datu saņēmējiem, viņiem uzliek pildīt prasības, kuras ir noteikti nepieciešamas, piemērotas un samērīgas demokrātiskā sabiedrībā un kuras, iespējams, negatīvi ietekmēs garantijas, ko nodrošina datu aizsardzības jomā piemērojamie tiesību akti un līguma standartklauzulas, vai ja turpmāka pārsūtīšana varētu radīt nopietnu kaitējumu datu subjektiem;

49. aicina 29. panta darba grupu izdot pamatnostādnes un ieteikumus par garantijām un aizsardzības pasākumiem, kas būtu jāiekļauj līgumsaistību instrumentos, ko piemēro ES personas datu pārsūtīšanai starptautiskā mērogā, lai nodrošinātu cilvēku privātuma, pamattiesību un brīvību aizsardzību, īpaši ņemot vērā trešo valstu tiesību aktus par izlūkošanu un valsts drošību, kā arī to uzņēmumu līdzdalību, kuri trešā valstī saņem datus, trešās valsts izlūkošanas aģentūrām veicot masveida novērošanas darbības;

50. aicina Komisiju bez kavēšanās izvērtēt savas izstrādātās līguma standartklauzulas, lai novērtētu, vai tajās tiek nodrošināta vajadzīgā aizsardzība saistībā ar piekļuvi personas datiem, kas saskaņā ar šīm klauzulām pārsūtīti izmeklēšanas nolūkā, un vajadzības gadījumā šīs klauzulas pārskatīt;

Datu pārsūtīšana saskaņā ar nolīgumu par savstarpēju tiesisko palīdzību

51. aicina Komisiju līdz 2014. gada beigām veikt pašreizējā nolīguma par savstarpēju tiesisko palīdzību padziļinātu izvērtēšanu atbilstīgi tā 17. pantam, lai pārbaudītu tā īstenošanu praksē un jo īpaši — vai ASV patiešām to ir izmantojušas, lai iegūtu informāciju vai pierādījumus ES, un vai nolīgums ir ticis pārkāpts, lai informāciju ES iegūtu tieši, kā arī lai novērtētu tā ietekmi uz cilvēku pamattiesībām; šādā novērtējumā veiktā analīze nebūtu jāpamato tikai ar ASV oficiālajiem paziņojumiem, tas būtu jāpamato arī ar īpašu ES veiktu vērtējumu; šādā padziļinātā pārskatā būtu jāizvērtē arī Savienības konstitucionālās uzbūves piemērošana šim instrumentam, lai pielīdzinātu to Savienības tiesību aktiem, jo īpaši ņemot vērā tam pievienoto 36. protokolu un tā 10. pantu, kā arī 50. deklarāciju, kas attiecas uz minēto protokolu; aicina arī Padomi un Komisiju izvērtēt dalībvalstu un ASV divpusējos nolīgumus, lai nodrošinātu šo divpusējo nolīgumu saskaņotību ar tiem, kurus ES saglabā vai nolemj saglabāt ar ASV;

ES savstarpējā palīdzība krimināllietās

52. prasa Padomei un Komisijai ziņot Parlamentam par to, kā dalībvalstis faktiski izmato Konvenciju par dalībvalstu savstarpēju palīdzību krimināllietās, jo īpaši tās III sadaļu par telesakaru pārtveršanu; aicina Komisiju, kā prasīts saskaņā ar 50. deklarāciju, līdz 2014. gada beigām izvirzīt priekšlikumu par 36. protokolu, lai pielīdzinātu to Lisabonas līguma sistēmai;

Datu pārsūtīšana saskaņā ar nolīgumiem par TFTP *un PDR*

53. uzskata, ka no informācijas, ko sniedz Eiropas Komisija un ASV Valsts kase, nav skaidrs, vai ASV izlūkošanas aģentūrām pašām vai sadarbojoties ar ES valstu izlūkošanas aģentūrām un nevēršoties pie esošajiem divpusējiem savstarpējās juridiskās palīdzības un tiesu iestāžu sadarbības kanāliem, nelikumīgi iekļūstot *SWIFT* tīklos vai banku operatīvajās sistēmās, vai sakaru tīklos, ir piekļuve *SWIFT* finanšu ziņojumiem ES;

54. atgādina par savu 2013. gada 23. oktobra rezolūciju un prasa Komisijai apturēt *TFTP* nolīguma darbību;

55. aicina Komisiju risināt jautājumu, kas rada bažas — ka trīs galvenās datorizētās rezervācijas sistēmas, ko visā pasaulē izmanto aviosabiedrības, atrodas ASV un ka pasažieru datu reģistra dati tiek saglabāti mākoņu sistēmās, kas darbojas ASV teritorijā saskaņā ar ASV tiesību aktiem, kuri nenodrošina atbilstīgu datu aizsardzības līmeni;

Pamatnolīgums par datu aizsardzību policijas un tiesu iestāžu sadarbības jomā ("jumta nolīgums")

56. uzskata, ka apmierinošs risinājums saistībā ar "jumta nolīgumu" ir priekšnoteikums pilnīgai uzticēšanās atjaunošanai transatlantisko partneru starpā;

57. prasa nekavējoties atsākt sarunas ar ASV par "jumta nolīgumu", kas ES pilsoņiem nodrošinātu tādas pašas tiesības kā ASV pilsoņiem; turklāt uzsver, ka nolīgumā būtu jāparedz efektīvi un praktiski īstenojami administratīvie un juridiskie tiesiskās aizsardzības līdzekļi visiem ES pilsoņiem ASV bez diskriminācijas;

58. prasa Komisijai un Padomei, kamēr "jumta nolīgums" nav stājies spēkā, neierosināt jaunus nozaru nolīgumus vai režīmus ar ASV par tiesībaizsardzības īstenošanai vajadzīgo personas datu pārsūtīšanu;

59. mudina Komisiju līdz 2014. gada aprīlim iesniegt precīzu ziņojumu par dažādiem sarunu pilnvaru punktiem un faktisko stāvokli;

Datu aizsardzības reforma

60. aicina Padomes prezidentvalsti un dalībvalstis ātrāk pabeigt darbu pie Tiesību aktu kopuma attiecībā uz datu aizsardzību, lai 2014. gadā to būtu iespējams pieņemt un tādējādi pavisam drīz ES pilsoņiem nodrošināt labāku datu aizsardzību; uzsver, ka apņēmīga iesaistīšanās un pilnīgs atbalsts no Padomes puses ir nepieciešams priekšnoteikumu, lai trešām valstīm apliecinātu ticamību un autoritāti;

61. uzsver, ka gan Datu aizsardzības regula, gan Datu aizsardzības direktīva ir vajadzīga, lai aizsargātu cilvēku pamattiesības, un tādēļ tās jāuzskata par kopumu, kas jāpieņem vienlaikus, lai nodrošinātu, ka visas ES datu aizsardzības darbības jebkuros apstākļos nodrošina augstu aizsardzības līmeni; uzsver, ka turpmākus tiesībaizsardzības iestāžu sadarbības pasākumus pieņems tikai pēc tam, kad Padome ar Parlamentu un Komisiju būs uzsākusi sarunas par Tiesību aktu kopumu attiecībā uz datu aizsardzību;

62. atgādina, ka jēdzieni "integrēta privātuma aizsardzība" un "privātuma aizsardzība pēc noklusējuma" ir datu aizsardzības stiprināšanas piemērs, tās jāizmanto kā pamatnostādnes attiecībā uz visiem produktiem, pakalpojumiem un sistēmām, kas tiek piedāvātas internetā;

63. uzskata, ka augstāki pārredzamības un drošības standarti tiešsaistes un telesakaru jomā ir vajadzīgs pamatelements virzībā uz labāku datu aizsardzības regulējumu; tāpēc aicina Komisiju iesniegt tiesību akta priekšlikumu par standartizētiem vispārīgiem noteikumiem un nosacījumiem attiecībā uz tiešsaistes un telesakaru jomu un pilnvarot uzraudzības iestādi, lai uzraudzītu šo vispārīgo noteikumu un nosacījumu ievērošanu;

