

USA Riikliku Julgeolekuagentuuri järelevalveprogramm, ELi liikmesriikide jälgimisasutused ning mõju ELi kodanike põhiõigustele

Euroopa Parlamendi 12. märtsi 2014. aasta resolutsioon USA Riikliku Julgeolekuagentuuri jälgimisprogrammi ja ELi liikmesriikide jälgimisasutuste ning nende mõju kohta ELi kodanike põhiõigustele ja Atlandi-ülesele koostööle justiits- ja siseküsimustes (2013/2188(INI))

Euroopa Parlament,

- võttes arvesse Euroopa Liidu lepingut (ELi leping), eriti selle artikleid 2, 3, 4, 5, 6, 7, 10, 11 ja 21,
- võttes arvesse Euroopa Liidu toimimise lepingut (ELi toimimise leping), eriti selle artikleid 15, 16 ja 218 ning V jaotist,
- võttes arvesse protokolli nr 36 üleminekusätete kohta ja selle artiklit 10 ning seda protokollit käsitlevat deklaratsiooni nr 50,
- võttes arvesse Euroopa Liidu põhiõiguste hartat, eelkõige selle artikleid 1, 3, 6, 7, 8, 10, 11, 20, 21, 42, 47, 48 ja 52,
- võttes arvesse Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni, eriti selle artikleid 6, 8, 9, 10 ja 13, ning selle protokolle,
- võttes arvesse inimõiguste ülddeklaratsiooni¹, eelkõige selle artikleid 7, 8, 10, 11, 12 ja 14,
- võttes arvesse kodaniku- ja poliitiliste õiguste rahvusvahelist pakti, eelkõige selle artikleid 14, 17, 18 ja 19,
- võttes arvesse Euroopa Nõukogu konventsiooni üksikisikute kaitse kohta isikuandmete automatiseeritud töötlemisel (ETS nr 108) ja selle konventsiooni 8. novembri 2001. aasta lisaprotokollit, milles käsitletakse järelevalveasutusi ja andmete liikumist üle piiri (ETS nr 181),
- võttes arvesse diplomaatiliste suhete Viini konventsiooni, eriti selle artikleid 24, 27 ja 40,
- võttes arvesse Euroopa Nõukogu küberkuritegevuse konventsiooni (ETS nr 185),
- võttes arvesse ÜRO eriraportööri 17. mail 2010 esitatud aruannet inimõiguste ja põhivabaduste edendamise ja kaitse kohta terrorismiga võitlemisel²,

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>

- võttes arvesse komisjoni teatist „Internet – põhimõtted ja juhtimine. Euroopa roll interneti tuleviku haldamise kujundamisel” (COM(2014)0072);
- võttes arvesse ÜRO eriraportööri 17. aprillil 2013 esitatud aruannet arvamus- ja sõnavabaduse edendamise ja kaitsmise kohta¹,
- võttes arvesse Euroopa Nõukogu ministrite komitee poolt 11. juulil 2002 vastu võetud suuniseid inimõiguste ning terrorismivastase võitluse kohta,
- võttes arvesse 1. oktoobri 2010. aasta Brüsseli deklaratsiooni, mis võeti vastu Euroopa Liidu liikmesriikide parlamentide luure- ja julgeolekuteenistuste järelevalvekomisjonide kuuendal konverentsil,
- võttes arvesse Euroopa Nõukogu Parlamentaarse Assamblee resolutsiooni nr 1954 (2013) riikide julgeoleku ja teabele juurdepääsu kohta,
- võttes arvesse Veneetsia komisjoni poolt 11. juunil 2007 vastu võetud raportit julgeolekuteenistuste demokraatliku järelevalve kohta² ning oodates suure tähelepanuga selle ajakohastamist 2014. aasta kevadeks,
- võttes arvesse Belgia, Madalmaade, Taani ja Norra luureteenistuste järelevalvekomisjonide liikmete tunnistusi,
- võttes arvesse Prantsusmaa³, Poola ja Ühendkuningriigi⁴ kohtutele ning Euroopa Inimõiguste Kohtule⁵ esitatud kohtuasju seoses massilise jälgimise süsteemidega,
- võttes arvesse nõukogu koostatud Euroopa Liidu lepingu artikli 34 kohast konventsiooni Euroopa Liidu liikmesriikide vahelise vastastikuse õigusabi kohta kriminaalasjades⁶ ja eelkõige selle III jaotist,
- võttes arvesse komisjoni 26. juuli 2000. aasta otsust 2000/520/EÜ piisava kaitse kohta, mis on ette nähtud programmi Safe Harbor põhimõtetega ja sellega seotud korduma kippuvate küsimustega, mille on välja andnud Ameerika Ühendriikide kaubandusministeerium,
- võttes arvesse komisjoni 13. veebruari 2002. aasta (SEC(2002)0196) ja 20. oktoobri 2004. aasta hindamisaruandeid programmi Safe Harbor põhimõtete rakendamise kohta (SEC(2004)1323),

1

http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

2

[http://www.venice.coe.int/webforms/documents/CDL-AD\(2007\)016.aspx](http://www.venice.coe.int/webforms/documents/CDL-AD(2007)016.aspx)

3

Rahvusvaheline Inimõiguste Föderatsioon (FIDH) ja La Ligue française pour la défense des droits de l’Homme et du Citoyen v. X (Prantsusmaa inimõiguste ja kodanike kaitse föderatsioon tundmatu vastu); Pariisi Tribunal de Grande Instance.

4

Privacy Internationali ja Liberty kohtuasjad nn Uurimisasutuste Tribunalis (Investigatory Powers Tribunal).

5

Big Brother Watch, Open Rights Group, English Pen ja Dr Constanze Kurz (hagi esitajad) artikli 34 kohane ühishagi Ühendkuningriigi (kostja) vastu.

6

EÜT C 197, 12.7.2000, lk 1.

- võttes arvesse komisjoni 27. novembri 2013. aasta teatist, mis käsitleb programmi Safe Harbor toimumist ELi kodanike ja ELis asutatud äriühingute seisukohast (COM(2013)0847), ja komisjoni 27. novembri 2013. aasta teatist usalduse taastamise kohta ELi ja Ameerika Ühendriikide vaheliste andmevoogude vastu (COM(2013)0846),
- võttes arvesse oma 5. juuli 2000. aasta resolutsiooni komisjoni otsuse eelnõu kohta piisava kaitse kohta, mis on ette nähtud programmi Safe Harbor põhimõtetega ja sellega seotud korduma kippuvate küsimustega, mille on välja andnud Ameerika Ühendriikide kaubandusministeerium¹, milles võeti seisukoht, et nimetatud süsteemi asjakohasust ei saa kinnitada, ning artikli 29 töörühma arvamusi ja konkreetsemalt selle 16. mai 2000. aasta arvamust 4/2000²,
- võttes arvesse USA ja ELi vahelisi lepinguid broneeringuinfo kasutamise ja edastamise kohta (PNR-leping), mis sõlmiti 2004., 2007.³ ja 2012.⁴ aastal,
- võttes arvesse USA ja ELi vahel sõlmitud broneeringuinfo kasutamist ja edastamist USA sisejulgeolekuministeeriumile käsitleva lepingu rakendamise ühist läbivaatamist⁵ ning selle põhjal koostatud komisjoni aruannet Euroopa Parlamendile ja nõukogule ühise läbivaatamise kohta (COM(2013)0844),
- võttes arvesse kohtujurist Cruz Villalóni arvamust, milles tehti järeldus, et direktiiv 2006/24/EÜ, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkuja tegevusega kaasnevate või nende töödeldud andmete säilitamist, on tervikuna vastuolus Euroopa Liidu põhiõiguste harta artikli 52 lõikega 1 ning selle artikkel 6 on vastuolus nimetatud harta artikliga 7 ja artikli 52 lõikega 1⁶,
- võttes arvesse nõukogu 13. juuli 2010. aasta otsust 2010/412/EL Euroopa Liidu ja Ameerika Ühendriikide vahelise lepingu (mis käsitleb finantstehinguid käsitlevate sõnumiandmete töötlemist ja edastamist Euroopa Liidust Ameerika Ühendriikidesse terroristide rahastamise jälgimise programmi raames) sõlmimise kohta⁷ ja sellele lisatud komisjoni ja nõukogu avaldusi,
- võttes arvesse Euroopa Liidu ja Ameerika Ühendriikide vahelist vastastikuse õigusabi osutamise lepingut⁸;
- võttes arvesse käimasolevaid läbirääkimisi ELi ja USA vahelise raamlepingu üle, milles käsitletakse kriminaalasjadega seotud politsei- ja õiguslase koostöö raames kriminaalkuritegude, sealhulgas terrorismi, ennetamise, uurimise, avastamise ja nende eest süüdistuse esitamise eesmärgil edastatavate ja töödeldavate isikuandmete kaitset (edaspidi „raamleping”),

¹ EÜT C 121, 24.4.2001, lk 152.

² <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp32en.pdf>

³ ELT L 204, 4.8.2007, lk 18.

⁴ ELT L 215, 11.8.2012, lk 5.

⁵ SEC(2013)0630, 27.11.2013.

⁶ Kohtujuristi Cruz Villalóni arvamus, 12. detsember 2013, kohtuasi C-293/12.

⁷ ELT L 195, 27.7.2010, lk 3.

⁸ ELT L 181, 19.7.2003, lk 34.

- võttes arvesse nõukogu 22. novembri 1996. aasta määrust (EÜ) nr 2271/96, mis käsitleb kaitset kolmanda riigi vastuvõetud õigusaktide eksterritoriaalse kohaldamise mõju ja nendel õigusaktidel põhinevate või neist tulenevate meetmete eest¹,
- võttes arvesse Brasiilia Liitvabariigi presidendi avaldust 24. septembril 2013 toimunud ÜRO Peaassamblee 68. istungjärgu avamisel ning Brasiilia Senatis moodustatud spionaaži uurimisega tegeleva parlamendikomisjoni tehtud tööd,
- võttes arvesse USA presidendi George W. Bushi poolt 26. oktoobril 2001 allkirjastatud PATRIOT Act'i,
- võttes arvesse 1978. aasta USA vastuluure seadust (Foreign Intelligence Surveillance Act, FISA) ja 2008. aasta FISA muutmise seadust,
- võttes arvesse USA presidendi 1981. aasta korraldust nr 12333, mida muudeti 2008. aastal,
- võttes arvesse USA presidendi Barack Obama 17. jaanuaril 2014 välja antud poliitikasuunist (Presidential Policy Directive PPD-28) teabesignaalide kohta,
- võttes arvesse USA Kongressis praegu menetletavaid õigusaktide ettepanekuid, sealhulgas andmekogumist käsitlevat US Freedom Act'i eelnõu, luuretegevuse järelevalve eelnõu, luuretegevuse reformi eelnõu ja teisi ettepanekuid,
- võttes arvesse eraelu puutumatuse ja kodanikuvabaduste järelevalve komitee, USA Riikliku Julgeolekunõukogu ning presidendi luure- ja kommunikatsioonitehnoloogia järelevalverühma ülevaateid, eelkõige viimati nimetatud 12. detsembri 2013. aasta aruannet „Vabadus ja julgeolek muutuvmas maailmas”,
- võttes arvesse Ameerika Ühendriikide Columbia ringkonna ringkonnakohtu 16. detsembri 2013. aasta otsust tsiviilhagi nr 13-0851 kohta (*Klayman et al. vs Obama et al.*) ja Ameerika Ühendriikide New Yorgi lõunapiirkonna ringkonnakohtu 11. juuni 2013. aasta otsust tsiviilhagi nr 13-3994 kohta (*ACLU et al. vs James R. Clapper et al.*),
- võttes arvesse 27. novembri 2013. aasta aruannet ELi ja USA andmekaitse ajutise töörühma ELi kaasjuhtide järeltule kohta²,
- võttes arvesse oma 5. septembri 2001. aasta³ ja 7. novembri 2002. aasta⁴ resolutsioone era- ja äriside pealtkuulamise üleilmse süsteemi (pealtkuulamissüsteemi Echelon) olemasolu kohta,
- võttes arvesse oma 21. mai 2013. aasta resolutsiooni ELi harta ja ühesuguste tingimuste kohta meediavabaduse tagamiseks kõikjal ELis⁵,
- võttes arvesse oma 4. juuli 2013. aasta resolutsiooni USA Riikliku Julgeolekuagentuuri jälgimisprogrammi ning ELi liikmesriikide jälgimisasutuste ja nende mõju kohta ELi

¹ EÜT L 309, 29.11.1996, lk 1.

² Nõukogu dokument 16987/2013.

³ EÜT C 72 E, 21.3.2002, lk 221.

⁴ ELT C 16 E, 22.1.2004, lk 88.

⁵ Vastuvõetud tekstid, P7_TA(2013)0203.

kodanike eraelu puutumatusele¹, milles tehti kodanikuvabaduste, justiits- ja siseasjade komisjonile ülesandeks viia läbi põhjalik uurimine sellel teemal,

- võttes arvesse töödokumenti nr 1 USA ja ELi jälgimisprogrammide ja nende mõju kohta ELi kodanike põhiõigustele,
- võttes arvesse töödokumenti nr 3 ELi ja USA jälgimistegevuse ja ELi andmekaitsealaste õigusaktide vahekorra kohta,
- võttes arvesse töödokumenti nr 4 USA jälgimistegevuse kohta seoses ELi andmetega ja selle võimalike õiguslike tagajärgede kohta Atlandi-ülestele kokkulepetele ja koostööle,
- võttes arvesse töödokumenti nr 5 liikmesriikide luureteenistuste ja ELi luureorganite demokraatliku järelevalve kohta,
- võttes arvesse väliskomisjoni töödokumenti ELi kodanike massilise elektroonilise jälgimise välispoliitiliste aspektide kohta;
- võttes arvesse oma 23. oktoobri 2013. aasta resolutsiooni organiseeritud kuritegevuse, korrupsiooni ja rahapesu ning soovitude kohta meetmete võtmiseks ja algatuste tegemiseks²,
- võttes arvesse oma 23. oktoobri 2013. aasta resolutsiooni terroristide rahastamise jälgimisprogrammi käsitleva lepingu peatamise kohta USA Riikliku Julgeolekuagentuuri jälgimistegevuse tõttu³,
- võttes arvesse oma 10. detsembri 2013. aasta resolutsiooni pilvandmetöötluse võimaluste kasutamise kohta Euroopas⁴,
- võttes arvesse institutsioonidevahelist kokkulepet Euroopa Parlamendi ja nõukogu vahel, mis käsitleb nõukogu valduses oleva salastatud teabe edastamist Euroopa Parlamendile ja selle töötlemist Euroopa Parlamendi poolt seoses teemadega, mis ei kuulu ühise välis- ja julgeolekupoliitika valdkonda⁵,
- võttes arvesse kodukorra VIII lisa,
- võttes arvesse kodukorra artiklit 48,
- võttes arvesse kodanikuvabaduste, justiits- ja siseasjade komisjoni raportit (A7-0139/2014),

Massijälgimise mõju

- A. arvestades, et andmekaitse ja eraelu puutumatus on põhiõigused; arvestades, et seetõttu tuleb julgeolekumeetmeid, sealhulgas terrorismivastaseid meetmeid võttes järgida õigusriigi põhimõtteid ja põhiõigustega seotud kohustusi, sealhulgas eraelu puutumatust

¹ Vastuvõetud tekstid, P7_TA(2013)0322.

² Vastuvõetud tekstid, P7_TA(2013)0444.

³ Vastuvõetud tekstid, P7_TA(2013)0449.

⁴ Vastuvõetud tekstid, P7_TA(2013)0535.

⁵ ELT C 353 E, 3.12.2013, lk 156.

ja andmekaitset;

- B. arvestades, et teabevood ja andmed, millel on praegu domineeriv roll igapäevaelus ja mis on osa iga isiku puutumatuses, peavad olema sissetungi eest samamoodi kaitstud nagu kodud;
- C. arvestades, et Euroopa ja Ameerika Ühendriikide vahelised sidemed põhinevad demokraatia, õigusriigi, vabaduse, õigluse ja solidaarsuse vaimul ja põhimõtetel;
- D. arvestades, et USA ja Euroopa Liidu ning selle liikmesriikide koostöö terrorismivastase võitluse valdkonnas jääb mõlema partneri julgeoleku ja ohutuse seisukohast väga tähtsaks;
- E. arvestades, et vastastikusel usaldusel ja mõistmisel on Atlandi-üleses dialoogis ja partnerluses keskne koht;
- F. arvestades, et pärast 2001. aasta 11. septembrit sai terrorismivastasest võitlusest enamiku valitsuste üks peamisi eesmärke; arvestades, et USA Riikliku Julgeolekuagentuuri (NSA) endise töötaja Edward Snowdeni lekitatud dokumentidel põhinevad paljastused sundisid poliitilisi liidreid tegelema luureasutuste jälgimistegevuse järelevalve ja kontrollimise probleemidega ning hindama nende tegevuse mõju põhiõigustele ja õigusriigi põhimõtetele demokraatlikus ühiskonnas;
- G. arvestades, et alates 2013. aasta juunist avalikkuse ette jõudnud informatsioon on põhjustanud ELis palju küsimusi seoses alljärgnevaga:
- USAs ja ELi liikmesriikides paljastatud jälgimissüsteemide ulatus;
 - ELi õigusnormide, põhiõiguste ja andmekaitseenormide rikkumine;
 - ELi ja USA kui Atlandi-üleste partnerite vahelise usalduse määr;
 - teatavate ELi liikmesriikide koostöö USA jälgimisprogrammide või meedia poolt paljastatud samaväärsete riiklike programmidega ja nendes osalemise määr;
 - USA poliitiliste organite ja teatavate ELi liikmesriikide oma luureringkondade üle teostatava kontrolli ja tõhusa järelevalve puudumine;
 - võimalus, et neid massilise jälgimise toiminguid kasutatakse muudel põhjustel kui üksnes riikliku julgeoleku ja terrorismivastase võitluse eesmärgil, näiteks majandus- ja tööstusspionaažiks või poliitilistel põhjustel portreeterimiseks;
 - ajakirjandusvabaduse piiramine ja konfidentsiaalsuskohustusega kutsealade esindajatega, sealhulgas advokaatide ja arstidega suhtlemise kahjustamine;
 - luureasutuste ja erasektori IT- ja telekommunikatsiooniettevõtete roll ja osalemise määr;
 - üha hägusamad piirid õiguskaitse ja luuretegevuse vahel, mille tõttu koheldakse iga kodanikku võimaliku kahtlusalusena ja jälgitakse teda;