Mākoņdatošana

64. norāda, ka minētās darbības ir negatīvi ietekmējušas uzticēšanos ASV mākoņdatošanai un mākoņdatošanas pakalpojumu sniedzējiem; tāpēc uzsver, ka mākoņdatošanas un IT risinājumu izveide Eiropā ir būtisks izaugsmes un nodarbinātības, mākoņdatošanas pakalpojumu un to sniedzēju uzticamības elements un nodrošina augstu personas datu aizsardzības līmeni;

65. aicina visas Savienības pašreizējās valsts struktūras neizmantot mākoņdatošanas pakalpojumus situācijās, uz kurām varētu attiekties trešo valstu tiesību akti;

66. atkārtoti pauž nopietnas bažas par to, ka tiem mākoņdatošanas pakalpojumu sniedzējiem, kuriem piemēro trešo valstu tiesību aktus vai kuri izmanto trešās valstīs bāzētus glabāšanas serverus, ES personas dati un saskaņā ar mākoņdatošanas līgumiem apstrādātā informācija obligāti ir tieši jāatklāj trešo valstu varas iestādēm, kā arī par tiešu attālu piekļuvi personas datiem un informācijai, ko apstrādā trešo valstu tiesībaizsardzības iestādes un izlūkdienesti;

67. pauž nožēlu par to, ka šāda piekļuve parasti tiek nodrošināta, trešās valsts iestādēm tieši piemērojot pašām savas tiesību normas un neizmantojot tiesiskai sadarbībai izveidotus starptautiskus instrumentus, piemēram, nolīgumus par savstarpēju tiesisko palīdzību (STP) vai cita veida tiesu iestāžu sadarbību;

68. aicina Komisiju un dalībvalstis ātrāk pabeigt Eiropas Mākoņdatošanas partnerības izveidi, vienlaikus nodrošinot pilnīgu pilsoniskās sabiedrības un tehniskās kopienas pārstāvju, piemēram, Interneta tehniskās uzdevumgrupas (*IETF*) iesaistīšanu un datu aizsardzības aspektu iekļaušanu;

69. mudina Komisiju sarunās par starptautiskiem nolīgumiem, kas ir saistīti ar personas datu apstrādi, pievērst īpašu uzmanību riskiem un problēmām, ko mākoņdatošana rada attiecībā uz pamattiesībām, jo īpaši, bet ne tikai tiesībām uz privāto dzīvi un personas datu aizsardzību, kā noteikts Eiropas Savienības Pamattiesību hartas 7. un 8. pantā; turklāt mudina Komisiju ņemt vērā sarunu partnervalsts noteikumus, ar kuriem nosaka tiesībaizsardzības iestāžu un izlūkdienestu piekļuvi mākoņdatošanas pakalpojumos apstrādātajiem personas datiem, jo īpaši pieprasot, lai šāda piekļuve notiktu tikai atbilstoši tiesību aktos paredzētajai kārtībai un ar precīzu juridisko pamatu, kā arī izvirzot prasību skaidri norādīt piekļuves apstākļus, šādas piekļuves mērķi, ieviestos drošības pasākumus datu nodošanā un personu tiesības, kā arī noteikumus par pārraudzību un efektīvas tiesiskās aizsardzības mehānismu;

70. atgādina, ka visiem uzņēmumiem, kas sniedz pakalpojumus Eiropas Savienībā, ir jāievēro ES tiesību akti, ka tie ir atbildīgi par jebkādiem pārkāpumiem un ka šajā ziņā nav pieļaujami nekādi izņēmumi, un uzsver, cik svarīgas ir efektīvas, samērīgas un atturošas administratīvās sankcijas, kuras var piemērot mākoņdatošanas pakalpojumu sniedzējiem, kuri neievēro ES datu aizsardzības standartus;

71. aicina Komisiju un dalībvalstu kompetentās iestādes novērtēt, kādā ziņā ES noteikumi par privātumu un datu aizsardzību ir pārkāpti, ES juridiskajām personām sadarbojoties ar slepenajiem dienestiem vai pieņemot trešo valstu varas iestāžu izdotus tiesas rīkojumus, kuros pieprasīti ES iedzīvotāju personas dati, tādējādi pārkāpjot ES datu aizsardzības tiesību aktus;

72. aicina uzņēmumus, kas sniedz jaunus pakalpojumus, kuros tiek izmantoti lieli datu apjomi un jaunas lietojumprogrammatūras, piemēram, "lietu internets" ("*Internet of Things*"), jau izstrādes posmā iekļaut datu aizsardzības pasākumus, lai saglabātu augstu iedzīvotāju uzticības līmeni;

*Transatlantiskais nolīgums par tirdzniecību un ieguldījumu partnerību (*TTIP)

73. atzīst, ka ES un ASV risina sarunas par transatlantisko tirdzniecības un ieguldījumu partnerību, kam ir milzīga nozīme turpmākas ekonomiskās izaugsmes radīšanā;

74. stingri uzsver, ņemot vērā digitālās ekonomikas nozīmi šajās attiecībās un jautājumu par ES un ASV savstarpējās uzticēšanās atjaunošanu, ka bez iepriekšēja piemērota risinājuma panākšanas attiecībā uz ES iedzīvotāju datu privātuma tiesībām, tostarp tiesībām uz administratīvu un tiesisku aizsardzību, Eiropas Parlamenta piekrišana *TTIP* nolīguma galīgajai redakcijai varētu tikt apdraudēta, ciktāl pilnībā nebūs pārtrauktas vispārējās masveida novērošanas darbības un ES iestāžu

un diplomātisko pārstāvniecību sakaru pārtveršana; uzsver, ka Parlaments tikai tad var piekrist *TTIP* nolīguma galīgajai redakcijai, ja nolīgumā cita starpā pilnā mērā būs ievērotas ES hartā atzītās pamattiesības un ja cilvēku privātās dzīves aizsardzību personas datu apstrādes un izplatīšanas jomā arī turpmāk regulēs *GATS* XIV pants; uzsver, ka ES datu aizsardzības tiesību aktus nekādi nevar uzskatīt par "patvaļīgu un nepamatotu diskrimināciju", piemērojot *GATS* XIV pantu;

Izlūkošanas dienestu demokrātiskā uzraudzība

75. uzsver, ka par spīti tam, ka izlūkošanas dienestu darbības uzraudzība būtu jāpamato gan ar demokrātisko leģitimitāti (stingru tiesisko regulējumu, iepriekšēju apstiprinājumu un paveiktā novērtējumu), gan ar atbilstīgām tehniskām spējām un īpašām zināšanām, vairākumam pašreizējo ES un ASV uzraudzības iestāžu dramatiski trūkst visa minētā, jo īpaši — tehnisko iespēju;

76. aicina, līdzīgi kā *Echelon* lietā, visus valstu parlamentus, kuri vēl nav to izdarījuši, izveidot izlūkošanas darbību jēgpilnu uzraudzību, ko veic parlamenta deputāti vai ekspertu struktūras, kurām ir likumīgas tiesības veikt izmeklēšanu; aicina valstu parlamentus, lai nodrošinātu izlūkošanas dienestu efektīvu uzraudzību, nodrošināt šādām uzraudzības komitejām/struktūrām pietiekamus resursus, tehnisko zinātību un juridiskus līdzekļus, tostarp tiesības veikt pārbaudes uz vietas;