- eraelu puutumatust ähvardavad ohud digitaalajastul ning massilise jälgimise mõju kodanikele ja ühiskondadele;
- H. arvestades, et enneolematu ulatusega spionaaži paljastamine nõuab USA ametivõimudelt, Euroopa institutsioonidelt ning liikmesriikide valitsustelt, parlamentidelt ja õigusasutustelt põhjalikku uurimist;
- I. arvestades, et USA ametivõimud on eitanud osa paljastatud teabe õigsust, kuid ei ole vaidlustanud valdavalt enamikku sellest; arvestades, et avalik arutelu on USAs ja teatavates ELi liikmesriikides paisunud väga laiaulatuslikuks; arvestades, et ELi valitsused ja parlamendid on liiga sageli vaikinud ega ole alustanud asjakohaseid uurimisi;
- J. arvestades, et president Obama teavitas hiljuti NSA ja selle jälgimisprogrammide reformist;
- K. arvestades, et võrreldes nii ELi institutsioonide kui ka teatavate ELi liikmesriikide võetud meetmetega on Euroopa Parlament võtnud väga tõsiselt oma kohustust kontrollida paljastusi ELi kodanike valimatu massilise jälgimise tavade kohta ja tegi oma 4. juuli 2013. aasta resolutsiooniga USA Riikliku Julgeolekuagentuuri jälgimisprogrammi ning ELi liikmesriikide jälgimisasutuste ja nende mõju kohta ELi kodanike eraelu puutumatusele kodanikuvabaduste, justiits- ja siseasjade komisjonile ülesandeks viia selles küsimuses läbi põhjalik uurimine;
- L. arvestades, et Euroopa institutsioonid on kohustatud tagama, et ELi õigust rakendatakse täielikult Euroopa kodanike hüvanguks ning et kolmandate riikide standardite või meetmete eksterritoriaalse mõju kergekäeline heakskiitmine ei kahjustaks ELi aluslepingute õigusjõudu;

Luurereformi arengusuunad USAs

- M. arvestades, et Columbia ringkonna ringkonnakohus otsustas oma 16. detsembri 2013. aasta otsusega, et metaandmete massiline kogumine NSA poolt on USA põhiseaduse neljanda muudatuse rikkumine¹; arvestades, et New Yorgi lõunapiirkonna ringkonnakohus aga otsustas oma 27. detsembri 2013. aasta otsuses, et kõnealune kogumine on seaduslik;
- N. arvestades, et Michigani idapiirkonna ringkonnakohtu otsuses on öeldud, et neljandas muudatuses sätestatakse, et kõik läbiotsimised peavad olema põhjendatud, mis tahes läbiotsimiseks peab olema läbiotsimismäärus, nimetatud määrus peab põhinema eelnevalt olemasoleval tõenäolisel põhjusel ja need peavad olema välja antud konkreetsete isikute, koha ja asjade kohta ning täidesaatvate korrakaitseametnike ja kodanike vahelülis peab olema erapooletu kohtunik²;
- O. arvestades, et presidendi luure- ja kommunikatsioonitehnoloogia järelevalverühm esitas oma 12. detsembri 2013. aasta aruandes USA presidendile 46 soovitusi; arvestades, et need soovitused rõhutavad vajadust kaitsta samaaegselt riiklikku julgeolekut ning eraelu puutumatust ja kodanikuvabadusi; arvestades, et sellega seoses kutsutakse USA valitsust

¹ Klayman *et al.* vs Obama *et al.*, tsiviilhagi nr 13-0851, 16. detsember 2013.

² ACLU vs NSA, nr 06-CV-10204, 17. august 2006.

üles lõpetama võimalikult kiiresti USA kodanike telefonikõnede väljavõtete massiline kogumine USA PATRIOT Act'i artikli 215 kohaselt, põhjalikult läbi vaatama NSA ja USA luurealase õigusraamistiku, et tagada õigus eraelu puutumatusele, lõpetama tasulise tarkvara saboteerimise või haavatavaks tegemise katsed (tagauksed ja pahavara), suurendama krüpteerimise kasutamist, eelkõige andmeedastuse korral, ja mitte töötama vastu andmekrüpteerimise standardite loomiseks tehtavatele jõupingutustele, nimetama ametisse avalikku huvi kaitsva advokaadi, kes kaitseks eraelu puutumatust ja kodanikuvabadusi välisluure järelevalvekohtus (Foreign Intelligence Surveillance Court), andma eraelu puutumatuse ja kodanikuvabaduste järelevalve komiteele õiguse teostada järelevalvet luureringkondade tegevuse üle mitte üksnes terrorismivastastel, vaid ka välisluure eesmärkidel, ning võtma vastu õigusrikkumistest teatajate kaebusi, kasutama vastastikuse õigusabi lepinguid elektroonilise teabevahetuse andmete saamiseks, ning mitte kasutama jälgimist tööstus- või ärisaladuste varastamise eesmärgil;

- P. arvestades, et vastavalt avalikule märgukirjale, mille saatsid president Obamale NSA endised tippjuhid ja luuretöötajate organisatsioon Veteran Intelligence Professionals for Sanity (VIPS) 7. jaanuaril 2014. aastal¹, ei suurenda andmete massiline kogumine võimet tulevasi terrorirünnakuid ennetada; arvestades, et märgukirja autorid rõhutavad, et NSA läbi viidud massilise jälgimise tulemusena ei ennetatud ühegi rünnakut ja miljardeid dollareid on kulutatud programmidele, mis on vähem tõhusad ja palju sekkuvamad kodanike eraellu kui asutusesisene tehnoloogia THINTHREAD, mis töötati välja 2001. aastal;
- Q. arvestades, et seoses luuretegevusega muude kui USA kodanike suhtes FISA artikli 702 kohaselt märgitakse USA presidendile esitatud soovitusel, et põhiküsimuseks on inimõiguste ülddeklaratsiooni artiklis 12 ning kodaniku- ja poliitiliste õiguste rahvusvahelise pakti artiklis 17 sätestatud õigus eraelu puutumatusele ja inimväärikusele; arvestades, et dokumendis ei soovitata siiski anda teiste riikide kodanikele samu õigusi ja kaitset nagu USA kodanikele;
- R. arvestades, et presidendi 17. jaanuari 2014. aasta poliitikasuunises teabesignaali kohta ja sellega seoses peetud kõnes märkis president Barack Obama, et massiline elektrooniline jälgimine on USA-le vajalik, et kaitsta oma riigi julgeolekut, kodanikke ning USA liitlas- ja partnerriikide kodanikke, samuti selleks, et edendada oma välispoliitilisi huve; arvestades, et poliitikasuunises on esitatud teatavad põhimõtted, mis puudutavad signaalteabe kogumist, kasutamist ja jagamist, ning sellega laiendatakse teiste riikide kodanikele teatavaid kaitsemeetmeid, millega neile nähakse ette osaliselt samaväärne kohtlemine nagu USA kodanikele, sealhulgas kaitsemeetmeid kõikide isikute isikuandmete suhtes sõltumata nende kodakondsusest või elukohast; arvestades, et president Obama ei nõudnud ühegi konkreetse ettepaneku tegemist, eriti seoses massilise jälgimistegevuse keelustamisega ning teiste riikide kodanikele haldus- ja õiguskaitsevahendite kehtestamisega;

Õigusraamistik

Põhiõigused

- S. arvestades, et aruandes ELi ja USA andmekaitse ajutise töörühma ELi kaasjuhtide

¹ <http://consortiumnews.com/2014/01/07/nsa-insiders-reveal-what-went-wrong>.

järelduste kohta antakse ülevaade õigusliku olukorra kohta USAs, kuid selles ei tuvastata USA jälgimisprogrammidega seotud asjaolusid; arvestades, et mitte mingit teavet ei ole avaldatud nn teise suundumuse tööühma kohta, mille raames arutavad liikmesriigid kahepoolset USA ametivõimudega riikliku julgeolekuga seotud teemasid;

- T. arvestades, et Euroopa Liidu põhiõiguste hartas ning Euroopa inimõiguste ja põhivabaduse kaitse konventsioonis sätestatud põhiõigused, eelkõige sõna-, ajakirjandus-, mõtte-, südametunnistuse-, usu- ja ühinemisvabadus, õigus eraelule, andmekaitsele ja tõhusale õiguskaitsevahendile, süütuse presumpatsioon ning õigus õiglasele kohtupidamisele ja mittediskrimineerimisele on demokraatia nurgakivid; arvestades, et inimeste massiline jälgimine ei sobi nimetatud põhimõtetega kokku;
- U. arvestades, et kõikides liikmesriikides kaitseb seadus advokaadi ja kliendi vahel konfidentsiaalselt edastatud teavet avalikustamise eest ning seda põhimõtet on tunnustanud ka Euroopa Kohus¹;
- V. arvestades, et oma 23. oktoobri 2013. aasta resolutsioonis organiseeritud kuritegevuse, korruptsiooni ja rahapesu kohta kutsus parlament komisjoni esitama seadusandlikku ettepanekut, millega kehtestatakse tõhus ja terviklik rikkumisest teatajate kaitse Euroopa programm, et kaitsta ELi finantshuve, ja lisaks sellele uurima küsimust, kas edaspidi võiks sarnases õigusaktis käsitleda ka teisi liidu pädevusvaldkondi;

Liidu pädevus julgeoleku valdkonnas

- W. arvestades, et ELi toimimise lepingu artikli 67 lõike 3 kohaselt püüab EL tagada kõrge turvalisuse taseme; arvestades, et aluslepingu sätetest (eelkõige ELi lepingu artikli 4 lõikest 2 ja ELi toimimise lepingu artiklitest 72 ja 73) võib mõista, et ELil on teatavad pädevused liidu ühise julgeolekuga seotud küsimustes; arvestades, et ELil on sisejulgeoleku küsimustes oma pädevus (ELi toimimise lepingu artikli 4 lõike 2 punkt j) ja ta on tegutsenud selle pädevuse raames ning teinud otsuseid mitme õigusvahendi kohta ja sõlminud rahvusvahelisi lepinguid (PNR- ja TFTP-leping), mille eesmärk on võidelda raskete kuritegude ja terrorismi vastu, ning kehtestanud sisejulgeoleku strateegia ja asutanud selles valdkonnas tegutsevad ametid;
- X. arvestades, et ELi toimimise lepingus on sätestatud järgmist: „Liikmesriigid võivad luua omavahel ja omal vastutusel riigi julgeoleku kaitsmise eest vastutavate haldusteenistuste vahel koostöö- ja koordinatsioonivorme, mida nad peavad asjakohaseks.” (ELi toimimise lepingu artikkel 73);
- Y. arvestades, et Euroopa Liidu toimimise lepingu artiklis 276 on sätestatud: „Vabadusel, turvalisusel ja õigusel rajanevat ala käsitleva kolmanda osa V jaotise 4. ja 5. peatüki sätetega seotud volituste teostamisel ei ole Euroopa Liidu Kohus pädev kontrollima liikmesriigi politsei või muu õiguskaitseorgani korraldatud operatsioonide põhjendatust või proportsionaalsust ega seda, kuidas liikmesriigid teostavad oma vastutust avaliku korra ja sisejulgeoleku tagamisel.”;
- Z. arvestades, et riiklik julgeolek, sisejulgeolek, ELi sisejulgeolek ja rahvusvaheline julgeolek on osaliselt kattuvad mõisted; arvestades, et rahvusvaheliste lepingute õiguse

¹ 18. mai 1982. aasta kohtuotsus kohtuasjas C-155/79: AM & S Europe Limited vs. Euroopa Ühenduste Komisjon.

Viini konventsioon, ELi liikmesriikide vahelise lojaalse koostöö põhimõte ja inimõigusi käsitleva õiguse kõikide erandite kitsa tõlgendamise põhimõte osutavad riikliku julgeoleku mõiste kitsendavale tõlgendamisele ning see nõuab, et liikmesriigid hoiduksid ELi pädevustesse sekkumast;

- AA. arvestades, et Euroopa aluslepingute kohaselt on Euroopa Komisjon aluslepingute kaitsja ja seepärast on komisjoni seadusjärgne kohustus uurida kõiki ELi õiguse võimaliku rikkumise juhtumeid;
- AB. arvestades, et kooskõlas ELi lepingu artikliga 6, milles osutatakse ELi põhiõiguste hartale ning Euroopa inimõiguste ja põhivabaduste kaitse konventsioonile, peavad riikliku julgeoleku valdkonnas tegutsevad liikmesriikide asutused ja isegi erasektori osalejad austama nimetatud konventsioonis sätestatud õigusi, olenemata sellest, kas tegemist on nende enda riigi või mõne teise riigi kodanikega;

Eksterritoriaalsus

- AC. arvestades, et kolmanda riigi poolt oma seaduste, määruste ning muude õigus- ja rakendusaktide eksterritoriaalne kohaldamine olukordades, mis kuuluvad ELi või selle liikmesriikide jurisdiktsiooni alla, võivad mõjutada kehtivat õiguskorda ja õigusriigi põhimõtet või isegi rikkuda rahvusvahelist või ELi õigust, sealhulgas füüsiliste ja juriidiliste isikute õigusi, võttes arvesse sellise kohaldamise ulatust ja väidetavat või tegelikku eesmärki; arvestades, et nimetatud asjaoludel on vaja võtta liidu tasemel meetmeid, millega tagatakse, et ELis järgitakse ELi lepingu artiklis 2, põhiõiguste hartas ning Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis sätestatud põhiõiguste, demokraatia ja õigusriigi põhimõtetega seotud ELi väärtusi, samuti neid aluspõhimõtteid kohaldavates teistes õigusaktides sätestatud füüsiliste ja juriidiliste õigusi, näiteks kõrvaldades, neutraliseerides, tõkestades või muul viisil tõrjudes kõnealuste kolmandate riikide õigusaktide mõju;

Andmete rahvusvaheline edastamine

- AD. arvestades, et kui ELi institutsioonid, organid, ametid või asutused või liikmesriigid edastavad USA-le isikuandmeid õiguskaitse eesmärgil ning seejuures ei võeta piisavaid tagatis- ja kaitsemeetmeid, et tagada ELi kodanike põhiõiguste (eelkõige õigus eraelu puutumatusle ja isikuandmete kaitsele) austamine, on asjaomane ELi institutsioon, organ, amet või asutus või asjaomane liikmesriik ELi toimimise lepingu artikli 340 või Euroopa Liidu Kohtu väljakujunenud kohtupraktika¹ kohaselt vastutav ELi õiguse rikkumise eest, mis hõlmab mis tahes ELi hartas sätestatud põhiõiguste rikkumist;
- AE. arvestades, et andmeedastus ei ole geograafiliselt piiratud, eriti suureneva globaliseerumise ja ülemaailmse teabevahetuse tingimustes, ning ELi seadusandja ees on uued ülesanded seoses isikuandmete ja teabevahetuse kaitsmisega; arvestades, et seepärast on äärmiselt oluline tugevdada ühiste standardite õigusraamistikke;
- AF. arvestades, et isikuandmete massiline kogumine ärieesmärkidel ja terrorismivastases ning rahvusvahelise raske kuritegevuse vastases võitluses seab ohtu ELi kodanike isikuandmed ja eraelu puutumatuslega seotud õigused;

¹ Vt eelkõige 19. novembri 1991. aasta kohtuotsust liidetud kohtuasjades C-6/90 ja C-9/90: Francovich ja teised vs. Itaalia.

Andmete edastamine USA-le programmi Safe Harbor alusel

- AG. arvestades, et USA andmekaitset käsitlev õigusraamistik ei taga ELi kodanikele piisaval tasemel kaitset;
- AH. arvestades, et selleks, et ELi andmekontrollijatel oleks võimalik edastada isikuandmeid mõnele USA üksusele, on komisjon oma otsuses 2000/520/EÜ tunnistanud programmi Safe Harbor põhimõtetega ja sellega seotud korduma kippuvate küsimustega, mille on välja andnud USA kaubandusministeerium, pakutava kaitse piisavust isikuandmete puhul, mida edastatakse EList USA organisatsioonidele, mis on ühinenud programmiga Safe Harbor;
- AI. arvestades, et oma 5. juuli 2000. aasta resolutsioonis väljendas Euroopa Parlament kahtlusi ja muret programmi Safe Harbor piisavuse pärast ning kutsus komisjoni üles oma otsust kogemuste ja mis tahes õigusliku arengu valguses aegsasti läbi vaatama;
- AJ. arvestades, et oma 12. detsembri 2013. aasta töödokumendis nr 4 (USA jälgimistegevuse kohta seoses ELi andmetega ja selle võimalike õiguslike tagajärgede kohta Atlandi-ülestele kokkulepetele ja koostööle) väljendasid raportöörid kahtlusi ja muret programmi Safe Harbor piisavuse pärast ja kutsusid komisjoni üles tunnistama kehtetuks oma otsuse programmi Safe Harbor piisavuse kohta ning leidma uusi õiguslikke lahendusi;
- AK. arvestades, et komisjoni otsuses 2000/520/EÜ nähakse ette, et liikmesriikide pädevad asutused võivad kasutada oma volitusi andmete edastamise peatamiseks organisatsioonile, mis on kohustunud järgima programmi Safe Harbor põhimõtteid, et tagada üksikisikute kaitse seoses nende isikuandmete töötlemisega, kui on väga tõenäoline, et programmi Safe Harbor põhimõtteid rikutakse või kui edastamise jätkamisel tekiks andmesubjektidele otsene raske kahju oht;
- AL. arvestades, et komisjoni otsuses 2000/520/EÜ nähakse samuti ette, et kui on tõendeid selle kohta, et nimetatud põhimõtete järgimise tagamise eest vastutav asutus ei täida oma rolli tõhusalt, peab komisjon teatama sellest USA kaubandusministeeriumile ja vajaduse korral esitama meetmed kõnealuse otsuse tühistamiseks või peatamiseks või selle reguleerimisala piiramiseks;
- AM. arvestades, et kahes esimeses, 2002. ja 2004. aastal avaldatud aruandes programmi Safe Harbor rakendamise kohta tuvastas komisjon mitmesuguseid puudujääke seoses programmi Safe Harbor nõuetekohase rakendamisega ja andis USA ametivõimudele arvukalt soovitusi nende puuduste kõrvaldamiseks;
- AN. arvestades, et oma kolmandas, 27. novembri 2013. aasta rakendamisaruanDES, mis koostati üheksa aastat pärast teise aruande valmimist, ilma et vahepeal oleks ühtegi teises aruanDES tuvastatud puudust kõrvaldatud, tuvastas komisjon programmis Safe Harbor veel erinevaid nõrku külgi ja puudujääke ning jõudis järeldusele, et ei saa jätkata selle praegusel kujul rakendamist; arvestades, et komisjon on rõhutanud, et USA luureasutuste laiaulatuslik juurdepääs USA-le programmi Safe Harbor raames sertifitseeritud üksuste poolt edastatud andmetele tõstatab tõsiseid küsimusi seoses ELi andmesubjektide andmete kaitse järjepidevusega; arvestades, et komisjon saatis USA ametivõimudele 13 soovitusi ning võttis ülesande selgitada 2014. aasta suveks koos USA ametivõimudega välja parandusmeetmed, mis tuleb võimalikult kiiresti rakendada

ning mis on programmi Safe Harbor põhimõtete toimimise täieliku läbivaatamise aluseks;

- AO. arvestades, et Euroopa Parlamendi kodanikuvabaduste, justiits- ja siseasjade komisjoni delegatsioon kohtus 28.–31. oktoobril 2013 Washingtonis USA kaubandusministeeriumi ja USA föderalse kaubanduskomisjoniga; arvestades, et USA kaubandusministeerium tunnistas organisatsioonide olemasolu, mis on ise võtnud kohustuse järgida programmi Safe Harbor põhimõtteid, kuid mis ilmselgelt enam ei täida programmi Safe Harbor nõudeid, kuigi jätkavad isikuandmete vastuvõtmist EList; arvestades, et USA föderaalne kaubanduskomisjon tunnistas, et programm Safe Harbor tuleks läbi vaadata, et seda täiustada, eelkõige seoses kaebuste esitamise ja alternatiivsete vaidluste lahendamise süsteemidega;
- AP. arvestades, et programmi Safe Harbor põhimõtete järgimist võib piirata riikliku julgeoleku, avaliku huvi või õiguskaitsevajaduste täitmiseks vajalikus ulatuses; arvestades, et kuna tegu on põhiõiguse suhtes tehtava erandiga, peab sellist erandit alati tõlgendama kitsendustega ja selline erand peab olema piiratud demokraatlikus ühiskonnas vajalikkuse ja proportsionaalsusega ning seaduses tuleb selgelt kehtestada tingimused ja kaitsemeetmed, mis muudavad selle piirangu seaduslikuks; arvestades, et USA ja EL, eeskätt komisjon, oleksid pidanud selgitama sellise erandi kohaldamisala, et vältida mis tahes tõlgendust või rakendamist, mis nullib sisuliselt muu hulgas põhiõiguse eraelu puutumatusele ja andmekaitsele; arvestades, et sellist erandit ei tohiks järelikult mitte mingil juhul kasutada viisil, mis kahjustab põhiõiguste harta, Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni, ELi andmekaitseseaduse ja programmi Safe Harbor põhimõtetega tagatavat kaitset või muudab selle olematuks; nõuab, et kui kasutatakse riikliku julgeoleku erandit, tuleb täpsustada, millise siseriikliku õigusakti alusel seda tehakse;
- AQ. arvestades, et USA luureasutuste ulatuslik juurdepääs on tõsiselt vähendanud Atlandi-ülest usaldust ning avaldanud kahjulikku mõju usaldusele ELis tegutsevate USA organisatsioonide vastu; arvestades, et olukorda halvendab veelgi asjaolu, et USA õigusaktides puuduvad õiguslikud ja halduslikud kaitsevahendid ELi kodanike jaoks, eelkõige luure eesmärgil toimuva jälgimise korral;

Andmete edastamine kolmandatele riikidele piisava kaitse otsuse alusel

- AR. arvestades, et ilmsiks tulnud teabe ning kodanikuvabaduste, justiits- ja siseasjade komisjoni uurimistulemuste kohaselt on Uus-Meremaa, Kanada ja Austraalia riikliku julgeoleku eest vastutavad asutused osalenud laiaulatuslikult elektroonilise side massilises jälgimises ning teinud USAga aktiivset koostööd programmi Five Eyes raames, ning võivad olla vahetanud omavahel EList edastatud ELi kodanike isikuandmeid;
- AS. arvestades, et komisjoni otsuses 2013/65/EL¹ ja otsuses 2002/2/EÜ² kinnitati, et Uus-Meremaa ja Kanada isikuandmete kaitse ja elektrooniliste dokumentide õigusaktiga on tagatud piisaval tasemel kaitse; arvestades, et eespool nimetatud paljastused kahjustavad tõsiselt usaldust nende riikide õigussüsteemide vastu seoses ELi kodanikele pakutava kaitse järjepidevusega; arvestades, et komisjon ei ole seda aspekti uurinud;

¹ ELT L 28, 30.1.2013, lk 12

² EÜT L 2, 4.1.2002, lk 13.

Andmete edastamine lepingu tingimuste ja muude vahendite alusel

- AT. arvestades, et direktiivis 95/46/EÜ sätestatakse, et rahvusvaheline andmeedastus kolmandale riigile võib toimuda ka konkreetsetele vahenditele toetudes, kus andmekontrollija esitab tõendina piisavad tagatised seoses üksikisikute eraelu puutumatuse ning põhiõiguste ja -vabaduste kaitsega ning seoses vastavate õiguste kasutamisega;
- AU. arvestades, et sellised tagatised võivad tuleneda eelkõige asjakohastest lepingutingimustest;
- AV. arvestades, et direktiiviga 95/46/EÜ antakse komisjonile õigus otsustada, kas konkreetsed lepingu tüüptingimused pakuvad nimetatud direktiiviga nõutud piisavat kaitset, ning arvestades, et selle alusel on komisjon võtnud vastu kolm lepingu tüüptingimuste mudelit andmete edastamiseks andmekontrollijatele ja -töötlejatele (ja alltöötlejatele) kolmandates riikides;
- AW. arvestades, et komisjoni otsustes, millega kehtestatakse lepingute tüüptingimused, sätestatakse, et liikmesriikide pädevad asutused võivad kasutada oma volitusi peatada andmete liikumine, kui on kindlaks tehtud, et andmeimportija või alltöötleja kohta kehtiva õigusaktiga kehtestatakse talle nõuded kalduda kõrvale kohaldatavast andmekaitseõigusest, et kõnealused nõuded lähevad kaugemale direktiivi 95/46/EÜ artiklis 13 sätestatud demokraatlikus ühiskonnas vajalikest piirangutest ja et need nõuded võivad tõenäoliselt omada määravat ebasoodsat mõju lepingu tüüptingimustega ettenähtud tagatistele; või kui on olemas tõenäosus, et lisas esitatud lepingu tüüptingimusi ei järgita ning et jätkuv edastamine põhjustaks andmesubjektidele tõsise kahju tekkimise ohu;
- AX. arvestades, et riiklikud andmekaitseasutused on välja töötanud siduvad kontsernisisised eeskirjad, et lihtsustada rahvusvahelist andmeedastust rahvusvahelises korporatsioonis piisavate kaitsemeetmetega, mis seostuvad eraelu puutumatuse ning põhiõiguste ja -vabaduste kaitsega ning vastavate õiguste kasutamisega; arvestades, et enne nende kasutamist peavad liikmesriikide pädevad asutused andma siduvate kontsernisiseste eeskirjade kasutamise loa, olles eelnevalt hinnanud nende vastavust ELi andmekaitseseadusele; arvestades, et siduvad kontsernisisised eeskirjad andmetöötlejatele on kodanikuvabaduste, justiits- ja siseasjade komisjoni isikuandmete kaitse üldmäärust käsitlevas raportis tagasi lükatud, kuna need jätaksid andmete kontrollija ja andmesubjekti ilma igasugusest kontrollist jurisdiktsiooni üle, milles nende andmeid töödeldakse;
- AY. arvestades, et Euroopa Parlamendil on Euroopa Liidu toimimise lepingu artikliga 218 talle antud pädevuse alusel kohustus teostada pidevat järelevalvet nende rahvusvaheliste kokkulepete väärtuse üle, millele ta on oma nõusoleku andnud;

Andmete edastamine terroristide rahastamise jälgimisprogrammi (TFTP) lepingu ja broneeringuinfo lepingu alusel

- AZ. arvestades, et oma 23. oktoobri 2013. aasta resolutsioonis väljendas Euroopa Parlament tõsist muret paljastuste pärast NSA tegevuse kohta seoses otsese juurdepääsuga finantstehinguid käsitlevatele sõnumiandmetele ja seotud andmetele, mis oleks kõnealuse TFTP lepingu, eelkõige selle artikli 1 selge rikkumine;

- BA. arvestades, et terroristide rahastamise jälgimisprogramm on väga oluline vahend terrorismi rahastamise ja raske kuritegevuse vastases võitluses, võimaldades terrorismivastastel uurijatel avastada seoseid uurimisobjektide ja teiste potentsiaalsete kahtlusosaluste vahel, kes on seotud terrorismi rahastamises kahtlustatavate terroristide laiemate võrgustikega;
- BB. arvestades, et Euroopa Parlament palus komisjonil lepingu peatada ning teha kogu asjakohane teave ja dokumendid viivitamata kättesaadavaks, et neid saaks Euroopa Parlamendis arutada; arvestades, et komisjon ei ole teinud kumbagi;
- BC. arvestades, et pärast meedias avaldatud süüdistusi otsustas komisjon alustada USAga TFTP lepingu artikli 19 kohaseid konsultatsioone; arvestades, et 27. novembril 2013 teavitas komisjoni volinik Cecilia Malmström kodanikuvabaduste, justiits- ja siseasjade komisjoni, et pärast kohtumist USA ametivõimudega ja pidades silmas USA ametivõimude poolt saadetud kirjades ja nende poolt kohtumiste ajal antud vastuseid otsustas komisjon konsultatsioonidest loobuda põhjendusel, et puuduvad tõendid, mis näitaksid, et USA valitsus on tegutsenud viisil, mis on nimetatud lepingu sätetega vastuolus, ning et USA on andnud kirjaliku kinnituse, et ei ole toimunud otsest andmete kogumist, mis oleks vastuolus TFTP lepingu sätetega; arvestades, et ei ole selge, kas USA ametiasutused on lepingust kõrvale hiilinud, saades andmetele juurdepääsu muude vahendite kaudu, nagu osutatakse USA ametivõimude 18. septembri 2013. aasta kirjas¹;
- BD. arvestades, et kodanikuvabaduste, justiits- ja siseasjade komisjoni delegatsiooni 28.–31. oktoobril 2013 toimunud Washingtoni visiidi ajal oli delegatsioonil kohtumine USA rahandusministeeriumis; arvestades, et USA rahandusministeeriumi väitel ei ole neil alates TFTP lepingu jõustumisest olnud juurdepääsu Ülemaailmse Pankadevahelise Finantsinfo Ühingu (Society for Worldwide Interbank Financial Telecommunication (SWIFT)) andmetele ELis, välja arvatud TFTP lepingu raamistikus; arvestades, et USA rahandusministeerium keeldus kommentaaride andmisest selle kohta, kas SWIFTi andmetele võisid juurde pääseda mis tahes muud USA valitsusorganid või ministeeriumid väljaspool TFTP lepingut ning kas USA administratsioon oli NSA massilisest jälgimistegevusest teadlik; arvestades, et 18. detsembril 2013 väitis Glenn Greenwald enne seda, kui kodanikuvabaduste, justiits- ja siseasjade komisjon alustas uurimist, et NSA ja Ühendkuningriigi Valitsusside Peakorter (Government Communications Headquarters (GCHQ)) sihtmärgiks olid SWIFTi võrgustikud;
- BE. arvestades, et Belgia ja Madalmaade andmekaitseasutused otsustasid 13. novembril 2013 viia läbi ühise uurimise SWIFTi maksevõrgustike turvalisuse küsimuses, et teha kindlaks, kas kolmandatel osalistel on võimalik saada volitamata või ebaseaduslikku juurdepääsu Euroopa kodanike pangaandmetele²;
- BF. arvestades, et vastavalt ELi ja USA broneeringuinfo lepingu ühise läbivaatamise

¹ Kirjas märgitakse, et „USA valitsus otsib ja hangib finantsteavet [...], mis on kogutud regulatiiv-, õiguskaitse, diplomaatiliste ja luurekanalite kaudu, samuti vahetuste kaudu välispartneritega [...], ning USA valitsus kasutab TFTP lepingut, et hankida SWIFTi andmeid, mida me muudest allikatest ei saa”.

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>

tulemustele avalikustas USA sisejulgeolekuministeerium NSAle broneeringuinfo andmeid 23 korral üksikjuhtumite kaupa terrorismivastaste juhtumite toetamiseks, mis on kooskõlas nimetatud lepingu konkreetsete tingimustega;

- BG. arvestades, et ühise läbivaatamise tulemustes ei mainita asjaolu, et luure-eesmärkidel isikuandmete töötlemise korral ei kaitse USA seaduste kohaselt ükski õiguslik ega halduslik vahend muude kui USA kodanike õigusi ning et põhiseadusega ette nähtud kaitse kehtib üksnes USA kodanike suhtes; arvestades, et selliste õigus- või haldusalaste õiguste puudumine muudab kehtivas PNR-lepingus sätestatud ELi kodanike kaitse tühiseks;

Andmete edastamine ELi ja USA vahelise kriminaalasjades osutatava vastastikuse õigusabi lepingu alusel

- BH. arvestades, et 6. juuni 2003. aasta ELi ja USA vaheline kriminaalasjades osutatava vastastikuse õigusabi leping¹ jõustus 1. veebruaril 2010 ning selle eesmärk on lihtsustada ELi ja USA vahelist koostööd, et võidelda tõhusamalt kuritegevuse vastu, võttes seejuures nõuetekohaselt arvesse üksikisikute õigusi ja õigusriigi põhimõtet;

Raamleping andmekaitse kohta politsei- ja õigusalase koostöö raames (raamleping)

- BI. arvestades, et nimetatud raamlepingu eesmärk on kehtestada õigusraamistik isikuandmete edastamiseks ELi ja USA vahel kriminaalasjades tehtava politsei- ja õigusalase koostöö raames – üksnes kuritegude, sealhulgas terrorismi ärahoidmise, uurimise, avastamise või nende eest vastutusele võtmise eesmärgil; arvestades, et nõukogu andis loa läbirääkimiste alustamiseks 2. detsembril 2010; arvestades, et kõnealune leping on äärmiselt tähtis ja see toimiks andmeedastuse lihtsustamise alusena politsei- ja õigusalase koostöö kontekstis ja kriminaalasjades;
- BJ. arvestades, et nimetatud lepingus tuleks sätestada selged ja täpsed õiguslikult siduvad andmetöötluseeskirjad ja selles tuleks eelkõige tunnustada ELi kodanike õigust pääseda õiguslikult juurde oma isikuandmetele USAs, neid parandada ja kustutada ning samuti ELi kodanike õigust tõhusatele halduslikele ja õiguslikele kaitsemehhanismile USAs ning andmetöötlustoimingute sõltumatu järelevalve;
- BK. arvestades, et oma 27. novembri 2013. aasta teatises märkis komisjon, et selle raamlepingu tulemuseks peaks olema kodanike kaitse kõrge tase Atlandi ookeani mõlemal kaldal ning see peaks tugevdama eurooplaste usaldust ELi ja USA vahelise andmevahetuse vastu, mis annab aluse ELi ja USA vahelise julgeolekualase koostöö ja partnerluse edasiarendamiseks;
- BL. arvestades, et läbirääkimised lepingu üle ei ole edenened, kuna USA valitsus on järjepidevalt keeldunud tunnustamast ELi kodanike õigust tõhusatele halduslikele ja õiguslikele kaitsemeetmetele ning kuna USAl on kindel kavatsus sätestada laiaulatuslikke erandeid lepingus sisalduvate andmekaitsepõhimõtete osas, näiteks eesmärgikohasuse põhimõte, andmete säilitamine või andmete edasisaatmine riigisisesele või välismaale;

Andmekaitsereform

¹ ELT L 181, 19.7.2003, lk 25.

- BM. arvestades, et ELi andmekaitse õigusraamistik on praegu läbivaatamisel, et luua kõikide andmetöötlustoimingute jaoks ELis kõikehõlmav, terviklik, nüüdisaegne ja kindel süsteem; arvestades, et 2012. aasta jaanuaris esitas komisjon seadusandlike ettepanekute paketi – isikuandmete kaitse üldmääruse¹, millega asendatakse direktiiv 95/46/EÜ ja millega kehtestatakse ühesugune õigus kogu ELis, ning direktiiv², millega kehtestatakse ühtlustatud raamistik õiguskaitseasutuste kõikide õiguskaitse eesmärgil tehtavate andmetöötlustoimingute suhtes ja millega vähendatakse praeguseid erinevusi liikmesriikide seadustes;
- BN. arvestades, et 21. oktoobril 2013 võttis kodanikuvabaduste, justiits- ja siseasjade komisjon vastu seadusandlikud raportid nimetatud kahe ettepaneku kohta ning otsuse läbirääkimiste alustamise kohta nõukoguga, mille eesmärk on võtta nimetatud õigusaktid vastu parlamendi praeguse koosseisu ametiaja jooksul;
- BO. arvestades, et kuigi 24.–25. oktoobril 2013 toimunud Euroopa Ülemkogul kutsuti üles võtma õigeaegselt vastu tugevat ELi üldist andmekaitseraamistikku, et suurendada kodanike ja ettevõtete usaldust digitaalmajanduse vastu, ei ole Euroopa Ülemkogu suutnud pärast kaks aastat kestnud arutelusid andmekaitse üldmääruse ja direktiivi küsimuses³ siiski jõuda üldise lähenemisviisini;

IT-julgeolek ja pilvandmetöötlus

- BP. arvestades, et Euroopa Parlamendi ülalnimetatud 10. detsembri 2013. aasta resolutsioonis rõhutati pilvandmetöötluse ettevõtete majanduslikku potentsiaali majanduskasvu ja tööhõive seisukohast; arvestades, et ennustuste kohaselt on pilvandmetöötluse turu väärtus 2016. aastaks 207 miljardit USA dollarit aastas, mis on kaks korda suurem kui aastal 2012;
- BQ. arvestades, et andmekaitse tase pilvandmetöötluse keskkonnas ei tohi olla madalam, kui seda nõutakse mis tahes muus andmetöötluse kontekstis; arvestades, et liidu andmekaitsealased õigusaktid kehtivad tänu oma tehnoloogilisele neutraalsusele juba praegu täielikult ELis osutatavate pilvandmetöötluse teenuste suhtes;
- BR. arvestades, et massijälgimine annab luureasutustele juurdepääsu ELi üksikisikute isikuandmetele, mis on salvestatud või muul viisil töödeldud USA suuremate pilveteenuste osutajatega sõlmitud pilveteenuste lepingute raames; arvestades, et USA luureasutused on pääsenud juurde ELi pinnal asuvatesse serveritesse salvestatud või muul viisil töödeldud isikuandmetele, murdes sisse Yahoo ja Google'i sisevõrkudesse; arvestades, et sellise tegevusega rikutakse rahvusvahelisi kohustusi ja Euroopa põhiõigusi, sealhulgas õigust era- ja perekonnaelu puutumatusele, teabevahetuse saladust, süütuse presumptsiooni, sõna- ja teabevabadust, kogunemis- ja ühinemisvabadust ning ettevõtlusvabadust; arvestades, et ei saa välistada, et luureasutused on pääsenud juurde ka liikmesriikide riigiasutuste või ettevõtete ja institutsioonide poolt pilveteenustes salvestatud teabele;
- BS. arvestades, et USA luureagentuurid kasutavad krüptograafiliste protokollide ja toodete süstemaatilise kahjustamise poliitikat, et neil oleks võimalik kinni püüda isegi

¹ COM(2012)0011, 25.1.2012.