77. prasa izveidot deputātu un ekspertu darba grupu, kas pārredzami un sadarbībā ar dalībvalstu parlamentiem pārbaudītu ieteikumus par to, kā uzlabot demokrātisko, kā arī parlamentāro uzraudzību pār izlūkdienestiem un kā pastiprināt uzraudzības sadarbību ES, jo īpaši attiecībā uz tās pārrobežu aspektu; uzskata, ka grupai būtu jo īpaši jāpārbauda iespēja noteikt Eiropas standartu minimumu vai pamatnostādnes izlūkošanas dienestu uzraudzībai (ex ante un ex post), pamatojoties uz pašreizējo paraugpraksi un starptautisku struktūru (ANO, Eiropas Padomes) ieteikumiem, tostarp jautājums par uzraudzības struktūras uzskatīšanu par trešo personu saskaņā ar "trešās personas likumu" vai "izcelsmes iestādes kontroles" principu, kā arī jautājums par ārvalstu izlūkošanas uzraudzību un pārskatatbildību un labākas pārredzamības kritēriji, pamatojoties uz vispārējo principu attiecībā uz piekļuvi informācijai un tā sauktajiem "Tshwane principiem" ([1]), kā arī principiem attiecībā uz jebkādas novērošanas ilgumu un apmēru, nodrošinot, ka tā ir samērīga un atbilst tās nolūkam;

78. aicina šo grupu līdz 2015. gada sākumam sagatavot ziņojumu un palīdzēt sagatavoties konferencei, kuru Parlaments rīkos kopā ar parlamentārām vai neatkarīgām dalībvalstu uzraudzības struktūrām;

79. aicina dalībvalstis izmantot paraugprakses piemērus, lai uzlabotu savu uzraudzības iestāžu piekļuvi informācijai par izlūkošanas darbībām (tostarp klasificētai informācijai un citu dienestu sniegtai informācijai) un noteikt pilnvaras pārbaudēm uz vietas, stingras pilnvaras veikt pratināšanu, nodrošināt atbilstīgus resursus tehniskās zināšanas, pilnīgu neatkarību no valdības un pienākumu ziņot attiecīgajiem parlamentiem;

80. aicina dalībvalstis izveidot uzraudzības iestāžu sadarbību, jo īpaši Eiropas tīklā valstu izlūkošanas pārraugiem (*ENNIR*);

81. mudina AP/PV regulāri ziņot Parlamenta atbildīgajiem dienestiem par ES Izlūkdatu analīzes centra (IntCen), kurš ietilpst Eiropas Ārējās darbības dienestā, darbībām, tostarp par galveno cilvēktiesību un piemērojamo ES datu privātuma noteikumu ievērošanu pilnībā, tādējādi ļaujot Parlamentam gūt labāku ieskatu ES politikas ārējā dimensijā; mudina AP/VP iesniegt priekšlikumu IntCen darbības juridiskajam pamatam, ja tiktu paredzētas darbības vai tālākas kompetences izlūkošanas jomā vai pašā datu vākšanas sistēmā, kam var būt ietekme uz ES iekšējās drošības stratēģiju;

([1]) "The Global Principles on National Security and the Right to Information" (Vispārējie principi attiecībā uz valsts drošību un tiesības uz informāciju), 2013. gada jūnijs.

82. aicina Komisiju līdz 2014. gada decembrim piedāvāt priekšlikumu par ES drošības pielaides izsniegšanas procedūru visām ES amatpersonām, jo pašreizējā sistēmā, kur drošības pielaides izsniegšanas procedūru veic valstspiederības dalībvalsts un valstu sistēmās ir atšķirīgas prasības un procedūru ilgums, tādējādi atkarībā no valstspiederības attieksme pret Parlamenta deputātiem un to darbiniekiem atšķiras;

83. atgādina Eiropas Parlamenta un Padomes iestāžu nolīguma noteikumus par to, kā Parlamentam nosūta un kā tas apstrādā Padomes rīcībā esošo klasificēto informāciju par jautājumiem, kas nav kopējās ārpolitikas un drošības politikas darbības jomā;

ES aģentūras

84. aicina Eiropola Apvienoto uzraudzības iestādi kopā ar valstu datu aizsardzības iestādēm līdz 2014. gada beigām veikt kopēju pārbaudi, lai novērtētu, vai valstu varas iestādes informāciju un personas datus, kas nodoti Eiropolam, ir ieguvušas likumīgi, jo īpaši tad, ja informāciju vai datus sākotnēji bija ieguvuši ES vai trešās valsts izlūkošanas dienesti, un vai ir izstrādāti atbilstīgi pasākumi, lai novērstu šādas informācijas vai datu izmantošanu un tālāku izplatīšanu; uzskata, ka Eiropolam nevajadzētu apstrādāt tādu informāciju un datus, kas iegūti, pārkāpjot pamattiesības, kuras būtu jāaizsargā saskaņā ar Pamattiesību hartu;

85. aicina Eiropolu pilnība izmantot tā pilnvaras un pieprasīt dalībvalstu kompetentajām iestādēm sākt kriminālizmeklēšanu par nozīmīgiem kiberuzbrukumiem un IT pārkāpumiem, kas satur pārrobežu ietekmes potenciālu; uzskata, ka būtu jāuzlabo Eiropola pilnvaras, lai tas varētu sākt patstāvīgu izmeklēšanu, ja ir radušās aizdomas par ļaunprātīgu uzbrukumu tīmekļa un divu vai vairāku dalībvalstu vai Savienības struktūru informācijas sistēmām ([1]); aicina Komisiju pārskatīt Eiropas Kibernoziedzības apkarošanas centra (*EC3*) darbību un vajadzības gadījumā iesniegt priekšlikumu visaptverošai sistēmai, kas palīdzētu stiprināt tā kompetenci;

Vārda brīvība

86. pauž nopietnas bažas par aizvien lielāku preses brīvības apdraudējumu un atturošo ietekmi uz žurnālistiem, ko valsts varas iestādes rada iebiedējot, jo īpaši attiecībā uz žurnālistu avotu konfidencialitāti; atkārto aicinājumus, kas pausti Parlamenta 2013. gada 21. maija rezolūcijā "ES harta — standartu noteikšana attiecībā uz plašsaziņas līdzekļu brīvību Eiropas Savienībā";

87. norāda uz to, ka tika apcietināts *David Miranda* un viņa rīcībā esošo materiālu Apvienotās Karalistes iestādes konfiscēja saskaņā ar 2000. gada Pretterorisma akta 7. pielikumu (kā arī avīzei *The Guardian* izvirzīja prasību iznīcināt vai atdot materiālu), un pauž bažas, ka tas, iespējams, ir nopietns ECTK 10. pantā un ES hartas 11. pantā atzītās vārda brīvības un plašsaziņas līdzekļu brīvības pārkāpums un ka šādos gadījumos varētu ļaunprātīgi izmantot tiesību normas, kuru mērķis ir cīņa pret terorismu;

88. vērš uzmanību uz ziņotājiem un viņu atbalstītājiem, tostarp žurnālistiem pēc viņu atklātajiem faktiem, doto solījumu; aicina veikt pārbaudi, vai turpmākajā tiesību akta priekšlikuma, ar ko izveido efektīvu un visaptverošu Eiropas ziņotāju aizsardzības programmu, ka tas jau tika pieprasīta parlamenta 2013. gada 23. oktobra rezolūcijā, būtu jāiekļauj arī citas Savienības kompetences jomas, īpašu uzmanību veltot tam, cik komplicēta ir ziņošana izlūkošanas jomā; aicina dalībvalstis rūpīgi izvērtēt iespēju piešķirt ziņotājiem starptautisko aizsardzību pret vajāšanu;

([1]) Eiropas Parlamenta 2014. gada 25. februāra nostāja par priekšlikumu Eiropas Parlamenta un Padomes regulai par Eiropas Savienības Aģentūru tiesībaizsardzības sadarbībai un apmācībai (Eiropolu) (Pieņemtie teksti, P7_TA(2014)0121)..