² COM(2012)0010, 25.1.2012.

³ http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf

krüpteeritud teabevahetust; arvestades, et NSA on kogunud suure arvu nn püsivaid nõrkusi (*zero-day exploits*) ehk IT turvaauke, mis ei ole üldsusele või toote müüjale veel teada; arvestades, et selline tegevus kahjustab ulatuslikult üleilmseid jõupingutusi IT turvalisuse parandamisel;

- BT. arvestades tõsiasja, et luureagentuurid on juurde pääsenud internetiteenuste kasutajate isikuandmetele, mis on olulisel määral vähendanud kodanike usaldust selliste teenuste vastu ja see on kahjustanud suurandmete tehnoloogiat ja uusi rakendusi (nagu nn asjade internet) kasutatavatesse teenustesse investeerivaid ettevõtjaid;
- BU. arvestades, et IT müüjad tarnivad sageli tooteid, mida ei ole nõuetekohaselt katsetatud IT turvalisuse suhtes või mille puhul mõnikord on müüja isegi tahtlikult lisanud nn tagaukse (*backdoor*) võimalused; arvestades, et tarkvaramüüjate vastutuseeskirjade puudumine on viinud sellise olukorrani, mida omakorda kasutavad ära luureagentuurid, kuid mis jätab alles ka ohu, et ründajaks on muutunud üksused;
- BV. arvestades, et selliseid uusi teenuseid ja rakendusi pakkuvate ettevõtete jaoks on väga oluline järgida andmekaitse-eeskirju ja nende andmesubjektide eraelu puutumatust, kelle andmeid kogutakse, töödeldakse ja analüüsitakse, et säilitada kodanike seas kõrge usalduse tase;

Luureteenistuste demokraatlik järelevalve

- BW. arvestades, et luureteenistustele antakse demokraatlikus ühiskonnas erilised volitused ja vahendid, et kaitsta põhiõigusi, demokraatiat ja õigusriigi põhimõtteid, kodanikuõigusi ning riiki sisemiste ja väliste ohtude eest, ning nende suhtes kohaldatakse demokraatlikku aruandluskohustust ja õiguslikku järelevalvet; arvestades, et neile antakse ainult sel eesmärgil eriõigused ja -volitused; arvestades, et neid volitusi tuleks kasutada põhiõiguste, demokraatia ja õigusriigi põhimõtetega seatud õiguslikes piirides ning nende kohaldamist tuleks rangelt kontrollida, sest vastasel korral ei ole need enam õiguspärased ja võivad kahjustada demokraatiat;
- BX. arvestades tõsiasja, et luureteenistustele on lubatud teatav salastatuse tase, mille eesmärk on hoida ära käimasolevate operatsioonide ohustamist, töömeetodite avalikustamist või agentide elu ohtu seadmist, ei või sellise salastatusega üle ega mööda minna nende teenistuste tegevuse demokraatliku ja õigusliku järelevalve ning läbipaistvuse eeskirjadest, eeskätt seoses põhiõiguste ja õigusriigi põhimõtete järgimisega, mis on demokraatliku ühiskonna alus;
- BY. arvestades, et suurem osa olemasolevatest riiklikest järelevalvemehhanismidest ja -organitest loodi või neid uuendati 1990. aastatel ning neid ei ole alati kohandatud viimase kümne aasta jooksul toimunud kiire poliitilise ja tehnoloogilise arenguga, mis on toonud kaasa tihenunud rahvusvahelise luurekoostöö, sealhulgas ka suure hulga isikuandmete vahetamise, ning see hägustab sageli luure- ja õiguskaitsetoimingute vahelist piiri;
- BZ. arvestades, et luuretegevuse üle teostatakse demokraatlikku järelevalvet siiski ainult riigi tasandil – vaatamata suurenenud teabevahetusele ELi liikmesriikide ning liikmesriikide ja kolmandate riikide vahel; arvestades, et lõhe ühelt poolt rahvusvahelise koostöö taseme ja teisalt riigi tasandiga piirduva järelevalve suutlikkuse vahel suureneb üha, mille tulemuseks on ebapiisav ja ebatõhus demokraatlik kontroll;

- CA. arvestades, et riiklikel järelevalveasutustel ei ole sageli täielikku juurdepääsu välisriigi luureasutusest saadud luureandmetele, mis võib põhjustada lünki, kus rahvusvaheline teabevahetus võib toimuda ilma piisava järelevalveta; arvestades, et probleemi on veelgi süvendanud nn kolmanda osapoole reegel või algse väljastaja kontrolli põhimõte, mille eesmärk on võimaldada algsel väljastajal säilitada kontrolli oma tundliku teabe edasise levitamise üle, kuid mida kahjuks sageli tõlgendatakse nii, nagu see kehtiks ka vastuvõtva teenistuse järelevalve suhtes;
- CB. arvestades, et erasektori ja avaliku sektori tegevuse läbipaistvuse reformi algatused on oluline tegur avalikkuse usalduse tagamiseks luureasutuste tegevuse vastu; arvestades, et õigussüsteemid ei tohiks takistada ettevõtetel avaldada üldsusele teavet selle kohta, kuidas nad käsitlevad valitsuse mitmesuguseid taotlusi ja kohtukorraldusi kasutajate andmetele juurdepääsuks, sealhulgas võimalust avaldada koondandmeid vastu võetud või tagasi lükatud taotluste ja korralduste arvu kohta;

Peamised järeldused

1. on arvamisel, et hiljutised õigusrikkumistest teatajate ja ajakirjanike paljastused ajakirjanduses kõrvuti käesoleva uurimise käigus antud eksperdiarvamusega, ametiasutuste omaksvõttudega ja ümberlükkamistega seoses nende väidetega annavad veenvaid tõendeid kaugeleulatuvate, keerukate ja tehnoloogiliselt väga arenenud süsteemide olemasolust, mille on loonud USA ja teatavate ELi liikmesriikide luureteenistused kogu maailma kodanike sideandmete, sealhulgas sisuandmete, asukohaandmete ning metaandmete kogumiseks, säilitamiseks ja analüüsimiseks enneolematu ulatuses ning valimatul ning kahtlust mitteärataval viisil;
2. osutab eriti USA NSA luureprogrammidele, mis võimaldavad pidada massilist järelevalvet ELi kodanike üle läbi otsese juurdepääsu juhtivate USA internetiettevõtete keskserveritele (PRISM programm), analüüsida infosisu ja metaandmeid (Xkeyscore programm), hiilida mööda online-krüpteeringutest (BULLRUN), pääseda juurde arvuti- ja telefonivõrkudele ning asukohaandmetele, samuti sellistele Suurbritannia luureameti GCHQ süsteemidele nagu ülesvoolu järelevalvetegevus (Tempora programm) ja dekrüpteerimisprogramm (Edgehill), suunatud vahendusründed (*man-in-the-middle*) teabesüsteemidele (programmid Quantumtheory ja Foxacid) ning päevas 200 miljoni SMS-tekstisõnumi kogumine ja säilitamine (programm Dishfire);
3. märgib, et Suurbritannia luureamet GCHQ on väidetavalt hakanud Belgacom'i süsteemidesse või neid pealt kuulanud; võtab teadmiseks Belgacom'i avaldused selle kohta, et ta ei saa kinnitada ega ümber lükata väidet, nagu oleksid ELi institutsioonid sihtmärgiks või kannaksid kahju, ning selle kohta, et kasutatud pahavara on äärmiselt keerukas ning selle väljaarendamine ja kasutamine nõuaks suurte rahaliste vahendite ja inimressursside kasutamist, mis ei oleks eraettevõtetele ega häkkeritele kättesaadav;
4. rõhutab, et usaldus on saanud tõsiselt kannatada – nii usaldus kahe Atlandi-ülese partneri vahel, ELi liikmesriikide vahel, kodanike ja nende valitsuste vahel, usaldus demokraatlike institutsioonide toimimise vastu mõlemal pool Atlandi ookeani, usaldus õigusriigi vastu kui ka usaldus IT-teenuste ja teabevahetuse turvalisuse vastu; on arvamisel, et usalduse taastamiseks kõikides nendes valdkondades on vaja viivitamata luua igakülgne reageerimiskava, mis sisaldaks paljusid avaliku kontrolli alla kuuluvaid meetmeid;

5. märgib, et mitme riigi valitsuse väitel on sellised massijärelevalveprogrammid vajalikud terrorismi vastu võitlemiseks; mõistab karmilt hukka terrorismi, kuid on täiesti veendunud, et terrorismivastane võitlus ei tohi kunagi õigustada suunamata, salajaste või isegi ebaseaduslike massijärelevalveprogrammide kasutamist; on seisukohal, et sellised programmid on vastuolus demokraatlikus ühiskonnas kehtivate vajalikkuse ja proportsionaalsuse põhimõtetega;
6. tuletab meelde ELi kindlat seisukohta, et vaja on leida õige tasakaal julgeolekumeetmete ning kodanikuvabaduste ja põhiõiguste austamise vahel ning tagada samal ajal eraelu puutumatuse ja andmekaitse põhimõtete hoolikas järgimine;
7. leiab, et sellises mahus andmete kogumine tekitab suuri kahtlusi selles, kas niisuguste meetmete puhul on lähtutud üksnes terrorismivastasest võitlusest, kuna see puudutab kõikvõimalike andmete kogumist kõikide kodanike kohta; osutab seetõttu võimalikele muudele eesmärkidele, sealhulgas poliitilistele motiividele ja majandusspionaažile, mille kahtlus tuleb täielikult välistada;
8. seab kahtluse alla mõnede liikmesriikide ulatusliku majandusspionaaži vastavuse ELi siseturu- ja konkurentsioigusega, mis on sätestatud Euroopa Liidu toimimise lepingu I ja VII jaotises; kinnitab taas lojaalse koostöö põhimõtet, nagu see on sätestatud Euroopa Liidu lepingu artikli 4 lõikes 3, ning põhimõtet, et liikmesriigid hoiduvad kõigist meetmetest, mis võiksid kahjustada liidu eesmärkide saavutamist;
9. märgib, et rahvusvahelised lepingud ja ELi ja USA õigusaktid ning siseriiklikud kontrollimehhanismid ei ole aidanud tagada vajalikku kontrolli ja tasakaalumehhanisme ega demokraatlikku vastutust;
10. mõistab hukka süütute inimeste isikuandmete, sealhulgas sageli eraelulise isikliku teabe massilise, süsteemse ja kõikehõlmava kogumise; rõhutab, et luureteenistuste kasutatavate massilise ja valimatu järelevalve süsteemidega rikutakse tõsiselt kodanike põhiõigusi; rõhutab, et õigus eraelu puutumatusele ei ole luksus, vaid vaba ja demokraatliku ühiskonna aluspõhimõte; juhib ühtlasi tähelepanu asjaolule, et massijärelevalvel võivad olla tõsised tagajärjed ajakirjandus-, mõtte- ja sõnavabadusele ja kogunemis- ja ühinemisvabadusele ning kogutud teavet võidakse suure tõenäosusega kasutada poliitiliste vastaste vastu; rõhutab, et sellised massijärelevalve meetmed hõlmavad ka luureteenistuste ebaseaduslikku tegevust ning tekitavad küsimuse siseriiklike õigusaktide eksterritoriaalse mõju kohta;
11. peab äärmiselt oluliseks tagada advokaatidele, ajakirjanikele, arstidele ja teistele reguleeritud kutsealade esindajatele konfidentsiaalsuse kaitse massijälgimismeetmete eest; rõhutab eriti, et kindlustunde puudumine advokaatide ja nende klientide teabevahetuse konfidentsiaalsuse suhtes mõjutaks negatiivselt ELi kodanike õigust saada õigusabi, õiguskaitse kättesaadavust ja õigust õiglasele kohtulikule arutamisele;
12. näeb järelevalveprogrammides järjekordset sammu n-ö täiemõõdulise ennetava riigi poole, kuna nende programmidega muudetakse demokraatlikes ühiskondades kehtivat kriminaalõiguse paradigma, kus igasuguseks sekkumiseks kahtlusaluste põhiõigustesse peab andma loa kohtunik või prokurör mõistliku kahtluse alusel ja seaduste kohaselt, ning selle asemel toetatakse segu häguste ja nõrkade õiguslike tagatistega õiguskaitse- ja luuretegevustest, mis ei ole sageli kooskõlas demokraatliku kontrolli ega võimude tasakaalu põhimõtte ja põhiõigustega, eriti süütuse presumptsiooniga; tuletab sellega

seoses meelde Saksamaa põhiseaduskohtu otsust ennetava ristjälituse (*präventive Rasterfahndung*) kasutamise keelamise kohta¹, välja arvatud juhul, kui esineb tõendeid konkreetsest ohust teistele tähtsatele õiguslikult kaitstud õigustele, kusjuures üldine ohuolukord või rahvusvahelised pinged ei ole piisavad, et lugeda sellised meetmed põhjendatuks;

13. on veendunud, et salajased õigusaktid ja kohtud on vastuolus õigusriigi põhimõttega; märgib, et mistahes kohtu või tribunali otsust ning ELi mittekuuluva riigi haldusasutuse otsust, millega lubatakse kas otseselt või kaudselt isikuandmete edastamist, ei tohi mingil viisil tunnustada ega jõustada mingil viisil, välja arvatud juhul, kui on olemas taotleva kolmanda riigi ja liidu või liikmesriigi vaheline vastastikuse õigusabi leping või rahvusvaheline kokkulepe ja eelnevalt on saadud pädevalt järelevalveasutuselt luba; tuletab meelde, et salakohtu või -tribunali mis tahes kohtuotsust või ELi mittekuuluva riigi haldusasutuse mis tahes otsust, millega antakse salaja luba kas otseseks või kaudseks jälgimistegevuseks, ei tunnustata ega kohaldata;
14. märgib, et eespool nimetatud probleeme on süvendanud tehnoloogia ja ühiskonnaelu kiire areng, kuna internet ja mobiilsed seadmed on kaasaegses igapäevaelus kõikjal olemas (lausandmetöötlus) ning enamiku internetiettevõtjate ärimudel rajaneb isikuandmete töötlemisel; on seisukohal, et selle probleemi ulatus on enneolematult suur; märgib, et see võib tekitada olukorra, kus andmete massilise kogumise ja töötlemise infrastruktuuri võidakse ära kasutada riigi poliitilise režiimi muutumise korral;
15. märgib, et ELi avaliku sektori institutsioonidele ja kodanikele ei ole võimalik tagada, et nende IT-turvalisus või -privaatsus oleks kaitstud hästivarustatud sissetungijate eest (puudub täielik IT-turvalisus); märgib, et maksimaalse IT-turvalisuse saavutamiseks peavad eurooplased olema valmis eraldama piisavalt nii inim- kui ka rahalisi vahendeid Euroopa sõltumatuse ja eneseusalduse säilitamiseks IT-valdkonnas;
16. on kindlalt vastu seisukohale, et kõik massijälgimise programmidega seotud probleemid on seotud ainult riikliku julgeolekuga ja kuuluvad seega liikmesriikide ainupädevusse; kordab, et liikmesriigid peavad oma riikliku julgeoleku tagamisel järgima täielikult ELi õigusakte ning Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni; tuletab meelde Euroopa Kohtu hiljutist otsust, milles märgitakse järgmist: „[...] kuigi liikmesriikide pädevuses on võtta meetmeid nende sise- ja välisjulgeoleku tagamiseks, ei saa üksnes asjaolu, et otsus puudutab riigi julgeolekut, tingida seda, et liidu õigus ei ole kohaldatav [...]”²; tuletab lisaks meelde, et ohus on kõikide ELi kodanike eraelu puutumatus kaitse, nagu ka ELi kommunikatsioonisüsteemide turvalisus ja usaldusväärsus; on seetõttu arvamisel, et ELi tasandi arutelud ja meetmed ei ole mitte ainult õiguspärased, vaid kujutavad endast ka ELi sõltumatuse küsimust;
17. kiidab institutsioone ja eksperte, kes on andud käesolevasse uurimisse oma panuse; peab kahetsusväärseks, et mõne liikmesriigi asutused on keeldunud tegemast koostööd uurimises, mida Euroopa Parlament viib praegu läbi kodanike huvides; tunneb heameelt mitme USA Kongressi ja teiste riikide parlamentide liikme avatuse üle;

¹ No 1 BvR 518/02, 4. aprill 2006.

² Otsus kohtuasjas C-300/11, ZZ v. Secretary of State for the Home Department, 4. juuni 2013.