89. aicina dalībvalstis nodrošināt, ka to tiesību akti, jo īpaši valsts drošības jomā, sniedz drošu alternatīvu klusēt par pārkāpumu, tostarp korupcijas, noziegumu, juridisko saistību pārkāpšanas, tiesu kļūdu un varas ļaunprātīgas izmantošanas, nodošanu atklātībai un ziņošanu par to, kas arī atbilst noteikumiem dažādos starptautiskos (ANO un Eiropadomes) dokumentos, kuri vērsti pret korupciju, *PACE* rezolūcijā 1729 (2010) izklāstītajiem noteikumiem, *Tshwane* principiem utt.;

ES IT drošība

90. norāda, ka nesenie gadījumi uzskatāmi pierāda to, cik neaizsargāta šobrīd ir ES un jo īpaši ES iestādes, valstu valdības un parlamenti, Eiropas lielie uzņēmumi, Eiropas IT infrastruktūras un tīkli pret veikliem uzbrukumiem, ko veic, izmantojot sarežģītas programmatūras un ļaunprogrammatūras; norāda, ka šādu uzbrukumu īstenošanai vajadzīgi tāda mēroga finanšu un cilvēku resursi, ka, šķiet, tos organizējušas valsts struktūras, pildot ārvalstu valdību prasības; šajā ziņā uzskata, ka nelikumīga iekļuve telesakaru uzņēmumā *Belgacom* vai tā datu pārtveršana ir uztraucošs piemērs uzbrukumam ES IT spējām; uzsver, ka ES IT spējas un drošības veicināšana arī samazina ES neaizsargātību pret nopietniem kiberuzbrukumiem, ko veic plašas noziedzīgās organizācijas vai teroristu grupas;

91. uzskata, ka atklājumus par masveida novērošanu, kas ierosināja šo krīzi, Eiropa var izmantot kā iespēju uzņemties iniciatīvu un izveidot neatkarīgas galveno IT resursu tehniskās spējas kā stratēģisku pasākumu, kam piešķirta galvenā prioritāte; uzsver, ka, lai šādas ES IT spējas gūtu uzticību, to pamatā jābūt atklātiem standartiem un atklātai un bezmaksas programmatūrai un, ja iespējams, arī aparatūrai, padarot visu šo jomu, sākot ar procesoru izstrādi un beidzot ar lietojumprogrammatūru līmeni, pārskatāmu ikvienai ieinteresētajai personai; norāda, ka nolūkā atjaunot konkurētspēju stratēģiskajā IT pakalpojumu nozarē, ir vajadzīga jauna vienošanās digitālajā jomā, kuras panākšanai kopīgus un plašus centienus veltītu gan ES iestādes, gan dalībvalstis, pētniecības iestādes, rūpniecības nozares un pilsoniskā sabiedrība; aicina Komisiju un dalībvalstis izmantot publisko iepirkumu kā virzītājspēku, lai atbalstītu šādas tehnisko resursu spējas ES, padarot ES drošības un privātuma standartus par galveno prasību IT preču un pakalpojumu publiskajā iepirkumā; tāpēc mudina Komisiju pārskatīt spēkā esošās publiskā iepirkuma direktīvas attiecībā uz tādu publisko iepirkumu, kura pamatā ir datu izmantošana, lai lemtu par ierobežojumiem — ka gadījumā, ja iepirkums ir saistīts ar drošības vai citām būtiskām interesēm, publiskā iepirkuma procedūrās drīkst piedalīties tikai sertificēti uzņēmumi un ES uzņēmumi;

92. stingri nosoda to, ka izlūkošanas dienesti mēģina mazināt IT drošības standartus un plašā IT sistēmu klāstā uzstādīt "rezerves izejas"; aicina Komisiju iesniegt tiesību akta projektu nolūkā aizliegt tiesībaizsardzības iestādēm izmantot "rezerves izejas"; tādēļ iesaka visās vidēs, kur ir problēmas ar IT drošību, izmantot atvērtā pirmkoda programmatūru;

93. aicina dalībvalstis, Komisiju, Padomi un Eiropadomi sniegt pilnīgu atbalstu, tostarp ar finansējumu pētniecības un attīstības jomā, Eiropas inovatīvās un tehnoloģiskās spējas attīstīšanai attiecībā uz IT rīkiem, uzņēmumiem un pakalpojumu sniedzējiem (aparatūra, programmatūra, pakalpojumi un tīkls), tostarp kiberdrošības garantēšanas nolūkā, kā arī šifrēšanas un kriptogrāfijas tehniskās spējas; aicina visas atbildīgās ES iestādes un dalībvalstis veikt ieguldījumus ES vietējās un neatkarīgās tehnoloģijās un masveidā attīstīt un palielināt atklāšanas spējas;

94. aicina Komisiju, standartizācijas organizācijas un *ENISA* līdz 2014. gada decembrim izstrādāt obligātos drošības un privātuma standartus, kā arī pamatnostādnes IT sistēmām, tīkliem un pakalpojumiem, tostarp mākoņdatošanas pakalpojumiem, lai nodrošinātu ES pilsoņu personas datu labāku aizsardzību un visu IT sistēmu integritāti; uzskata, ka šādi standarti varētu kļūt par rādītāju jauniem globāliem standartiem un tie būtu jānosaka atvērtā un demokrātiskā procedūrā, ko nevirza viena valsts, struktūra vai starptautisks uzņēmums; uzskata, ka, lai gan nolūkā atbalstīt cīņu pret terorismu ir jāņem vērā likumīgi tiesībaizsardzības un izlūkošanas apsvērumi, tiem nebūtu jāmazina visu IT sistēmu uzticamība; pauž atbalstu Interneta tehniskās uzdevumgrupas (*IETF*) nesen pieņemtajiem lēmumiem iekļaut valdības interneta drošības apdraudējumu modelī;

95. norāda, ka gan ES, gan valstu telesakaru regulatīvās iestādes un atsevišķos gadījumos arī telesakaru uzņēmumi nepārprotami ir nevērīgi izturējušies pret savu lietotāju un klientu IT drošību; aicina Komisiju pilnā mērā izmantot pilnvaras, kas tai piešķirtas E-privātuma un telekomunikāciju direktīvā, lai stiprinātu sakaru konfidencialitātes aizsardzību, veicot pasākumus, kuri nodrošinātu termināļu aprīkojuma atbilstību lietotāju tiesībām uzraudzīt un aizsargāt savus personas datus, un lai garantētu telesakaru tīklu un pakalpojumu augstu drošības līmeni, tostarp prasot izmantot jaunākās sakaru galšifrēšanas iespējas;

96. atbalsta ES kiberstratēģiju, tomēr uzskata, ka tajā nav paredzēti visi iespējamie draudi un tā būtu jāpaplašina, lai ietvertu valsts ļaunprātīgu rīcību; uzsver nepieciešamību pēc stingrākas IT drošības un IT sistēmu izturētspējas;

97. aicina Komisiju vēlākais līdz 2015. gada janvārim piedāvāt rīcības plānu, lai palielinātu ES neatkarību IT nozarē, paredzot saskaņotāku pieeju Eiropas IT tehnisko spēju (tostarp IT sistēmas, aprīkojums, pakalpojumi, mākoņdatošana, šifrēšana un anonimizācija) uzlabošanai un būtiski svarīgu IT infrastruktūru (tostarp attiecībā uz īpašumtiesībām un neaizsargātību) aizsardzībai;