18. on teadlik asjaolust, et nii lühikese aja jooksul on olnud võimalik ainult kõikide 2013. aasta juulis kerkinud probleemide esialgne uurimine; tunnistab, et ilmsiks tulnud on tulnud palju asjaolusid ja need tekitavad endiselt probleeme; rakendab seetõttu pikemaajalisel kavandamisel põhinevat lähenemisviisi, mis hõlmab konkreetseid ettepanekuid ja mehhanisme järgmise parlamendi koosseisu ametiajal võetavateks järeelmeetmeteks ja millega tagatakse, et järeldused jäävad ELi poliitilises tegevuskavas tähtsale kohale;
19. kavatseb paluda uuel Euroopa Komisjonilt, mille koosseis määratakse kindlaks pärast 2014. aasta mais toimuvaid Euroopa Parlamendi valimisi, kindlate poliitiliste kohustuste võtmist käimasoleva uurimise ettepanekute ja soovitude rakendamiseks;

Soovitused

20. kutsub USA ametiasutusi ja ELi liikmesriike, kes seda veel teinud ei ole, keelustama massilise jälgimistegevuse;
21. palub ELi liikmesriikidel ja eeskätt neil, kes osalevad programmides Nine Eyes ja Fourteen Eyes¹, põhjalikult hinnata ja vajaduse korral läbi vaadata oma luureteenistuste tegevust reguleerivad siseriiklikud õigusaktid ja tavad, et tagada nende suhtes parlamendi kontroll, õiguslik ja avalikkuse järelevalve ning seaduslikkuse, vajalikkuse ja proportsionaalsuse, nõuetekohase menetluse, kasutaja teavitamise ja läbipaistvuse põhimõtete, sealhulgas ÜRO heade tavade kogumiku ja Veneetsia komisjoni soovitude järgimine ning nende vastavus Euroopa inimõiguste konventsiooni normidele ja liikmesriikide põhiõiguste alal võetud kohustustele, eriti andmekaitse, eraelu puutumatuse ja süütuse presumptsiooni osas;
22. palub ELi liikmesriike ja eeskätt Ühendkuningriigil, Prantsusmaal, Saksamaal, Rootsil, Madalmaadel ja Poolal seoses Euroopa Parlamendi 4. juuli 2013. aasta resolutsiooni ja uurimisega seotud kuulamistega tagada, et nende praegune ja edaspidine luureasutuste tegevust reguleeriv õigusraamistik ja jälgimismehhanism oleks kooskõlas Euroopa inimõiguste konventsiooni ja Euroopa Liidu andmekaitset käsitlevate õigusaktidega; kutsub nimetatud liikmesriike selgitama väiteid massilise jälgimistegevuse, sealhulgas piiriülese teabevahetuse massiline jälgimise, kaablipõhise side suunamata jälgimise, võimalike kokkulepete kohta luureteenistuste ja telekommunikatsiooniettevõtete vahel seoses isikuandmetele juurdepääsu ja nende vahetamisega ning juurdepääsuga siderajatistele, sealhulgas Atlandi-ülestele kaablitele, USA luuretöötajate ilma järelevalveta jälgimistegevuse ja varustuse kohta ELi territooriumil üle ning selle vastavuse kohta ELi õigusaktidele; palub nimetatud riikide parlamentidel tihendada luuretegevuse järelevalveasutuste koostööd Euroopa tasandil;
23. kutsub Ühendkuningriiki eeskätt seoses luureteenistuse GCHQ massilisele jälgimisele viitavate ulatuslike meediakajastustega vaatama läbi kehtiva õigusraamistiku, mis koosneb kolmest eraldiseisvast, kuid omavahel keerukas koostoimes olevast õigusaktist, nimelt 1998. aasta inimõiguste seadusest, 1994. aasta luureteenistuste seadusest ning 2000. aasta uurimisvolituste korraldamise seadusest;

¹ Programmi Nine Eyes kuuluvad USA, Ühendkuningriik, Kanada, Austraalia, Uus-Meremaa, Taani, Prantsusmaa, Norra ja Madalmaad; programmis Fourteen Eyes osalevad eespool nimetatud riigid ning lisaks Saksamaa, Belgia, Itaalia, Hispaania ja Rootsi.

24. võtab teadmiseks Taani 2002. aasta luure- ja julgeolekuseaduse läbivaatamise (Desseni komisjoni 2. detsembri 2013. aasta aruanne); toetab läbivaatamise komisjoni neid soovitusi, mille eesmärk on parandada Taani luureteenistuste läbipaistvust ning kontrolli ja järelevalvet nende üle; palub Madalmaadel hoiduda luureteenistuste volituste laiendamisest, et luureteenistused ei saaks süütute kodanike suunamata ja laiaulatuslikku jälgimist teostada ka kaablipõhise side kaudu, arvestades eeskätt tõsiasja, et üks suurimaid interneti vahetuspunkte maailmas asub Amsterdavis (AMS-IX); nõuab ettevaatust uue ühendatud küberüksuse Sigint volituste ja võimekuse kindlaksmääramisel, samuti USA luure töötajate Taani territooriumil viibimise ja nende tegevuse suhtes;
25. kutsub liikmesriike, sealhulgas siis, kui neid esindavad luureasutused, üles hoiduma kolmandatelt riikidelt andmete vastuvõtmisest, kui need on kogutud ebaseaduslikult, ning mitte lubama kolmandate riikide valitsustel või ametitel teostada liikmesriigi territooriumil jälgimistegevust, mis on siseriiklike õigusaktide kohaselt ebaseaduslik või ei vasta rahvusvaheliste või ELi õigusaktidega kehtestatud õigustagatistele, kaasa arvatud inimõiguste kaitsele Euroopa Liidu lepingu, Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni ja Euroopa Liidu põhiõiguste harta kohaselt;
26. nõuab massilise pealtkuulamise ja veebikaamera kujutiste töötlemise lõpetamist kõigi salateenistuste poolt; kutsub liikmesriike üles täies ulatuses uurima, kas, kuidas ja mil määral on nende vastavad salateenistused osalenud veebikaamera kujutiste kogumises ja töötlemises ning kustutama kõik salvestatud kujutised, mis on kogutud selliste massijärelevalveprogrammide abil;
27. kutsub liikmesriike üles viivitamata täitma Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni kohaselt kohustust kaitsta oma kodanikke jälgimise eest, mis ei ole konventsiooniga kooskõlas, kaasa arvatud juhul, kui selle eesmärk on kaitsta riiklikku julgeolekut, ning mida teostavad kolmandad riigid või nende enda luureteenistused, ning tagama, et kolmanda riigi õigusaktide eksterritoriaalne rakendamine ei kahjustaks õigusriigi põhimõtet;
28. kutsub Euroopa Nõukogu peasekretäri algatama artikli 52 menetlust, mille kohaselt „Euroopa Nõukogu peasekretäri taotlusel esitab iga kõrge lepinguosaline selgituse, kuidas tema siseriiklik õigus kindlustab käesoleva konventsiooni mis tahes sätete tõhusa elluviimise”;
29. kutsub liikmesriike üles võtma viivitamata asjakohaseid meetmeid, sealhulgas kohtumeetmeid nende suveräänsuse ja seeläbi üldise rahvusvahelise õiguse rikkumise vastu, mida teostatakse massijälgimisprogrammide kaudu; kutsub lisaks liikmesriike üles kasutama kõiki olemasolevaid rahvusvahelisi meetmeid ELi kodanike põhiõiguste kaitsmiseks, eelkõige käivitades kodaniku- ja poliitiliste õiguste rahvusvahelise pakti artikli 41 kohase riikidevahelise kaebemenetluse;
30. kutsub liikmesriike üles looma tõhusaid mehhanisme, mille kaudu need, kes vastutavad õigusriigi põhimõtteid ja kodanike põhiõigusi rikkuvate (massi)järelevalveprogrammide eest, võetakse sellise võimu kuritarvitamise eest vastutusele;
31. kutsub USAd üles viivitamata oma õigusakte läbi vaatama, et viia need kooskõlla rahvusvahelise õigusega, tunnistada ELi kodanike eraelu puutumatust ja teisi õigusi, pakkuda ELi kodanikele õiguskaitset, seada ELi kodanike õigused samale alusele USA

kodanike õigustega ning allkirjastada vabatahtlik protokoll, mis võimaldab üksikisikutel esitada kaebusi kodaniku- ja poliitiliste õiguste rahvusvahelise pakti alusel;

32. tervitab sellega seoses USA presidendi Obama 17. jaanuaril 2014 välja antud presidendi poliitilises direktiivis esitatud märkusi kui sammu jälgimise ja andmetöötluse riikliku julgeoleku eesmärgil lubamise piiramise ja kõigi isikute isikuandmete võrdse kohtlemise poole USA luurekogukonna poolt, sõltumata kodakondsusest või elukohast; ootab selles kontekstis siiski edasisi konkreetseid samme ELi ja USA suhetes, mis esmalt tugevdavad usaldust Atlandi-ülese andmeedastuse vastu ja pakuvad siduvaid tagatisi ELi kodanike kasutatavatele eraelu puutumatuse õigustele, nagu on käesolevas raportis üksikasjalikult esitatud;
33. rõhutab oma tõsist muret Euroopa Nõukogu küberkuritegevuse konventsiooni komitees 23. novembri 2001. aasta küberkuritegevuse konventsiooni (Budapesti konventsiooni) artikli 23 (milles käsitletakse piiriülest juurdepääsu salvestatud arvutiandmetele, mille puhul on vajalik nõusolek või mis on avalikult kättesaadavad) tõlgendamisega seotud töö pärast, ja on vastu mis tahes lisaprotokolli sõlmimisele või suunistele, mille eesmärk on laiendada selle sätte kohaldamisala kõnealuse konventsiooniga kehtestatud praegusest korrast kaugemale, mis juba niigi on suur erand territoriaalsuse põhimõtte suhtes, kuna see võib anda õiguskaitseasutustele tõkestamata kaugjuurdepääsu teistes jurisdiktsioonides paiknevatele serveritele ja arvutitele, ilma et neil oleks vaja kasutada vastastikuse õigusabi kokkuleppeid ja muid õiguslase koostöö vahendeid, mis on kehtestatud tagamaks üksikisiku põhiõigusi, sealhulgas andmekaitset ja nõuetekohase protsessi õigust, eelkõige Euroopa Nõukogu konventsiooni 108;
34. palub komisjonil hinnata enne 2014. aasta juulit määruse (EÜ) nr 2271/96 kohaldatavust isikuandmete ülekandmist käsitlevate õigusaktide kollisioonijuhtumite suhtes;
35. palub põhiõiguste ametil uurida põhjalikult põhiõiguste kaitset seoses jälgimisega ning eelkõige ELi kodanike praegust õiguslikku olukorda seoses kõnealuste tavade seotud õiguskaitsevahenditega;

Andmete rahvusvaheline edastamine

USA andmekaitse õigusraamistik ning USA Safe Harbor

36. märgib, et meediapaljastustes nimetatud ettevõtted, kes on seotud USA NSA teostatava ELi andmesubjektide laiaulatusliku jälgimisega, on ettevõtted, kes on iseseisvalt liitunud programmiga Safe Harbor, ning et programm Safe Harbor on õigusvahend, mida kasutatakse ELi isikuandmete ülekandmiseks USAsse (nt Google, Microsoft, Yahoo!, Facebook, Apple, LinkedIn); tunneb muret, et kõnealused organisatsioonid ei ole krüpteerinud oma andmekeskuste vahelist teavet ja sidet, võimaldades luureteenistustel seeläbi teavet hankida; tervitab sellega seoses mõnede USA ettevõtete hilisemaid avaldusi, et nad kiirendavad kavasid oma ülemaailmsete andmekeskuste vaheliste andmevoogude krüpteerimiseks;
37. on arvamisel, et USA luureametite laiaulatuslik juurdepääs ELi isikuandmetele, mida töötleb programm Safe Harbor, ei vasta riikliku julgeoleku kaalutlustel tehtava erandi kriteeriumile;
38. on seisukohal, et kuna praeguses olukorras ei taga programmi Safe Harbor põhimõtted

ELi kodanikele nõuetekohast kaitset, tuleks selliseid ülekandeid teostada teiste õigusaktide alusel, nagu näiteks lepingulised klauslid või siduvad kontsernisisesed eeskirjad, tingimusel, et need vahendid sätestavad konkreetsed õigustagatised ja kaitsevahendid ning neist ei saa mööda minna muude õigusraamistikega;

39. on arvamisel, et komisjon ei ole tegutsenud, et parandada programmi Safe Harbor praeguse rakendamise hästi tuntud puudusi;
40. kutsub komisjoni üles esitama meetmed, et peatada kohe komisjoni otsus 2000/520/EÜ, millega tunnistati programmi Safe Harbor privaatsuspõhimõtete ning USA kaubandusministeeriumi väljastatud seonduvate korduma kippuvate küsimuste asjakohasust; palub USA ametiasutustel seetõttu esitada ettepaneku sellise uue raamistiku kohta isikuandmete ülekandmiseks ELilt USA-le, mis vastaks liidu andmekaitseenõuetele ning pakuks piisavat kaitsetaset;
41. kutsub liikmesriikide pädevaid asutusi, eelkõige andmekaitseasutusi, kasutama oma volitusi ning viivitamata peatama andmevood mis tahes organisatsiooni, kes on kinnitanud USA programmi Safe Harbor põhimõtete järgimist, ning nõudma, et selliseid andmevoogusid teostataks ainult teiste õigusaktide alusel, tingimusel et need sisaldavad vajalikke õigustagatisi ja kaitsevahendeid seoses üksikisikute privaatsuse ning põhiõiguste ja -vabadustega;
42. kutsub komisjoni üles esitama 2014. aasta detsembriks põhjaliku hinnangu USA eraelu puutumatust käsitleva raamistiku kohta, mis hõlmab kaubandus-, õiguskaitse- ja luuretegevust, ning USAs üldise andmekaitseseaduse puudumisel põhinevad konkreetsed soovitusel; ergutab komisjoni kaasama USA administratsiooni, et kehtestada õigusraamistik, mis pakub eraisikutele kõrgetasemelist kaitset seoses nende isikuandmetega, kui selliseid andmeid edastatakse USA-le, ning tagada ELi ja USA eraelu puutumatust käsitlevate raamistike võrdsus;

Piisava kaitse otsusega andmete edastamine muudele kolmandatele riikidele

43. tuletab meelde, et direktiivis 95/46/EÜ on sätestatud, et isikuandmeid võib kolmandasse riiki edastada üksnes juhul, kui kõnealuses kolmandas riigis on tagatud nende kaitse piisav tase, ilma et see piiraks siseriiklikke sätteid, mis on vastu võetud nimetatud direktiivi muude sätete alusel, ning kõnealuse sätte eesmärk on tagada ELi andmekaitseseaduste kaitse jätkuvus, kui isikuandmeid edastatakse väljapoole ELi;
44. tuletab meelde, et direktiivis 95/46/EÜ on sätestatud, et andmekaitse taseme piisavust kolmandates riikides tuleb hinnata, pidades silmas kõiki andmete edastamise toimingute või andmete edastamise toimingute kogumi asjaolusid; samuti tuletab meelde, et kõnealune direktiiv annab komisjonile rakendusvolitused, et otsustada, kas kolmas riik tagab andmekaitse piisava taseme, pidades silmas direktiivis 95/46/EÜ sätestatud kriteeriume; tuletab meelde, et direktiiv 95/46/EÜ annab komisjonile volitused otsustada, et kolmas riik ei taga piisavat kaitsetaset;
45. tuletab meelde, et viimasel juhul peavad liikmesriigid võtma vajalikke meetmeid, et vältida sama liiki andmete edastamist kõnealusesse kolmandasse riiki, ja et komisjon alustab läbirääkimisi, et olukorda parandada;
46. kutsub komisjoni ja liikmesriike üles viivitamata hindama, kas Uus-Meremaa eraelu

puutumatust käsitleva õigusakti ning Kanada isikuandmete kaitset ja elektroonilisi dokumente käsitleva õigusakti piisav kaitsetase, nagu on deklareeritud komisjoni otsustes 2013/65/EL ja 2002/2/EÜ, on mõjutanud nende riikide luureasutuste seotust ELi kodanike massilise jälgimisega, ning vajadusel võtma asjakohaseid meetmeid piisava kaitse otsuste peatamiseks või tühistamiseks; kutsub samuti komisjoni üles hindama olukorda teiste riikide puhul, kes on saanud piisavuse reitingu; loodab, et komisjon esitab aruande Euroopa Parlamendile oma järelduste kohta eespool nimetatud riikides hiljemalt 2014. aasta detsembriks;

Andmete edastamine lepingutingimuste ja muude vahendite alusel

47. tuletab meelde, et riiklikud andmekaitseasutused on märkinud, et lepingu tüüptingimused ja siduvad kontsernisisised eeskirjad ei ole sõnastatud isikuandmete massilise jälgimise juurdepääsu olukordi silmas pidades ja et selline juurdepääs ei ole kooskõlas lepingutingimuste ja siduvate kontsernisiseste eeskirjade erandite sätetega, mis viitavad üksikutele eranditele õigustatud huvi puhul demokraatlikus ühiskonnas, kui see on vajalik ja proportsionaalne;
48. kutsub liikmesriike üles keelustama või peatama andmeedastused kolmandatesse riikidesse, mis põhinevad lepingu tüüptingimustel, lepingutingimustel või siduvatel kontsernisisestel eeskirjadel, mis on kinnitatud riiklike pädevate asutuste poolt, kui on tõenäoline, et õigus, millele andmete saaja allub, määrab talle nõudmised, mis lähevad kaugemale piirangutest, mis on demokraatlikus ühiskonnas rangelt vajalikud, asjakohased ja proportsionaalsed, ja millel on tõenäoliselt kahjulik mõju tagatistele, mida annavad kohaldatavad andmekaitseseadused ja lepingu tüüptingimused, või kuna jätkuv edastamine võib tekitada suurt kahju andmesubjektidele;
49. kutsub artikli 29 töörühma üles välja andma suunised ja soovitusel tagatiste ja kaitse kohta, mida peaksid sisaldama ELi isikuandmete rahvusvahelise edastamise lepingulised vahendid, et tagada üksikisikute eraelu puutumatus, põhiõiguste ja -vabaduste kaitse, võttes eelkõige arvesse kolmandate riikide luure- ja riikliku julgeoleku õigusakte ning kolmandas riigis andmeid vastuvõtivate ettevõtete osalust kolmanda riigi luureasutuste massilise jälgimise toimingutes;
50. palub komisjonil viivitamata üle vaadata kehtestatud lepingulised tüüptingimused, et hinnata, kas need pakuvad vajalikku kaitset seoses edastatud isikuandmetele juurdepääsuga luure eesmärkidel, ning vajaduse korral need läbi vaadata;

Andmete edastamine vastastikuse õigusabi kokkuleppe alusel

51. kutsub komisjoni üles enne 2014. aasta lõppu läbi viima põhjaliku olemasoleva vastastikuse õigusabi kokkuleppe hindamise kooskõlas selle artikliga 17, et kontrollida selle praktilist rakendamist, eelkõige seda, kas USA on seda tõhusalt kasutanud EList teabe või tõendite saamiseks ja kas lepingust on kõrvale hoitud, et saada teavet otse EList, ning hinnata mõju üksikisikute põhiõigustele; selline hindamine ei peaks viitama üksnes USA ametlikele avaldustele kui analüüsi piisavale alusele, vaid peaks põhinema ka ELi erihinnangutel; kõnealune põhjalik läbivaatus peaks käsitlema ka liidu konstitutsioonilise struktuuri rakendamise tagajärgi sellele vahendile, et viia see kooskõlla liidu õigusaktidega, võttes arvesse eelkõige protokolli 36 ja selle artiklit 10 ning seda protokolli käsitlevat deklaratsiooni 50; palub samuti nõukogul ja komisjonil hinnata liikmesriikide ja USA vahelisi kahepoolseid lepinguid, et valvata selle järele, et

need kahepoolsed lepingud oleksid kooskõlas lepingutega, mis EL on sõlminud või otsustab sõlmida USAga;