98. aicina Komisiju saistībā ar nākamo programmas "Apvārsnis 2020" darba programmu palielināt resursu apmēru, lai nodrošinātu izaugsmi Eiropas pētniecībai, attīstībai, inovācijai un apmācībai IT jomā, jo īpaši saistībā ar privātuma uzlabošanas tehnoloģijām un infrastruktūrām, kriptoloģiju, drošu datošanu, optimālajiem drošības risinājumiem, tostarp atvērtā pirmkoda drošības risinājumiem, un citiem informācijas sabiedrības pakalpojumiem, un arī veicināt iekšējo tirgu attiecībā uz Eiropas programmatūrām, materiāliem un šifrētiem saziņas līdzekļiem un komunikācijas infrastruktūrām, tostarp izstrādājot visaptverošu ES rūpniecības stratēģiju attiecībā uz IT rūpniecību; uzskata, ka īpaša nozīme pētniecībā ir mazajiem un vidējiem uzņēmumiem; uzsver, ka nekādu ES finansējumu nedrīkstētu piešķirt projektiem, kuru vienīgais mērķis ir izstrādāt instrumentus nelegālai piekļuvei IT sistēmām;

99. prasa Komisijai precizēt pašreizējos pienākumus un vēlākais līdz 2014. gada decembrim pārskatīt, vai Eiropola Kibernoziedzības apkarošanas centram un citiem Savienības specializēto zināšanu centriem, *ENISA*, *CERT-EU* un *EDPS* būtu jāpaplašina pilnvaras, jāuzlabo koordinēšana un/vai jāpiešķir papildu resursi un jāuzlabo tehniskās spējas, lai ļautu tiem uzņemties galveno lomu, nodrošinot Eiropas sakaru sistēmas, uzlabotu to iespējas efektīvāk novērst un izmeklēt lielus pārkāpumus IT jomā ES un veikt (vai šajā darbā atbalstīt dalībvalstu un ES struktūras) izmeklēšanu uz vietas saistībā ar lieliem pārkāpumiem IT jomā; jo īpaši aicina Komisiju apsvērt iespēju pastiprināt *ENISA* lomu ES iestāžu iekšējo sistēmu aizsardzībā un izveidot *ENISA* struktūrā Datorapdraudējumu reaģēšanas vienību (*CERT*) Eiropas Savienībai un tās dalībvalstīm;

100. prasa Komisijai apsvērt nepieciešamību pēc ES IT akadēmijas, kur būtu visu saistīto jomu labākie neatkarīgie Eiropas un starptautiskie eksperti, kuru uzdevums būtu profesionāli konsultēt visas attiecīgās ES iestādes un struktūras par IT tehnoloģijām, tostarp par drošības stratēģijām;

101. aicina Eiropas Parlamenta priekšsēdētāja pakļautībā esošā Eiropas Parlamenta sekretariāta kompetentos dienestus vēlākais līdz 2015. gada jūnijam, iesniedzot vēlākais līdz 2014. gada decembrim starpposma ziņojumu, rūpīgi pārskatīt un novērtēt Eiropas Parlamenta IT drošības uzticamību, galveno uzmanību pievēršot: budžeta līdzekļiem, darbinieku resursiem, tehniskajām spējām, iekšējai organizācijai un visiem attiecīgajiem elementiem, lai panāktu Parlamenta IT sistēmu augstu drošības līmeni; uzskata, ka šāds novērtējums sniegtu vismaz informācijas analīzi un ieteikumus šādos jautājumos:

— vai ir vajadzīgas regulāras, stingras un neatkarīgas drošības revīzijas un nelikumīgas piekļuves pārbaudes, izvēloties ārējos drošības ekspertus un nodrošinot to darba pārredzamību un to akreditācijas datu garantijas attiecībā pret trešām valstīm vai jebkurām citām likumīgām interesēm;

— konkrētu paraugprakses IT drošības/privātuma prasību iekļaušana jaunu IT sistēmu publiskā iepirkuma procedūrās, tostarp iespēja par iepirkuma nosacījumu noteikt prasību par atvērtā pirmkoda programmatūru vai arī prasību, ka jutīgās, ar drošību saistītās jomās publiskā iepirkuma procedūrās var piedalīties vienīgi uzticami Eiropas uzņēmumi;

— to uzņēmumu saraksts, kuriem ir līgums ar Eiropas Parlamentu IT un telekomunikāciju jomās, ņemot vērā jebkuru informāciju, kas atklājusies par to sadarbību ar izlūkdienestiem (piemēram, klajā nākusī informācija par VDI līgumiem ar tādiem uzņēmumiem kā *RSA*, kuru produktus Eiropas Parlaments izmanto, lai, domājams, aizsargātu deputātu un darbinieku attālinātu piekļuvi saviem datiem), tostarp iespējamību, ka tādus pašus pakalpojumus varētu sniegt citi, vēlams — Eiropas — uzņēmumi;

— to programmatūru, un jo īpaši "gatavās" komerciālās programmatūras, ticamība un izturētspēja, kuras ES iestādes izmanto savās IT sistēmās, attiecībā uz nelikumīgu piekļuvi un traucējumiem, ko rada ES vai trešo valstu tiesībaizsardzības un izlūkošanas iestādes, arī ņemot vērā attiecīgos starptautiskos standartus, paraugprakses drošības riska pārvaldības principus un ES Tīklu un informācijas drošības standartu izmantošana drošības pārkāpumu gadījumā;

— atvērtā pirmkoda sistēmu plašāka izmantošana;

— darbības un pasākumi, kas veicami nolūkā risināt ar mobilo ierīču (piemēram, darba vai privātie viedtālruņi, planšetdatori) plašāku izmantošanu saistītās problēmas un novērst to ietekmi uz sistēmas IT drošību;

— Eiropas Parlamenta dažādo darbavietu savstarpējo sakaru un Eiropas Parlamentā izmantoto IT sistēmu drošība;

— Parlamenta IT sistēmā vajadzīgo serveru un IT centru izmantošana un atrašanās vieta un to ietekme uz sistēmu drošību un integritāti;

— spēkā esošo drošības pārkāpumu noteikumu faktiskā īstenošana un kompetento iestāžu tūlītēja ziņošana par šiem pārkāpumiem publiski pieejamos telesakaru tīklos;

— Eiropas Parlamenta datu uzglabāšanas pakalpojumu izmantošana mākonī, tostarp uzglabāto datu veids, satura un piekļuves aizsardzības veids un mākoņa serveru atrašanās vieta, precizējot piemērojamo datu aizsardzības un izlūkošanas tiesisko regulējumu, kā arī izvērtējums attiecībā uz to, kā mākoņu serverus būtu iespējams izvietot vienīgi ES teritorijā;

— plāns, kas nodrošinātu plašākas kriptogrāfijas tehnoloģiju izmantošanas iespējas, jo īpaši, autentiskuma apstiprināšanas galšifrēšanu visiem IT un sakaru pakalpojumiem, piemēram, mākoņdatošanas, e-pasta, tūlītējas ziņojumapmaiņas un telefonijas pakalpojumiem;

— elektroniskā paraksta izmantošana e-pasta vēstulēs;

— plāns sistēmas *GNU Privacy Guard* izmantošanai, šo sistēmu izmantojot kā noklusēto šifrēšanas standartu e-pasta vēstulēm un vienlaikus nodrošinot iespēju izmantot elektronisko parakstu;

— iespēja izveidot drošu tūlītējās ziņojumapmaiņas pakalpojumu Eiropas Parlamentā, tādējādi nodrošinot drošus sakarus, izmantojot serveri, kas izskata tikai šifrētu saturu;

102. aicina visas ES iestādes un aģentūras, jo īpaši Eiropadomi, Padomi, Eiropas Ārējās darbības dienestu (arī ES delegācijas), Komisiju, Tiesu un Eiropas Centrālo banku, vēlākais līdz 2015. gada jūnijam, iesniedzot līdz 2014. gada decembrim starpposma ziņojumu, sadarbībā ar ENISA, Eiropolu un datorapdraudējumu reaģēšanas vienībām (CERT) veikt līdzīgu uzdevumu; aicina dalībvalstis veikt līdzīgu novērtējumu;