ELi vastastikune abi kriminaalasjades

52. palub nõukogul ja komisjonil teavitada parlamenti, kuivõrd on liikmesriigid tegelikult kasutanud konventsiooni liikmesriikide vahelise vastastikuse õigusabi kohta kriminaalasjades, eelkõige selle kolmandat jaotist telekommunikatsiooni pealtkuulamise kohta; kutsub komisjoni üles esitama kooskõlas deklaratsiooniga 50 ettepanekut protokollis 36 kohta vastavalt nõutule enne 2014. aasta lõppu, et kohandada see Lissaboni lepingu raamistikuga;

Andmete edastamine TFTP- ja PNR-lepingu alusel

53. on seisukohal, et Euroopa Komisjoni ja USA rahandusministeeriumi antud andmed ei täpsusta, kas USA luureasutustel on juurdepääs SWIFT-finantstehinguid käsitlevatele sõnumitele ELis, jälgides SWIFT-võrgustikke või panga operatsioonisüsteeme või sidevõrke, üksi või koos ELi riiklike luureasutustega, ning ilma et toetutaks olemasolevatele vastastikuse õigusabi ja õiguslase koostöö kahepoolsetele kanalitele;
54. tuletab meelde oma 23. oktoobri 2013. aasta resolutsiooni ja palub komisjonil peatada TFTP-leping;
55. palub komisjonil reageerida murettekitavale asjaolule, et kolm peamist arvutipõhist broneerimissüsteemi, mida kasutavad lennufirmad üle maailma, paiknevad USAs ja et broneeringuinfo andmed salvestatakse pilvesüsteemis, mis tegutseb USA pinnal USA õigusaktide alusel, kus puudub piisav andmekaitse;

Raamleping andmekaitse kohta politsei- ja õiguslase koostöö raames (nn laiahaardeline leping)

56. leiab, et raamlepingu kohane rahuldav lahendus on Atlandi-üleste partnerite vahelise täieliku usalduse taastamise eeltingimuseks;
57. nõuab viivitamatut läbirääkimiste taasalustamist USAga seoses raamlepinguga, mis peaks seadma ELi kodanike õigused võrdsele alusele USA kodanike õigustega; rõhutab, et lisaks peaks leping tagama tõhusa ja rakendatava haldus- ja õiguskaitse kõigile ELi kodanikele USAs, ilma diskrimineerimiseta;
58. nõuab, et komisjon ja nõukogu ei algataks USAga mis tahes uusi valdkondlikke lepinguid ega lepinguid isikuandmete edastamiseks õiguskaitse eesmärkidel enne raamlepingu jõustumist;
59. nõuab tungivalt, et komisjon esitaks üksikasjaliku aruande läbirääkimisvolituste erinevate punktide kohta ja viimasest hetkeseisust 2014. aasta aprilliks;

Andmekaitse reform

60. nõuab, et nõukogu eesistuja ja liikmesriigid kiirendaksid oma tööd kogu andmekaitse paketiga, et selle saaks vastu võtta 2014. aastal, nii et kõik ELi kodanikud saaksid juba lähitulevikus nautida kõrgetasemelist andmekaitset; rõhutab, et nõukogu otsustav tegutsemine ja täielik toetus on vajalikud tingimused usaldusväarsuse ja otsusekindluse

tõestamiseks kolmandatele riikidele;

61. rõhutab, et nii andmekaitsemäärus kui ka andmekaitse direktiiv on vajalikud üksikisikute põhiõiguste kaitsmiseks ja seetõttu tuleb neid käsitleda pakulina, mis võetakse vastu üheaegselt, et tagada kõikide ELi andmetöötlustoimingute kõrgetasemeline kaitse igas olukorras; rõhutab, et võtab täiendavaid õiguskaitsealase koostöö meetmeid alles siis, kui nõukogu on alustanud parlamendi ja komisjoniga läbirääkimisi andmekaitse paketi teemal;
62. tuletab meelde, et lõimitud eraelukaitse ja eraelu kaitsvate vaikesätete käsitleused tugevdavad andmekaitset ning neist tuleks juhinduda kõikide internetis pakutavate toodete, teenuste ja süsteemide puhul;
63. peab interneti ja telekommunikatsiooni valdkonna suuremat läbipaistvust ja rangemaid kaitsestandardeid vajalikuks selleks, et tagada parem andmekaitsekord; palub seetõttu komisjonil esitada seadusandlik ettepanek interneti- ja telekommunikatsiooniteenuseid käsitlevate standardsete üldtingimuste kohta ning anda järelevalveasutusele volitus kontrollida üldtingimuste täitmist;

Pilvandmetöötlus

64. märgib, et USA pilvandmetöötlust ja pilveteenuse osutajaid mõjutavad negatiivselt eespool nimetatud tavad; rõhutab seetõttu Euroopa pilveteenuste ja IT-lahenduste arendamise tähtsust majanduskasvule ja tööhõivele ning usaldusele pilveteenuste ja nende osutajate vastu ning kõrgetasemelise isikuandmete kaitse tagamiseks;
65. palub kõiki liidu avaliku sektori asutusi, et nad ei kasutaks selliseid pilveteenuseid, millele võivad kohalduda muud kui ELi õigusaktid;
66. kordab oma tõsist muret seoses pilvandmetöötluse lepingute raames töödeldud ELi isikuandmete ja teabe kohustusliku otsese avaldamisega kolmandate riikide ametiasutustele pilveteenuste osutajate poolt, kelle suhtes kohaldatakse kolmanda riigi seadusi või kes kasutavad kolmandas riigis asuvat serverit, ning seoses kolmandate riikide õiguskaitseasutuste ja luureteenistuste otsese kaugjuurdepääsuga isikuandmetele ja töödeldavale teabele;
67. mõistab hukka asjaolu, et kolmandate riikide ametiasutused saavad sellise juurdepääsu tavaliselt oma õigusnormide otsese jõustamise kaudu, kasutamata seejuures õiguslikuks koostööks loodud rahvusvahelisi vahendeid, nagu vastastikune õigusabi või muu õiguslane koostöö;
68. kutsub komisjoni ja liikmesriike üles kiirendama tööd Euroopa pilvandmetöötluspartnerluse valdkonnas, kaasates täielikult nii kodanikuühiskonna kui ka tehnikaringkonnad, näiteks interneti-ehituse töökond (IETF), ning käsitledes ühtlasi andmekaitse aspekte;
69. nõuab tungivalt, et komisjon pööraks isikuandmete töötlemist hõlmavate rahvusvaheliste lepingute üle läbirääkimisi pidades erilist tähelepanu riskidele ja probleemidele, mida pilvandmetöötlus põhjustab põhiõiguste suhtes ning eelkõige – kuid mitte ainult – õiguse suhtes eraelu puutumatusele ja isikuandmete kaitsele, nagu on sätestatud Euroopa Liidu põhiõiguste harta artiklites 7 ja 8; nõuab lisaks tungivalt, et

komisjon võtaks arvesse läbirääkimiste partneri siseriiklikke eeskirju, mis reguleerivad õiguskaitse- ja luureasutuste juurdepääsu pilvandmetöötamise teenuste kaudu töödeldavatele isikuandmetele, eelkõige nõudes, et sellise juurdepääsu võib anda ainult seadusjärgse menetlemise põhimõtete täielikul järgimisel ning et sellise juurdepääsu lubamiseks peab olema üheselt mõistetav õiguslik alus, samuti nõudes, et oleks määratletud täpsed juurdepääsutingimused, juurdepääsu andmise eesmärk, andmete üleandmisel rakendatavad turvameetmed ja eraisikute õigused, samuti järelevalve- ja tõhusa hüvitamise mehhanismi eeskirjad;

70. tuletab meelde, et eranditult kõik ELis teenuseid osutavad ettevõtted peavad järgima ELi õigusakte ja vastutavad nende rikkumise eest, ning rõhutab tõhusate, proportsionaalsete ja hoiatavate halduskaristuste tähtsust, mida võidakse rakendada nende pilvandmetöötamise teenuse osutajate suhtes, kes ei järgi ELi andmekaitse standardeid;
71. palub komisjonil ja liikmesriikide pädevatel asutustel hinnata, millises ulatuses on ELi juriidiliste isikute koostöös salateenistustega või nõustumisel kolmandate riikide asutuste kohtu lubadega, milles taotletakse ELi kodanike isikuandmete avaldamist ELi andmekaitsealaste õigusaktide vastaselt, rikutud ELi eeskirju eraelu puutumatuse ja andmekaitse kohta;
72. kutsub Big Data tehnoloogiat kasutavaid uusi teenuseid ning uusi rakendusi, nagu asjade internet, pakkuvaid ettevõtjaid üles võtma juba arendamise etapis andmekaitsemeetmeid, et säilitada kodanike suur usaldus;

Atlandi-ülene kaubandus- ja investeerimispartnerlus (TTIP)

73. tunnustab, et EL ja USA peavad läbirääkimisi Atlandi-ülese kaubandus- ja investeerimispartnerluse üle, millel on suur strateegiline tähtsus edasise majanduskasvu loomisel;
74. rõhutab, arvestades digitaalmajanduse tähtsust ELi ja USA suhetes ning nendevahelise usalduse taastamisel, et Euroopa Parlamendi nõustumine lõpliku TTIP-lepinguga ei ole kindel enne, kui üldist massilist jälgimist ja isikuandmete suuremahulist töötlemist ning ELi institutsioonide ja diplomaatiliste esinduste pealtkuulamist ei ole täielikult lõpetatud ning kuni ei ole leitud sobivat lahendust ELi kodanike andmekaitseõiguse, muu hulgas haldus- ja õiguskaitse asjus; rõhutab, et parlament nõustub lõpliku TTIP-lepinguga ainult juhul, kui leping austab täielikult muu hulgas ELi põhiõiguste hartas tunnustatud põhiõigusi, ja et isikute eraelu kaitse seoses isikuandmete töötlemise ja levitamisega peab jätkuma GATSi artikli XIV kohaselt; rõhutab, et GATSi artikli XIV kohaldamisel ei saa ELi andmekaitsealaseid õigusakte pidada „meelevaldseks või õigustamatuks diskrimineerimiseks”;

Luureteenistuste demokraatlik järelevalve

75. rõhutab, et vaatamata asjaolule, et luureteenistuste tegevuse järelevalve peaks põhinema nii demokraatlikul õiguspärasusel (tugev õiguslik raamistik, eelnev loa taotlemine ja järelkontroll) kui ka piisaval tehnilisel suutlikkusel ja asjatundlikkusel, jääb enamikul praegustel ELi ja USA järelevalveasustusel puudu mõlemast, eelkõige tehnilisest suutlikkusest;
76. kutsub, nagu ta tegi Echelon juhtumil, kõiki riiklikke parlamente, kes ei ole seda

veel teinud, sisse seadma luuretegevuse mõtestatud järelevalve parlamendiliikmete poolt või õiguslike uurimisvõimetega ekspertasutuste poolt; kutsub liikmesriikide parlamente üles tagama, et sellistel järelevalvekomiteedel/-asutustel oleks luureteenistuste tõhusaks kontrollimiseks piisavalt vahendeid, tehnilist asjatundlikkust ja õiguslikke vahendeid, muu hulgas kohapealsete kontrollkäikude tegemise õigus;

77. nõuab parlamendiliikmetest ja ekspertidest koosneva töörühma loomist, et vaadata läbi läbipaistval viisil ja koostöös liikmesriikide parlamentidega soovitusel, kuidas parandada luureteenistuste demokraatlikku järelevalvet, sh parlamentaarset järelevalvet, ning suurendada järelevalvealast koostööd ELis, eriti seoses piiriülese mõõtmega; on seisukohal, et töörühm peaks eelkõige uurima võimalust kehtestada Euroopa miinimumstandardid või suunised luureteenistuse (eel- ja järel-) kontrolliks, tuginedes olemasolevatele parimatele tavadele ja rahvusvaheliste organisatsioonide (ÜRO, Euroopa Nõukogu) soovitudele, muu hulgas käsitlema probleemi, et järelevalveasutusi käsitletakse „kolmanda osapoolse sättes” või „allikakontrolli” põhimõtte kolmanda osapoolena seoses välisriikide luure järelevalve ja vastutusega, tõhustatud läbipaistvuse kriteeriumid, mis põhineksid üldisel teabele juurdepääsu põhimõttel ja nn Tshwane põhimõtetel¹, ning põhimõtted, mis puudutavad piirangute seadmist mis tahes jälgimise kestusele ja ulatusele eesmärgiga tagada, et nad oleksid proportsionaalsed ja piiritletud eesmärgiga;
78. palub kõnealusel töörühmal koostada raporti konverentsi jaoks, mille parlament kavatseb korraldada 2015. aasta alguseks koos riiklike (parlamentaarsete või sõltumatute) järelevalveasutustega, ning abistada parlamenti konverentsi ettevalmistamisel;
79. kutsub liikmesriike üles toetuma parimatele tavadele, et parandada oma järelevalveasutuste juurdepääsu teabele luuretegevuse kohta (sealhulgas salastatud teabele ja muudest teenustest pärinevale teabele) ning kehtestada õigus teostada kohapealseid külastusi, tugev ülekuulamisõiguste kogum, piisavad vahendid ja tehniline asjatundlikkus, range sõltumatus oma valitsusest ning aruandekohustus oma parlamendile;
80. kutsub liikmesriike üles arendama koostööd järelevalveasutuste seas, eelkõige Euroopa riiklike luureasutuste järelevalvekomisjonide võrgustikus (ENNIR);
81. nõuab tungivalt, et liidu välisasjade ja julgeolekupoliitika kõrge esindaja ja komisjoni asepresident annaks parlamendi asjaomastele organitele korrapäraselt aru ELi välis teenistuse alla kuuluva ELi luureandmete analüüsikeskuse (IntCen) tegevuse kohta, sealhulgas põhiõiguste ja kohaldatavate ELi andmekaitsealaste eeskirjade täieliku järgimise kohta, mis võimaldab Euroopa Parlamendil teostada ELi poliitika välismõõtmel üle paremat järelevalvet; nõuab tungivalt, et komisjon ja liidu välisasjade ja julgeolekupoliitika kõrge esindaja ja komisjoni asepresident esitaksid ettepaneku IntCeni tegevuse õigusliku aluse kohta, kui kavandatakse operatsioone või tulevase pädevusi luure valdkonnas või oma andmekogumisvahendit, mis võib mõjutada ELi sisejulgeoleku strateegiat;
82. kutsub komisjoni üles esitama 2014. detsembriks ettepaneku ELi julgeolekukontrolli korra kohta kõikidele ELi ametiisikutele, kuna praegune süsteem, mis tugineb

¹ The Global Principles on National Security and the Right to Information, juuni 2013.

päritoluliikmesriigi poolt võetud julgeolekukontrolli kohustusel, näeb ette erinevad nõuded ja menetluste kestuse riiklikes süsteemides, põhjustades seega parlamendiliikmete ja nende töötajate erinevat, rahvusest sõltuvat kohtlemist;

83. tuletab meelde Euroopa Parlamendi ja nõukogu institutsioonidevahelise kokkuleppe sätteid, mis käsitlevad nõukogu valduses oleva salastatud teabe edastamist parlamendile ja selle töötlemist parlamendi poolt seoses teemadega, mis ei kuulu ühise välis- ja julgeolekupoliitika valdkonda, mida peaks kasutama ELi tasandi järelevalve parandamiseks;

ELi ametid

84. kutsub Europoli ühist järelevalveasutust koos riiklike andmekaitseasutustega teostama enne 2014. aasta lõppu ühiskontrolli, et teha kindlaks, kas Europoliga jagatud teave ja isikuandmed on riiklike asutuste poolt seaduslikult omandatud, eelkõige see, kas teabe või andmed olid algselt omandanud ELi või kolmandate riikide luureteenistused, ning kas on rakendatud asjakohased meetmed, et takistada sellise teabe või andmete kasutamist või edasist levitamist; on seisukohal, et Europol ei tohiks töödelda teavet või andmeid, mis on saadud Euroopa Liidu põhiõiguste hartaga kaitstud põhiõigusi rikkudes;
85. palub Europolil kasutada täielikult ära oma volitusi nõuda liikmesriikide pädevatelt asutustelt kriminaaluurimise algatamist seoses suurte küberrünnakute ja IT-rikkumistega, millel on võimalikud piiriülesed tagajärjed; on veendunud, et Europoli volitusi tuleks suurendada, et võimaldada tal kahe või enama liikmesriigi või liidu organi võrgu- ja infosüsteemide pahatahtliku ründe kahtluse korral algatada ise uurimine¹; palub komisjonil läbi vaadata küberkuritegevuse vastase võitluse Euroopa keskuse tegevus ning esitada vajaduse korral ettepanek tervikliku raamistiku kohta, et suurendada küberkuritegevuse vastase võitluse Euroopa keskuse pädevusi;

Sõnavabadus

86. väljendab sügavat muret kasvavate ohtude pärast ajakirjandusvabadusele ja riigiasutuste hirmutamise halvava mõju pärast ajakirjanikele, eelkõige seoses ajakirjanduslike allikate konfidentsiaalsuse kaitsega; kordab 21. mai 2013. aasta resolutsioonis „ELi harta: ühesugused tingimused meediavabaduse tagamiseks kõikjal ELis” väljendatud nõudeid;
87. võtab teadmiseks David Miranda kinnipidamise ja tema valduses olevate materjalide arestimise Ühendkuningriigi ametivõimude poolt „Terrorismi õigusakt 2000” seitsmenda plaani alusel (ja samuti nõude ajalehele Guardian materjalid hävitada või üle anda) ning väljendab sügavat muret, et see kujutab endast võimalikku tõsist sõna- ja meediavabaduse rikkumist, nagu on sätestatud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklis 10 ja ELi harta artiklis 11, ning et terrorismivastaseks võitluseks mõeldud õigusakte võib sellises olukorras kuritarvitada;
88. juhib tähelepanu teiste õigusrikkumistest teatajate ja nende toetajate, sh nende paljastusi