103. uzsver, ka attiecībā uz ES ārējām darbībām būtu jāveic saistīto budžeta vajadzību novērtējums un vispirms nekavējoties jāveic pasākumi saistībā ar Eiropas ārējās darbības dienestu (EĀDD), un ka 2015. gada budžeta projektā tam jāparedz pienācīgs finansējums;

104. uzskata, ka masveida IT sistēmas, ko izmanto brīvības, drošības un tiesiskuma telpā, piemēram, Šengenas Informācijas sistēma II, *Eurodac* un nākotnē iespējamās sistēmas, piemēram, *EU-ESTA*, būtu jāizstrādā un jāpārvalda tādā veidā, lai neradītu iespēju apdraudēt datus, kā tas notiek ar trešo valstu varas iestāžu pieprasījumiem; prasa aģentūrai *eu-LISA* līdz 2014. gada beigām ziņot Parlamentam par izmantojamo sistēmu drošumu;

105. aicina Komisiju un EĀDD ņemt vērā starptautisko līmeni, jo īpaši ASV, un, sadarbojoties ar ieinteresētajiem partneriem, ieviest interneta demokrātiskas pārvaldības ES stratēģiju, lai novērstu nevajadzīgu ietekmi, ko ar organizāciju ICANN un IANA darbību starpniecību rada jebkura atsevišķa iestāde, uzņēmums vai valsts, šajās organizācijās nodrošinot visu ieinteresēto personu pienācīgu pārstāvību, vienlaikus novēršot valsts kontroles vai cenzūras palielināšanos vai interneta "balkanizēšanos" vai fragmentēšanos;

106. aicina Es uzņemties vadošo lomu, pārveidojot interneta kopējo uzbūvi un pārvaldību, lai pievērstos riskiem, kas saistīti ar datu plūsmām un datu glabāšanu, cenšoties panākt datu apjoma samazināšanu un pārredzamību un decentralizēt jēldatu glabāšanu lielapjoma atmiņā, kā arī panākt interneta datplūsmas pārmaršrutēšanu vai visas interneta datplūsmas pilnīgu galšifrēšanu, lai datplūsmu nevajadzīga maršrutēšana caur tādu valstu teritorijām, kuras neievēro pamattiesību, datu aizsardzības un privātuma pamatstandartus, neradītu risku;

107. aicina popularizēt:

— ES meklētājprogrammas un ES sociālos tīklus kā vērtīgu instrumentu, ko izmantot virzībā uz ES neatkarību IT jomā;

— Eiropas IT pakalpojumu sniedzējus;

— sakaru plūsmu, tostarp izmantojot e-pastu un īsziņas, vispārēju šifrēšanu;

— galvenos Eiropas IT jomas elementus, piemēram, klienta serveru operētājsistēmas risinājumus, atvērtā pirmkoda standartu izmantošanu, Eiropas elementu tīklu savienošanai, piemēram, maršrutētāju, izstrādi;

108. aicina Komisiju iesniegt tiesību akta priekšlikumu par datplūsmu maršrutēšanas sistēmu, ieskaitot zvanu ierakstu (CDR) apstrādi ES līmenī, kas būs pašreizējā interneta apakšstruktūra un nešķērsos ES robežas; norāda, ka visi dati par datplūsmu maršrutēšanu un CDR ir jāapstrādā saskaņā ar ES tiesisko regulējumu;

109. aicina dalībvalstis, sadarbojoties ar *ENISA*, Eiropola Kibernoziedzības apkarošanas centru, datorapdraudējumu reaģēšanas vienībām un valstu datu aizsardzības iestādēm un kibernoziedzības novēršanas vienībām attīstīt drošības kultūru un rīkot izglītošanas un izpratnes veidošanas kampaņas, lai iedzīvotājiem radītu iespēju pieņemt apzinātus lēmumus par personas datu ievietošanu tiešsaistē un to labāku aizsardzību, tostarp, izmantojot šifrēšanu un drošu mākoņdatošanu, pilnībā izmantojot sabiedrību interesējošas informācijas platformu, kas paredzēta Universālā pakalpojuma direktīvā;

110. aicina Komisiju līdz 2014. gada decembrim iesniegt tiesību aktu projektus, kuros programmatūru un aparatūras ražotāji tiek mudināti uzlabot drošību un savos produktos izmantot integrētas privātuma aizsardzības un privātuma aizsardzības pēc noklusējuma iespējas, tostarp ieviešot atturošus stimulus par lielapjoma personas datu nepiemērotu un nesamērīgu vākšanu un paredzot arī ražotāju juridisko atbildību par zināmu neaizsargātu vietu nelabošanu, kļūdainiem vai nedrošiem produktiem vai par slepenu rezerves izeju instalēšanu, kas ļauj veikt neautorizētu piekļuvi datiem un to apstrādi; šajā saistībā aicina Komisiju novērtēt iespēju izveidot IT aparatūras sertifikācijas vai apstiprināšanas shēmu, tostarp ES līmeņa pārbaudes procedūras nolūkā nodrošināt šo izstrādājumu integritāti un drošību;

Uzticības atjaunošana

111. uzskata, ka papildus nepieciešamībai pēc tiesību aktu izmaiņām nodarītais kaitējums ir pierādījis, ka ASV ir jāatgūst savu ES partneru uzticība, jo galvenokārt ir apdraudētas ASV izlūkošanas aģentūru darbības;

112. norāda, ka radītā uzticības krīze ietekmē:

— ASV un ES sadarbības atmosfēru, jo dažas valstu izlūkošanas darbības var apdraudēt Savienības mērķu sasniegšanu;

— iedzīvotājus, kas saprot, ka viņus var izspiegot ne vien trešās valstis vai starptautiski uzņēmumi, bet arī savas valsts valdība;

— pamattiesību, demokrātijas un tiesiskuma ievērošanu, kā arī uzticēšanos demokrātiskajiem, tiesiskajiem un parlamentārajiem aizsardzības pasākumiem un uzraudzībai digitālā sabiedrībā;

ES un ASV starpā

113. atgādina svarīgo vēsturisko nozīmi ES dalībvalstu un ASV partnerībai, kuras pamatā ir ticība demokrātijai, tiesiskumam un pamattiesību ievērošanai;

114. uzskata, ka iedzīvotāju masveida novērošana un politisko vadītāju izspiegošana ASV ir radījusi nopietnu apdraudējumu ES un ASV attiecībām un negatīvi ietekmē uzticēšanos ASV organizācijām, kas darbojas ES; to vēl vairāk saasina tas, ka ASV tiesību aktos nav paredzēti tiesiskie un administratīvie līdzekļi, lai ES pilsoņi varētu iegūt tiesisko aizsardzību, it sevišķi, kad tiek veiktas novērošanas darbības izlūkošanas vajadzībām;

115. atzīst, ņemot vērā globālos uzdevumus, kas jārisina ES un ASV, ka ir jāturpina stiprināt transatlantiskā partnerība un ka ir būtiski svarīgi turpināt transatlantisko sadarbību terorisma apkarošanas jomā, balstoties uz jaunizveidotu uzticību, kuras pamatā ir patiesa un kopīga tiesiskuma ievērošana un atteikšanās no jebkādas pēc nejaušības principa veiktas masveida uzraudzības prakses; tāpēc pieprasa, lai ASV veiktu konkrētus pasākumus, kas atjaunotu uzticēšanos, un vēlreiz uzsver partnerības kopējās pamatvērtības;

116. pauž gatavību aktīvi iesaistīties dialogā ar ASV darījumpartneriem, lai pašreiz notiekošajās Amerikas sabiedrības un Kongresa debatēs par uzraudzības reformu un izlūkošanas uzraudzības pārskatīšanu tiktu risināti jautājumi par ES pilsoņu, iedzīvotāju un citu personu, ko aizsargā ES tiesību normas, tiesībām uz privāto dzīvi, vienlīdzīgām tiesībām uz informāciju un garantētu privātās dzīves aizsardzību ASV tiesās, ieskaitot tiesiskās aizsardzības līdzekļus, — piemēram, pārskatot Privātās dzīves aktu un Elektronisko sakaru privātuma aktu un ratificējot Starptautiskā pakta par pilsoniskajām un politiskajām tiesībām (*ICCPR*) Pirmo Fakultatīvo protokolu, tā lai likvidētu pašreizējo diskrimināciju;