¹ Euroopa Parlamendi 25. veebruari 2014. aasta seisukoht ettepanekule võtta vastu Euroopa Parlamendi ja nõukogu määrus, mis käsitleb Euroopa Liidu õiguskaitsekoostöö ja -koolituse ametit (Europol) Vastuvõetud tekstid, P7_TA(2014)0121.

uurivate ajakirjanike raskele olukorrale; palub komisjonil uurida, kas tulevase õigusakti ettepanek, millega luuakse rikkumisest teatajate tõhus ja terviklik Euroopa kaitseprogramm, mida parlament nõudis juba oma 23. oktoobri 2013. aasta resolutsioonis, peaks hõlmama ka teisi liidu pädevusvaldkondi, pöörates erilist tähelepanu rikkumisest teatamise keerukusele luurevaldkonnas; kutsub liikmesriike üles põhjalikult uurima võimalust anda õigusrikkumistest teatajatele rahvusvaheline kaitse süüdistuste eest;

89. palub liikmesriikidel tagada, et nende õigusaktid, eriti riikliku julgeoleku valdkonnas, pakuvad kuritegude avalikustamise ja neist teatamise korral (sh korruptsioon, kriminaalkuriteod, õiguslike kohustuste rikkumine, ekslik kohtumõistmine ja võimu kuritarvitamine) vaikumisele turvalist alternatiivi, mis on kooskõlas eri rahvusvaheliste (ÜRO ja Euroopa Nõukogu) instrumentidega võitluseks korruptsiooni vastu, Euroopa Nõukogu Parlamentaarset Assamblee resolutsiooniga 1729 (2010), Tshwane põhimõtetega jne;

ELi IT-turvalisus

90. juhib tähelepanu sellele, et hiljutised juhtumid näitavad selgelt ELi – eelkõige ELi institutsioonide, riikide valitsuste ja parlamentide, Euroopa oluliste ettevõtete, Euroopa IT-infrastruktuuri ja võrgustike – äärmist haavatavust kõrgetasemeliste, keerulise tarkvara ja pahavara abil teostatud rünnakute suhtes; märgib, et nende rünnakute läbiviimiseks on vajalikud sellised rahalised vahendid ja inimressursid, et need pärinevad tõenäoliselt sellistelt riigiasutustelt, kes tegutsevad välisriikide valitsuste nimel; peab sellega seoses telekommunikatsiooniettevõtte Belgacom häkkimist või pealtkuulamist murettekitavaks näiteks rünnakust ELi IT-võimekuse vastu; rõhutab, et ELi IT-võimekuse ja -turvalisuse edendamine vähendab ELi haavatavust raskete kübarrünnakute suhtes, mida korraldavad suured kuritegelikud organisatsioonid või terrorirühmitised;
91. on seisukohal, et massilise jälgimise paljastusi, mis selle kriisi tekitasid, saab Euroopa kasutada võimalusena võtta initsiatiiv ja luua esmatähtsa strateegilise meetmena tugev ja sõltumatu IT-võimekus; rõhutab, et usalduse taastamiseks peab Euroopa asjaomane IT-võimekus põhinema võimalikult suures osas avatud standarditel ning avatud tarkvaral ja võimaluse korral riistvaral, et kogu tarneahel alates protsessori disainist kuni rakendusteni oleks läbipaistev ja kontrollitav; juhib tähelepanu sellele, et IT-teenuste strateegilises sektoris konkurentsivõime taastamiseks on vaja uut Digital Deal'i sarnast algatust ning ELi institutsioonide, liikmesriikide, teadusasutuste, tööstusettevõtjate ja kodanikuühiskonna ühiseid suuri jõupingutusi; palub komisjonil ja liikmesriikidel kasutada avalikke hankeid tõukejõuna sellise ressursi võimekuse toetamiseks ELis, muutes ELi turvalisuse ja privaatsuse standardid IT-kaupade ja -teenuste põhinõudeks avalikes hangetes; nõuab seetõttu, et komisjon vaataks läbi praegused avaliku hanke tavad seoses andmetöötlusega, et kaaluda hankemenetluste piiramist sertifitseeritud ettevõtete ja võib-olla ELi ettevõtetega, kui hange on seotud julgeoleku või muude väga oluliste huvidega;
92. mõistab teravalt hukka asjaolu, et välisluureteenistused püüavad alandada IT-turvanõudeid ja paigaldada suurele hulgale IT-süsteemidele tagauksed; palub komisjonil esitada õigusakti eelnõu tagauste kasutamise keelustamise kohta õiguskaitseasutuste poolt; soovib seepärast kõikides keskkondades, kus IT-turvalisus tekitab muret,

kasutada avatud lähtekoodiga tarkvara;

93. palub liikmesriikidel, komisjonil, nõukogul ja Euroopa Ülemkogul toetada täielikult – muu hulgas teadus- ja arendustegevuse rahastamise kaudu – Euroopa innovatiivse ja tehnoloogilise suutlikkuse arengut IT-vahendite, -ettevõtete ja -teenusepakkujate (riistvara, tarkvara, teenused ja võrgud) näol, pidades muu hulgas silmas küberjulgeolekut ning krüpteerimise ja krüptograafia võimalusi; kutsub kõiki vastutavaid ELi institutsioone ja liikmesriike üles investeerima kohalikesse ja sõltumatutesse ELi tehnoloogiatesse ning arendama ja suurendama jõuliselt avastamissuutlikkust;
94. palub komisjonil, standardiseerimisasutustel ning Euroopa Liidu Võrgu- ja Infoturbeametil (ENISA) 2014. aasta detsembriks välja töötada turvalisust ja privaatsust käsitlevad miinimumnõuded ja suunised IT-süsteemidele, -võrkudele ja -teenustele, muuhulgas pilvandmetöötuse teenustele, et kaitsta paremini ELi kodanike isikuandmeid ja kõikide IT-süsteemide terviklust; usub, et sellised standardid võiksid olla aluseks uutele ülemaailmsetele standarditele ning need tuleks kehtestada avatud ja demokraatliku protsessiga, mida ei juhi üksik riik, asutus ega rahvusvaheline ettevõte; on arvamisel, et ehkki on vaja arvestada õiguspäraseid õiguskaitse- ja luurekaalutlusi, et toetada võitlust terrorismi vastu, ei tohiks need kaasa tuua IT-süsteemide usaldusväärsuse üldist nõrgestamist; toetab interneti-ehituse töökonna (IETF) hiljutisi otsuseid kaasata valitsused interneti turvalisuse ohumudelisse;
95. juhhib tähelepanu sellele, et ELi ja riiklikud telekommunikatsiooni reguleerivad asutused – ning teatavatel juhtudel ka telekommunikatsiooniettevõtted – on selgelt jätnud tähelepanuta kasutajate ja klientide IT-turvalisuse; palub komisjonil ära kasutada oma olemasolevaid e-privaatsuse ja telekommunikatsiooni raamdirektiivist tulenevaid volitusi, et tugevdada side konfidentsiaalsuse kaitset, võttes vastu meetmed, mis tagavad terminaliseadmete kokkusobivuse kasutajate õigustega kaitsta ja kontrollida oma isikuandmeid ning telekommunikatsioonivõrkude ja -teenuste kõrgetasemelise turvalisuse, sealhulgas side kaasaegse otspunktkrüpteerimise kaudu;
96. toetab ELi küberstrateegiat, kuid leiab, et see ei hõlma kõiki võimalikke ohte ning seda peaks laiendama, et hõlmata riigi pahatahtlikku käitumist; rõhutab vajadust tugevama IT-turvalisuse ja IT-süsteemide vastupanuvõime järele;
97. kutsub komisjoni üles esitama hiljemalt 2015. aasta jaanuariks tegevusplaani, et arendada IT-valdkonnas välja ELi suurem sõltumatus, muu hulgas ühtsem lähenemisviis Euroopa IT-võimekuse edendamisele (sealhulgas IT-süsteemid, seadmed, teenused, pilvandmetöötlus, krüpteerimine ja anonüümsus) ning väga tähtsa IT-infrastruktuuri kaitsele (muu hulgas seoses omandiõiguse ja haavatavusega);
98. palub komisjonil järgmise Horisont 2020 tööprogrammi raames suunata rohkem vahendeid Euroopa IT-valdkonna teadus- ja arendustegevuse, innovatsiooni ja koolituse edendamiseks, eelkõige privaatsuse täiustamise tehnoloogia ja infrastruktuuri, krüptoloogia, turvalise andmetöötuse, avatud lähtekoodidega turvalahenduste ja muude infoühiskonna teenuste edendamiseks, samuti edendada Euroopa tark- ja riistvara siseturgu, krüpteeritud kommunikatsioonivahendeid ja sideinfrastruktuuri, muu hulgas arendades välja tervikliku ELi tööstusstrateegia IT-tööstuse jaoks; on seisukohal, et väikestel ja keskmise suurusega ettevõtjatel on teadusuuringutes eriline roll; rõhutab, et ELi vahendeid ei tohiks eraldada lihtsalt IT-süsteemidele ebaseadusliku juurdepääsu

vahendite väljatöötamiseks;

99. palub komisjonil kaardistada praegused kohustused ja hiljemalt 2014. aasta detsembriks läbi vaadata ENISA, Europoli küberkuritegevuse vastase võitluse keskuse ja teiste liidu eriteadmiste keskuste, ELi infoturbeintsidentidega tegeleva rühma (CERT-EU) ja Euroopa andmekaitseinspektori (EDPS) suuremate volituste, parema kooskõlastamise ja/või täiendavate ressursside ja tehnilise võimekuse vajadus, et nad saaksid mängida võtmerolli Euroopa kommunikatsioonisüsteemide turvaliseks muutmisel, olla tõhusamad suurte IT-rikkumiste uurimisel ELis ning suurte IT-rikkumistega seotud kohapealsete tehniliste uurimiste teostamisel (või liikmesriikide ja ELi institutsioonide uurimistel abistamisel); eelkõige palub komisjonil kaaluda ENISA rolli tugevdamist ELi institutsioonide siseste süsteemide kaitsmisel ning moodustada ENISA struktuuri ELi ja liikmesriikide infoturbeintsidentidega tegelev rühm (CERT);
100. palub komisjonil ühtlasi hinnata vajadust ELi infotehnoloogia akadeemia järele, mis ühendaks kõikide seotud valdkondade parimad sõltumatud Euroopa ja rahvusvahelised asjatundjad, kelle ülesanne on anda kõigile asjaomastele ELi institutsioonidele ja asutustele teaduslikku nõu IT-tehnoloogia, sealhulgas turvastrateegiate kohta;
101. palub, et Euroopa Parlamendi sekretariaadi pädevad talitused korraldaksid parlamendi presidendi vastutusel hiljemalt 2015. aasta juuniks, esitades vahearuande hiljemalt 2014. aasta detsembriks põhjaliku parlamendi IT-turvalisuse töökindluse läbivaatamise ja hindamise, mis keskendub eelarvelistele vahenditele, inimressurssidele, tehnilisele võimekusele, sisemisele töökorraldusele ja kõikidele asjakohastele elementidele, et saavutada parlamendi IT-süsteemide kõrgetasemeline turvalisus; usub, et selline hindamine peaks tagama teabe, analüüsi ja soovitusel vähemalt alljärgneva kohta:
- vajadus korrapärase, rangete ja sõltumatute turbeauditite ja läbitungimiskatsete järele väliste turvaekspertide valimisega, kes tagavad läbipaistvuse ja tõendid kolmandate riikide suhtes võetud kohustuste või mis tahes muu huvi puudumise suhtes;
 - parimatele tavadele vastavate IT-turvalisuse/privaatsuse nõuete lisamine uute IT-süsteemide pakkumismenetlustesse, sealhulgas avatud lähtekoodiga tarkvara nõue võimaliku ostutingimusena, või kui tegemist on tundlike julgeolekuga seonduvate valdkondadega, siis usaldusväärsete Euroopa ettevõtjate hankes osalemise nõue;
 - nimekiri ettevõtetest, kellel on leping parlamendiga IT- ja sidevaldkonnas, võttes arvesse kogu teavet, mis on ilmnunud nende koostöö kohta luureasutustega (nt NSA lepingute avalikustamine ettevõttega nagu RSA, kelle tooteid Euroopa Parlament kasutab, et väidetavalt kaitsta oma liikmete ja töötajate andmete kaugjuurdepääsu), sealhulgas samade teenuste pakkumise võimalust muude, eelistatavalt Euroopa ettevõtjate poolt;
 - kogu ELi institutsioonide IT-süsteemides kasutatava tarkvara, eriti kaubandusliku valmistarkvara usaldusväärsus ja vastupidavus seoses ELi või kolmandate riikide õiguskaitse- ja luureasutuste läbitungimise ja sissetungidega, võttes samuti arvesse asjaomaseid rahvusvahelisi standardeid, parimatele tavadele vastavaid julgeolekuriskide haldamise põhimõtteid ning

julgeolekunõuete rikkumist käsitlevate ELi võrgu- ja infoturbe standardite järgimist;

- kasutada rohkem avatud lähtekoodiga süsteeme;
 - vajalikud tegevused ja meetmed selleks, et tegeleda mobiilsete töövahendite (nt nutitelefonid, tahvelarvutid) suurenenud ametialase ja isikliku kasutamise ja selle mõjuga IT-süsteemide turvalisusele;
 - parlamendi erinevate töökohtade vaheliste sidesüsteemide ja parlamendis kasutatavate IT-süsteemide turvalisus;
 - parlamendi IT-süsteemide serverite ja IT-keskuste kasutamine ja asukoht ning mõju süsteemide turvalisusele ja ühtsusele;
 - olemasolevate turvanõuete rikkumist käsitlevate eeskirjade tegelik rakendamine ning pädevate asutuste viivitamatu teavitamine üldkasutatavate sidevõrkude teenuste osutajate poolt;
 - pilvandmetöötluse ja pilvepõhiste salvestamisteenuste kasutamine parlamendi poolt, sh mis laadi andmeid salvestatakse, kuidas on sisu ja juurdepääs kaitstud ning kus pilveteenuse serverid asuvad, selgitades kohaldatavat andmekaitse ja luure õigusraamistikku ning hinnates võimalust kasutada ainult ELi territooriumil asuvaid pilveteenuste servereid;
 - krüptograafiliste tehnoloogiate suuremat kasutamist võimaldav kava, eelkõige kõikide IT- ja sideteenuste, nagu pilvandmetöötlus, e-post, kiirsõnumid ja telefoniside, otsast lõpuni autenditud krüpteerimine;
 - elektroonilise allkirja kasutamine e-kirjades;
 - e-kirjade krüpteerimise vaikestandardi (nt GNU Privacy Guard) kasutamise kava, võimaldamaks samal ajal ka digiallkirja kasutamist;
 - turvalise kiirsõnumiteenuse loomine parlamendis, mis võimaldaks turvalist suhtlemist, nii et server näeb ainult krüpteeritud sisu;
102. nõuab, et ELi institutsioonid ja asutused viiksid koostöös ENISA, Europol ja CERTidega läbi sarnase hindamise hiljemalt 2015. aasta juuniks, esitades vahearuande hiljemalt 2014. aasta detsembriks, eelkõige Euroopa Ülemkogu, Euroopa Nõukogu, Euroopa välisteenistus (sealhulgas ELi delegatsioonid), komisjon, Euroopa Kohus ja Euroopa Keskpank; kutsub liikmesriike üles korraldama sarnast hindamist;
103. rõhutab, et tuleks teha ELi välisteenistuse eelarveliste vajadustega seotud hindamine ja võtta viivitamatult esmased meetmed ning eraldada asjakohased rahalised vahendid 2015. aasta eelarveprojekti;
104. on seisukohal, et vabadusel, turvalisusel ja õigusel rajaneval alal kasutatavad suured IT-süsteemid, nagu teise põlvkonna Schengeni infosüsteem, viisainfosüsteem, Eurodac ja võimalikud tulevased süsteemid, nagu ELi reisiloa elektrooniline süsteem, tuleks välja töötada ja rakendada sellisel viisil, mis tagavad, et andmeid ei seata ohtu kolmandate

riikide asutuste nõudmiste tulemusel; nõuab, et vabadusel, turvalisusel ja õigusel rajaneva ala suuremahuliste IT-süsteemide operatiivjuhtimise Euroopa amet (eu-LISA) esitaks 2014. aasta lõpuks Euroopa Parlamendile aruande olemasolevate süsteemide usaldusväärsuse kohta;

105. kutsub komisjoni ja Euroopa välisteenistust võtma meetmeid rahvusvahelisel tasandil, eelkõige koos ÜROga, ja koostöös huvitatud osapooltega rakendama ELi strateegiat interneti demokraatlikuks haldamiseks, et vältida üksikisiku, ettevõtte või riigi sobimatut mõju ICANNi ja IANA tegevusele, tagades asjakohase esindatuse kõikidele huvitatud osalistele nendes asutustes ning vältides samas riigipoolse kontrolli või tsensuuri hõlbustamist või interneti nn balkaniseerumist ja killustumist;
106. nõuab, et EL võtaks juhtpositsiooni interneti struktuuri ja juhtimise ümberkujundamisel, et käsitleda andmevoogude ja -salvestamisega seotud ohte, püüeldes andmete vähendamise ja läbipaistvuse ning vähem tsentraliseeritud toorandmete massilise säilitamise poole, samuti internetiliikluse ümbersuunamise või kogu internetiliikluse täieliku otspunktkrüpteerimise suunas, et vältida praegusi riske, mis on seotud liikluse põhjendamatu suunamisega läbi nende riikide territooriumide, kes ei vasta põhiõiguste, andmekaitse ja privaatsuse põhistandarditele;
107. nõuab järgmiste valdkondade edendamist:
 - ELi otsingumootorid ja suhtlusvõrgud, mis oleks väga oluline samm ELi IT-sõltumatuse suunas;
 - Euroopa IT-teenuste osutajad;
 - üldise teabevahetuse, sealhulgas e-posti ja SMS-side krüpteerimine;
 - Euroopa infotehnoloogia põhielemendid, näiteks klientide serverite operatsioonisüsteemide lahendused, kasutades avatud lähtekoodi standardeid, ja Euroopa võrguühenduselementide, näiteks ruuterite arendamine;
108. palub komisjonil esitada seadusandlik ettepanek ELi marsruutimissüsteemi kohta, sh salvestatud kõneandmete töötlemine ELi tasandil, mis kujutab endast interneti allsüsteemi ja ei laiene väljapoole ELi piire; märgib, et kõiki marsruutimis- ja salvestatud kõneandmeid tuleks töödelda kooskõlas ELi õigusraamistikuga;
109. kutsub liikmesriike koostöös ENISA, Europol'i küberkuritegude keskuse, CERTide ning riiklike andmekaitseasutuste ja küberkuritegude üksustega üles arendama turbekultuuri ning alustama hariduse ja teadlikkuse tõstmise kampaaniat, et võimaldada kodanikel teha teadlikumaid valikuid, milliseid isikuandmeid sisestada internetti ja kuidas neid andmeid paremini kaitsta, muu hulgas krüpteerimise ja turvalise pilvandmetöötluse abil, kasutades täielikult ära universaalteenuste direktiivis sätestatud avaliku huvi teabeplatvormi;
110. nõuab, et komisjon esitaks 2014. aasta detsembriks seadusandlikud ettepanekud, et julgustada tark- ja riistvara tootjaid võtma kasutusele disaini- ja vaikeomaduste poolest turvalisemad ja eraelu kaitsvad tooted, muu hulgas kehtestades stiimulid isikuandmete põhjendamatu ja ebaproportsionaalse kogumise vältimiseks, tootjatele õigusliku vastutuse seoses lappimata teadaolevate turvaaukude, vigase või mitteturvalise tarkvara

ja salajaste tagauste paigaldamisega, mis võimaldavad andmetele lubamatut juurdepääsu ja nende töötlemist; palub sellega seoses komisjonil hinnata IT-riistvara sertifitseerimis- või valideerimissüsteemi, sh ELi tasandi katsetamismenetluste loomise võimalust, et tagada toodete terviklus ja turvalisus;