117. pieprasa veikt vajadzīgās reformas un sniegt Eiropas iedzīvotājiem efektīvas garantijas, lai nodrošinātu to, ka novērošana un datu apstrāde ārvalstu izlūkošanas vajadzībām ir samērīga un tiek ierobežota ar precīzi izstrādātiem noteikumiem un ir saistīta ar pamatotām aizdomām par terorisma darbībām vai ar tās iespējamiem cēloņiem; uzsver, ka šim mērķim ir vajadzīga pārredzama juridiskā uzraudzība;

118. uzskata, ka no mūsu Amerikas partneriem ir vajadzīgs skaidrs politisks vēstījums, kas pierādītu, ka ASV nošķir sabiedrotos un pretiniekus;

119. mudina ES Komisiju un ASV administrāciju saistībā ar pašreizējām sarunām par ES un ASV jumta līgumu par datu pārsūtīšanu tiesībaizsardzības vajadzībām risināt jautājumu par ES pilsoņu tiesībām uz informāciju un tiesisko aizsardzību un, pildot ES un ASV tieslietu ministru sanāksmē 2013. gada 18. novembrī pausto apņemšanos, pabeigt šīs sarunas līdz 2014. gada vasarai;

120. mudina ASV pievienoties Eiropadomes Konvencijai par personu aizsardzību attiecībā uz personas datu automātisko apstrādi (108. konvencija), tāpat kā tās pievienojās 2001. gada Konvencijai par kibernoziegumiem, tādējādi stiprinot transatlantisko sabiedroto kopējo juridisko pamatu;

121. aicina ES iestādes izpētīt iespējas izveidot ASV rīcības kodeksu, kas garantētu, ka ASV neizspiego ES iestādes un ēkas;

Eiropas Savienībā

122. uzskata arī, ka uzticēšanos, tostarp uzticēšanos dalībvalstu starpā un iedzīvotāju un viņu dalībvalstu varas iestāžu starpā, ir mazinājusi ES dalībvalstu iesaistīšanās un darbības; uzskata, ka zaudēto uzticēšanos spēs atjaunot tikai pilnīgi skaidri novērošanas mērķi un līdzekļi, sabiedriskā apspriešana un — noteikti — tiesību aktu pārskatīšana un darbības, kas paredzētas masveida novērošanas darbību izbeigšanai un tiesiskās un parlamentārās uzraudzības sistēmas stiprināšanai; atgādina, ar kādām grūtībām saistīta visaptverošas ES drošības politikas izstrādāšana, notiekot masveida izlūkošanas darbībām, un uzsver, ka ES princips par godīgu sadarbību pieprasa, lai dalībvalstis atturētos no izlūkdienestu darbību veikšanas citu dalībvalstu teritorijā;

123. norāda, ka dažas ES dalībvalstis ir izveidojušas divpusējus sakarus ar ASV varas iestādēm saistībā ar iespējamiem spiegošanas gadījumiem un ka dažas valstis (Apvienotā Karaliste) ir noslēgušas vai plāno noslēgt (Vācija, Francija) tā dēvētos "spiegošanas novēršanas nolīgumus"; uzsver, ka šīm dalībvalstīm pilnībā ir jāievēro ES kopējās intereses un tiesiskais regulējums; uzskata šādus divpusējus nolīgumus par neproduktīviem un neatbilstošiem, jo šī problēma ir jārisina no Eiropas aspekta; aicina Padomi informēt Parlamentu par dalībvalstu sarunām par ES līmeņa savstarpējas spiegošanas novēršanas nolīgumu;

124. uzskata, ka šādos nolīgumos nedrīkstētu pārkāpt Savienības līgumus, jo īpaši lojālas sadarbības principu (saskaņā ar LES 4. panta 3. punktu), vai kopumā vājināt ES politikas virzienus — iekšējo tirgu, godīgu konkurenci, industriālo un sociālo attīstību; nolemj pārskatīt visus šādus nolīgumus, lai novērtētu to saderību ar Eiropas tiesību aktiem, un saglabā tiesības ierosināt Līgumā paredzētās procedūras, ja tiks pierādīts, ka šādi nolīgumi ir pretrunā Savienības kohēzijai vai tās pamatprincipiem;

125. aicina dalībvalstis veltīt visas pūles, lai nodrošinātu labāku sadarbību nolūkā nodrošināt garantijas pret spiegošanu, sadarbojoties ar attiecīgajām Es struktūrām un aģentūrām, lai aizsargātu ES pilsoņus un iestādes, Eiropas uzņēmumus, ES rūpniecību un visas IT infrastruktūras un tīklus, kā arī Eiropas pētniecību; uzskata, ka priekšnoteikums efektīvai informācijas apmaiņai ir aktīva ES ieinteresēto personu iesaistīšanās; norāda, ka draudi drošībai ir kļuvuši starptautiskāki, izkliedētāki un kompleksāki, tādējādi nepieciešama labāka Eiropas sadarbība; uzskata, ka šai tendencei vajadzētu gūt labāku atspoguļojumu Līgumos, un tādēļ aicina pārskatīt Līgumus, lai pastiprinātu prasību pēc nopietnas dalībvalstu un Savienības sadarbības attiecībā uz mērķi panākt drošības telpas izveidošanu un novērst Savienībā savstarpēju dalībvalstu izlūkošanu;

126. uzskata, ka visās attiecīgajās ES iestādēs un ES delegācijās obligāti ir nepieciešamas pret noklausīšanos drošas sakaru struktūras (e-pasts un telesakari, tostarp fiksētās tālruņa līnijas un mobilie tālruņi) un pret noklausīšanos drošas sanāksmju telpas; tāpēc aicina izveidot šifrētu ES iekšējo e-pasta sistēmu;

127. aicina Padomi un Komisiju bez tālākas vilcināšanās piekrist priekšlikumam, ko Eiropas Parlaments pieņēma 2012. gada 23. maijā, par Eiropas Parlamenta regulu par sīki izstrādātiem noteikumiem, kas reglamentē Eiropas Parlamenta izmeklēšanas tiesību īstenošanu, un ar kuru aizstāj Eiropas Parlamenta, Padomes un Komisijas Lēmumu (95/167/EK, Euratom, EOTK), priekšlikuma iesniegšanu balstot uz LESD 226. pantu; aicina pārskatīt Līgumu, lai paplašinātu šīs izmeklēšanas pilnvaras tā, lai bez ierobežojumiem un izņēmumiem aptvertu visas Savienības kompetences vai darbības jomas un iekļautu iespēju veikt nopratināšanu pēc zvēresta došanas;

Starptautiskajā mērogā

128. aicina Komisiju vēlākais 2015. gada janvārī piedāvāt ES stratēģiju interneta demokrātiskas pārvaldības jomā;

129. aicina dalībvalstis pildīt 35. starptautiskajā datu aizsardzības un privātuma komisāru konferencē pausto aicinājumu "atbalstīt Starptautiskā pakta par pilsoniskajām un politiskajām tiesībām (*ICCPR*) 17. panta papildu protokola pieņemšanu, kas būtu pamatots ar standartiem, kuri izstrādāti un apstiprināti starptautiskajā konferencē, un noteikumiem Pakta 16. piezīmē, ko ierosinājusi Cilvēktiesību komiteja, lai saskaņā ar tiesiskuma principu izstrādātu globāli piemērojamus standartus datu aizsardzības un privātuma aizsardzības jomā"; aicina dalībvalstis, pildot iepriekš minēto aicinājumu, atbalstīt tādas starptautiskas ANO aģentūras izveidi, kas būtu atbildīga jo īpaši par uzraudzības instrumentu parādīšanās uzraudzību un par to izmantošanas regulēšanu un izmeklēšanu; prasa Augstajai pārstāvei/Komisijas priekšsēdētāja vietniecei un Eiropas Ārējās Darbības dienestam uzņemties iniciatīvu;