Usalduse taastamine

111. usub, et lisaks vajadusele muutuste järele seadusandluses on küsitlus näidanud USA vajadust taastada usaldus oma ELi partnerite seas, kuna kõne all on eeskätt USA luureasutuste tegevus;
112. juhib tähelepanu, et usalduskriis laieneb:
 - ELi-sisesele koostöövalmidusele, kuna mõned riiklikud luuretegevused võivad ohustada liidu eesmärkide saavutamist;
 - kodanikele, kes saavad aru, et mitte ainult kolmandad riigid või rahvusvahelised ettevõtted, vaid ka nende oma valitsused võivad nende järele luurata;
 - austusele põhiõiguste, demokraatia ning õigusriigi põhimõtete vastu ning demokraatlike, kohtulike ja parlamentaarsete tagatiste ning järelevalve usaldusväärsusele digitaalses ühiskonnas;

ELi ja USA vahel

113. tuletab meelde olulist ajaloolist ja strateegilist partnerlust ELi liikmesriikide ja USA vahel, mis põhineb ühisel usul demokraatiasse, õigusriiki ja põhiõigustesse;
114. usub, et kodanike massiline jälgimine ja poliitiliste juhtide järel luuramine USA poolt on põhjustanud tõsist kahju ELi ja USA suhetele ning mõjutanud ebasoodsalt ELis tegutsevate USA organisatsioonide usaldusväärsust; olukorda halvendavad täiendavalt õigus- ja haldusabivahendite puudumine ELi kodanikele hüvitise määramiseks US õigusaktide kohaselt, eelkõige luure eesmärgil jälgimise juhtumite puhul;
115. tunnistab, et arvestades ülemaailmseid väljakutseid, millega EL ja USA kokku puutuvad, tuleb Atlandi-ülest partnerlust täiendavalt tugevdada, ning et on ülitähtis, et jätkuks Atlandi-ülene koostöö terrorismivastases võitluses, võttes uueks aluseks õigusriigi põhimõtte ühisel austamisel põhineva usalduse ja igasuguse valimatu massilise jälgimise keelustamise; rõhutab seega, et USA peab võtma selgeid meetmeid usalduse taastamiseks ja uuesti rõhutama partnerluse aluseks olevaid ühiseid põhiväärtusi;
116. on valmis pidama dialoogi USA partneritega, et jätkuvas Ameerika avalikus ja kongressisisises arutelus jälgimise reformi ja luure järelevalve läbivaatamise üle käsitletaks ELi kodanike, elanike ja muude ELi õigusega kaitstud isikute eraelu puutumatuse õigust ja muid õigusi, et USA kohtutes oleks tagatud võrdse teabe õigused ja eraelu puutumatuse, muu hulgas õiguskaitse, kasutades selleks näiteks andmekaitseseaduse ning elektroonilise side andmekaitseseaduse läbivaatamist ning kodaniku- ja poliitiliste õiguste rahvusvahelise pakti esimese fakultatiivprotokolli ratifitseerimist, nii et praegust diskrimineerimist ei põlistataks;

117. rõhutab, et tuleb teha vajalikke reforme ja anda eurooplastele tõhusad garantiid, et tagada, et jälgimine ja andmetöötlus välismaise luure eesmärkidel on proportsionaalne ja piiratud selgelt kindlaks määratud tingimustega ja seotud mõistliku kahtlusega ning tõenäolise terroristliku tegevusega; rõhutab, et selle eesmärgi suhtes tuleb kohaldada läbipaistvat kohtulikku järelevalvet;
118. leiab, et meie Ameerika partneritelt on vaja selgeid signaale, et tõendada, et USA eristab liitlasi ja vaenlasi;
119. nõuab tungivalt, et komisjon ja USA valitsus käsitleksid jätkuvate õiguskaitse eesmärgil andmete edastamise raamlepingut käsitlevate ELi ja USA läbirääkimiste raames ELi kodanike teabe- ja kohtuliku kaitse õigusi ning viiksid kõnealused läbirääkimised vastavalt ELi ja USA justiits- ja siseministrite 18. novembri 2013. aasta kohtumisel võetud kohustusele lõpule enne 2014. aasta suve;
120. julgustab USAd liituma Euroopa Nõukogu isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooniga (konventsioon nr 108), nagu ta liitus 2001. aasta küberkuritegevuse konventsiooniga, tugevdades seega Atlandi-üleste liitlaste ühist õiguslikku alust;
121. kutsub ELi üles uurima võimalust kehtestada koos USAga käitumisjuhend, mis tagaks, et USA ei teostaks luuretegevust ELi institutsioonide ja asutuste vastu;

Euroopa Liidus

122. on samuti veendunud, et ELi liikmesriikide osalemine ja meetmed on viinud usalduse kadumiseni muu hulgas liikmesriikide vahel ning kodanike ja riiklike ametiasutuste vahel; on arvamisel, et ainult täielik selgus jälgimise eesmärkide ja vahendite küsimuses, avalik arutelu ja lõpuks õigusaktide läbivaatamine, sh massilise jälgimistegevuse lõpetamine ja kohtuliku ja parlamentaarse järelevalvesüsteemi tugevdamine, võivad taastada kaotatud usalduse; rõhutab taas ELi tervikliku julgeolekupoliitika väljaarendamisega seotud raskusi, kui toimub selline massiline jälgimine, ning rõhutab, et ELi usaldusliku koostöö põhimõtte nõuab, et liikmesriigid hoiduksid luuretegevusest teiste liikmesriikide territooriumil;
123. märgib, et mõni liikmesriik on kahepoolses suhtluses USA ametiasutustega seoses väidetava luuramisega ja et mõni neist (Ühendkuningriik) on sõlminud nn luuramisvastased kokkulepped või näevad ette nende sõlmimist (Saksamaa, Prantsusmaa); toonitab, et need liikmesriigid peavad täiel määral jälgima ELi kui terviku huvisid ja õigusraamistikku; peab selliseid kahepoolseid kokkuleppeid takistavaks ja asjakohatuks, võttes arvesse vajadust käsitleda seda probleemi Euroopa tasandil; palub, et nõukogu teavitaks parlamenti liikmesriikide poolsetest arengutest üleeuroopalise vastastikuse luuramise keelustamise kokkuleppe suunas;
124. leiab, et sellised kokkulepped ei tohiks rikkuda liidu aluslepinguid, eriti lojaalse koostöö põhimõtet (Euroopa Liidu lepingu artikli 4 lõige 3), ega õõnestada ELi poliitikat üldiselt ning konkreetsemalt siseturgu, õiglast konkurentsi ning majanduslikku, tööstuslikku ja sotsiaalset arengut; otsustab kõik asjaomased kokkulepped läbi vaadata, et need oleksid kooskõlas Euroopa Liidu õigusega, ja jätab endale õiguse aktiveerida aluslepingus sätestatud menetlused juhul, kui tõendatakse, et kõnealused kokkulepped lähevad vastuollu liidu sidusus- või aluspõhimõtetega, millel see põhineb;

125. palub liikmesriikidel teha suuri jõupingutusi, et tagada parem koostöö eesmärgiga pakkuda kaitset luuramise vastu koostöös asjaomaste ELi organite ja ametitega, et kaitsta ELi kodanikke ja institutsioone, Euroopa ettevõtteid, ELi tööstust, IT-infrastruktuuri ja võrke, samuti Euroopa teadust; on seisukohal, et ELi sidusrühmade aktiivne osalemine on tulemusliku teabevahetuse eeltingimus; toonitab, et julgeolekuohud on muutunud rahvusvahelisemaks, levinumaks ja keerukamaks ning see nõuab tõhustatud koostööd Euroopa tasandil; on veendunud, et selline areng peaks paremini kajastuma aluslepingutes, ning seetõttu nõuab aluslepingute läbivaatamist, et tugevdada liikmesriikide ja liidu vahelise usaldusliku koostöö ideed seoses turvalise ala saavutamise ja vältida liikmesriikide vastastikust luuretegevust liidus;
126. peab tingimata vajalikuks, et kõikidel asjaomastel ELi institutsioonidel ja ELi delegatsioonidel oleksid olemas pealtkuulamiskindlad sidesüsteemid (e-post ja telekommunikatsioonivahendid, sh laua- ja mobiiltelefonid) ning pealtkuulamiskindlad koosolekuruumid; nõuab seetõttu ELi krüpteeritud sise-e-posti süsteemi loomist;
127. palub, et komisjon nõustuks viivitamata Euroopa Parlamendi 23. mai 2012. aasta ettepanekuga võtta vastu Euroopa Parlamendi määrus erisätete kohta, millega reguleeritakse Euroopa Parlamendi uurimisõiguse kasutamist ning tunnistatakse kehtetuks Euroopa Parlamendi, nõukogu ja komisjoni otsus 95/167/EÜ, Euratom, ESTÜ, mis esitati ELi toimimise lepingu artikli 226 alusel; nõuab aluslepingu läbivaatamist, et laiendada selliseid uurimisõigusi, nii et need hõlmaksid ilma piirangute ja eranditeta kõiki liidu pädevus- ja tegevusalasid ning sisaldaksid võimalust isikuid vande all küsitleda;

Rahvusvahelisel tasandil

128. kutsub komisjoni üles esitama hiljemalt 2015. aasta jaanuariks interneti demokraatliku juhtimise ELi strateegiat;
129. kutsub liikmesriike üles järgima andmekaitse ja eraelu puutumatuse eest vastutavate volinike 35. rahvusvahelise konverentsi üleskutset pooldada lisaprotokolli vastuvõtmist kodaniku- ja poliitiliste õiguste rahvusvahelise pakti artiklile 17, mis peaks põhinema standarditel, mis on välja töötatud ja heaks kiidetud rahvusvahelise konverentsi poolt, ja pakti juurde kuuluva inimõiguste komitee üldise märkuse nr 16 sätetel, et luua ülemaailmselt kohaldatavad standardid andmekaitse ja eraelu puutumatuse kaitsmiseks kooskõlas õigusriigi põhimõttega; palub, et liikmesriigid nõuaksid seejuures ka ÜRO rahvusvahelist allasutust, mille ülesandeks oleks eeskätt jälgida seiresüsteemide väljatöötamist ning reguleerida ja uurida nende kasutamist; palub kõrgel esindajal ja komisjoni asepresidendil ning Euroopa välisteenistusel võtta kasutusele proaktiivne lähenemisviis;
130. kutsub liikmesriike üles töötama ÜROs välja sidusat ja tugevat strateegiat, toetades eelkõige resolutsiooni „Õigus eraelu puutumatusele digitaalajastul”, mille algatasid Brasiilia ja Saksamaa ning mille ÜRO Peaassamblee kolmas komitee (inimõiguste komitee) 27. novembril 2013 vastu võttis, samuti võtma rahvusvahelisel tasandil täiendavaid meetmeid eraelu puutumatuse ja andmekaitsega seotud põhiõiguste kaitsmiseks, vältides samal ajal riigipoolse kontrolli või tsensuuri hõlbustamist ja interneti killustumist, muu hulgas tegema algatust rahvusvaheliseks lepinguks, millega keelustatakse massiline jälgimistegevus ning luuakse amet selle järelevalveks;

Prioriteetide kava: Euroopa digitaalne habeas corpus – põhiõiguste kaitsmine digitaalajastul

131. otsustab esitada ELi kodanikele, institutsioonidele ja liikmesriikidele üldmainitud soovitusel prioriteetide kavana parlamendi järgmiseks ametiajaks; palub komisjonil ja käesolevas resolutsioonis nimetatud teistel ELi institutsioonidel, organitel, ametitel ja asutustel, kooskõlas Euroopa Liidu toimimise lepingu artikliga 265, toimida vastavalt käesolevas resolutsioonis esitatud soovitudele ja taotlustele;
132. otsustab käivitada kava „Euroopa digitaalne *habeas corpus* – põhiõiguste kaitsmine digitaalajastul”, mis põhineb järgmisel kaheksal meetmel, mille rakendamise üle ta järelevalvet teostab:
- Meede 1. Võtta 2014. aastal vastu andmekaitsepakett;
 - Meede 2. Sõlmida ELi ja USA raamleping, mis kindlustab kodanike põhiõiguse eraelu puutumatusele ja andmekaitsele ning tagab ELi kodanikele nõuetekohased hüvitusemehhanismid, muu hulgas andmeedastuse puhuks ELilt USA-le õiguskaitse eesmärgil;
 - Meede 3. Peatada programm Safe Harbor, kuni on tehtud täielik läbivaatamine ja praegused lüngad on parandatud, kindlustades, et isikuandmete edastamine ärielistel eesmärkidel liidult USA-le võib toimuda ainult kõrgeimaid ELi standardeid järgides;
 - Meede 4. Peatada TFTP-leping kuni (i) raamlepingu läbirääkimised on lõpule viidud; (ii) lõpule on viidud põhjalik uurimine ELi analüüsi põhjal ja nõuetekohaselt on käsitletud kõiki muresid, mille parlament tõstatas oma 23. oktoobri 2013. aasta resolutsioonis;
 - Meede 5. Hinnata kõiki isikuandmetega seonduvaid kokkuleppeid ja mehhanisme või teabevahetust kolmandate riikidega, tagamaks, et jälgimistegevusega ei kahjustata õigust eraelu puutumatusele ja isikuandmete kaitsele, ning võtta vajalikke järelemeetmeid;
 - Meede 6. Kaitsta õigusriigi põhimõtet ja ELi kodanike põhiõigusi (muu hulgas ajakirjandusvabaduse ohtude eest), üldsuse õigust saada erapooletut teavet ja ametialast konfidentsiaalsust (sealhulgas advokaadi ja kliendi suhteid) ning tagada rikkumistest teavitajate tõhustatud kaitse;
 - Meede 7. Töötada välja suurema IT-sõltumatuse Euroopa strateegia (uus Digital Deal) sarnane algatus koos piisavate vahendite eraldamisega riiklikul ja ELi tasandil), et edendada IT-tööstust ning võimaldada Euroopa ettevõtetel kasutada ära ELi eraelu puutumatuse valdkonna konkurentsieelist;
 - Meede 8. Arendada ELi olulist rolli interneti demokraatlikul ja neutraalsel juhtimisel;
133. palub ELi institutsioonidel ja liikmesriikidel edendada kava „Euroopa digitaalne *habeas corpus* – põhiõiguste kaitsmine digitaalajastul”; võtab endale kohustuse toimida ELi kodanike õiguste kaitsjana järgmise ajakavaga rakendamise jälgimiseks:

- aprill–märts 2015: järelevalverühm, mis põhineb kodanikuvabaduste, justiits- ja siseasjade komisjoni uurimisrühmal, mis vastutab kõigi uute paljastuste jälgimise eest seoses uurimise mandaadi ja käesoleva resolutsiooni rakendamise kontrollimisega;
- alates juulist 2014: alaline järelevalvemehhanism andmeedastuse ja kohtuliku hüvitise jaoks pädeva komisjoni raames;
- kevad 2014: ametlik üleskutse Euroopa Ülemkogule lisada „Euroopa digitaalne *habeas corpus* – põhiõiguste kaitsmine digitaalajastul” suunistesse, mis võetakse vastu Euroopa Liidu toimimise lepingu artikli 68 alusel;
- sügis 2014: kohustuse võtmine, et „Euroopa digitaalne *habeas corpus* – põhiõiguste kaitsmine digitaalajastul” ja seonduvad soovitusel toimivad peamiste kriteeriumidena järgmise komisjoni heakskiitmiseks;
- 2014: konverents, mis toob kokku kõrgetasemelised Euroopa eksperdid erinevates IT-turvalisust soodustavates valdkondades (sealhulgas matemaatika, krüptograafia ja eraelu puutumatust soodustavad tehnoloogiad), et aidata edendada ELi IT-strateegiat järgmise parlamendi ametiaja jaoks;
- 2014–2015: usaldus- / andmekaitse- / kodanike õiguste rühm tuleb kutsuda kokku korrapäraselt Euroopa Parlamendi ja USA Kongressi vahel ning teiste kohustuse võtnud kolmandate riikide (sh Brasiilia) parlamentidega;
- 2014–2015: konverents Euroopa riiklike parlamentide luurejärelevalveorganitega;

o
o o

134. teeb presidendile ülesandeks edastada käesolev resolutsioon Euroopa Ülemkogule, nõukogule, komisjonile, liikmesriikide parlamentidele ja valitsustele, riiklikele andmekaitseasutustele, Euroopa andmekaitseinspektorile, eu-LISA-le, ENISA-le, Euroopa Liidu Põhiõiguste Ametile, artikli 29 töörühmale, Euroopa Nõukogule, Ameerika Ühendriikide Kongressile, USA valitsusele, Brasiilia Liitvabariigi presidendile, valitsusele ja parlamendile ning ÜRO peasekretärile;
135. teeb kodanikuvabaduste, justiits- ja siseasjade komisjonile ülesandeks pöörduda selle küsimusega täiskogu istungjärgul parlamendi poole aasta pärast käesoleva resolutsiooni vastuvõtmist; peab väga oluliseks hinnata, mil määral on järgitud Euroopa Parlamendi poolt vastu võetud soovitusi, ja analüüsida kõiki juhtusid, kui neid soovitusi ei ole järgitud.