130. aicina dalībvalstis Apvienoto Nāciju Organizācijā izstrādāt saskaņotu un stingru stratēģiju, jo īpaši atbalstot rezolūciju par tiesībām uz privāto dzīvi digitālajā laikmetā, ko ierosināja Brazīlija un Vācija un ko 2013. gada 27. novembrī pieņēma ANO ģenerālās asamblejas trešajā komitejā (Cilvēktiesību komiteja), kā arī īstenojot turpmāku rīcību, lai aizsargātu privātuma un datu aizsardzības pamattiesības un stiprinātu tās starptautiskā līmenī, vienlaikus novēršot jebkādu valsts kontroles veicināšanu vai cenzūru vai interneta sadrumstalošanu, tostarp — iniciatīvu attiecībā uz starptautisku paktu, kas aizliedz masveida novērošanas darbības, un aģentūru tā pārraudzīšanai;

Prioritāšu plāns — „Eiropas digitālā personas neaizskaramība – pamattiesību aizsardzība digitālajā laikmetā

131. nolemj iesniegt ES pilsoņiem, iestādēm un dalībvalstīm minētos ieteikumus kā prioritāšu plānu nākamajam likumdošanas ciklam; aicina Komisiju un šajā rezolūcijā minētās pārējās ES iestādes, struktūras, birojus un aģentūras saskaņā ar LESD 265. pantu rīkoties, ievērojot šajā rezolūcijā ietvertos ieteikumus un aicinājumus;

132. nolemj sākt plānu "Eiropas digitālā personas neaizskaramība – pamattiesību aizsardzība digitālajā laikmetā" ar šādām 8 darbībām, kuru īstenošanu tas pārraudzīs:

— Darbība Nr. 1. Pieņemt datu aizsardzības tiesību aktu kopumu 2014. gadā.

— Darbība Nr. 2. Noslēgt ES un ASV "jumta nolīgumu", kas iedzīvotājiem garantēs pamattiesības uz privātumu un datu aizsardzību un ES pilsoņiem nodrošinās pienācīgus tiesiskās aizsardzības mehānismus, tostarp gadījumos, kad datu pārsūtīšana no ES uz ASV tiek veikta tiesībaizsardzības nolūkos.

— Darbība Nr. 3. Līdz pilnīgas pārskatīšanas pabeigšanai un pašreizējo nepilnību novēršanai apturēt droša patvēruma sistēmas darbību, nodrošinot, ka personas datu pārsūtīšanu komerciālos nolūkos no Savienības uz ASV drīkst veikt tikai atbilstīgi augstākajiem ES standartiem.

— Darbība Nr. 4. Apturēt *TFTP* nolīguma noslēgšanu līdz: i) sarunu pabeigšanai par "jumta nolīgumu"; ii) rūpīgas izmeklēšanas pabeigšanai, kas veikta, ņemot vērā ES analīzi, un līdz brīdim, kad pienācīgi būs novērstas visas bažas, ko Parlaments pauda savā 2013. gada 23. oktobra rezolūcijā.

— Darbība Nr. 5. Novērtēt visus tādus nolīgumus, mehānismus un informācijas apmaiņu ar trešām valstīm, kas ietver personas datus, nolūkā nodrošināt, ka uzraudzības pasākumu dēļ netiek pārkāptas tiesības uz privātumu un uz personas datu aizsardzību, un veikt nepieciešamās papilddarbības.

— Darbība Nr. 6. Aizsargāt tiesiskumu un ES pilsoņu pamattiesības (tostarp pret draudiem preses brīvībai), sabiedrības tiesības saņemt objektīvu informāciju un profesionālo konfidencialitāti (tostarp jurista un klienta attiecībās), kā arī nodrošināt ziņotāju aizsardzības uzlabošanu.

— Darbība Nr. 7. Izstrādāt ES stratēģiju lielākas IT neatkarības jomā ("jauna vienošanās digitālajā jomā", tostarp pietiekamu resursu piešķiršana valstu un ES līmenī), lai veicinātu IT nozares uzplaukumu un ļautu Eiropas uzņēmumiem izmantot ES privātuma konkurētspējas priekšrocības.

— Darbība Nr. 8. Panākt, ka ES kļūst par paraugu demokrātiskas un neitrālas interneta pārvaldības jomā;

133. aicina Es iestādes un dalībvalstis atbalstīt un veicināt "Eiropas digitālo personas neaizskaramību", kas aizsargā pamattiesības digitālajā laikmetā; apņemas kļūt par ES pilsoņu tiesību sargu saskaņā ar norādīto īstenošanas uzraudzības grafiku:

— 2014. gada aprīlis – 2015. gada marts: uzraudzības grupa, kuras pamatā ir LIBE komitejas izmeklēšanas grupa, kas uzraudzītu jebkādus jaunus atklājumus attiecībā uz izmeklēšanas pilnvarām un rūpīgi pārbaudītu šīs rezolūcijas īstenošanu;

— no 2014. gada jūnija: pastāvīgs datu pārsūtīšanas uzraudzības mehānisms un tiesiskās aizsardzības līdzekļi atbildīgajā komitejā;

— 2014. gada pavasaris: oficiāls aicinājums Eiropadomei iekļaut "Eiropas digitālo personas neaizskaramību — pamattiesību aizsardzību digitālajā laikmetā" pamatnostādnēs, kas jāpieņem saskaņā ar LESD 68. pantu;

— 2014. gada rudens: apņemšanās, ka "Eiropas digitālā personas neaizskaramība — pamattiesību aizsardzība digitālajā laikmetā" un saistītie ieteikumi kļūs par galveno kritēriju nākamās Komisijas apstiprināšanai;

— 2014: konference, kurā piedalītos augsta līmeņa Eiropas eksperti dažādās jomās, kas saistītas ar IT drošību (tostarp matemātiķi, kriptogrāfi un privātuma uzlabošanas tehnoloģiju speciālisti), lai nākamajā sasaukumā palīdzētu veicināt ES IT stratēģijas attīstību;

— 2014–2015: Eiropas Parlamenta un ASV kongresa uzticamības/datu/pilsoņtiesību grupas regulāras sanāksmes, iesaistoties arī citiem trešo valstu, tostarp Brazīlijas, parlamentiem, kas pauduši vēlmi sadarboties;

— 2014–2015: konference, kurā piedalītos Eiropas valstu parlamentu izlūkošanas uzraudzības iestādes;

o

o o

134. uzdod priekšsēdētājam nosūtīt šo rezolūciju Eiropadomei, Padomei, Komisijai, dalībvalstu parlamentiem un valdībām, valstu datu aizsardzības iestādēm, *EDPS*, *eu-LISA*, *ENISA*, Pamattiesību aģentūrai, 29. panta darba grupai, Eiropas Padomei, Amerikas Savienoto Valstu kongresam, ASV administrācijai, Brazīlijas Federatīvās Republikas prezidentam, valdībai un parlamentam un Apvienoto Nāciju Organizācijas ģenerālsekretāram;

135. uzdod Pilsoņu brīvību, tieslietu un iekšlietu komitejai iesniegt Parlamentam izskatīšanai šo jautājumu plenārsēdē gadu pēc šīs rezolūcijas pieņemšanas; uzskata, ka ir ļoti svarīgi novērtēt, cik lielā mērā ir ievēroti Parlamenta pieņemtie ieteikumi, un analizēt visus gadījumus, kad šādi ieteikumi nav ievēroti.