Onsdagen den 12 mars 2014

P7_TA(2014)0230

Amerikanska NSA:s övervakningsprogram, övervakningsorgan i olika medlemsstater samt inverkan på EU-medborgarnas grundläggande rättigheter

Europaparlamentets resolution av den 12 mars 2014 om amerikanska NSA:s övervakningsprogram, övervakningsorgan i olika medlemsstater samt inverkan på EU-medborgarnas grundläggande rättigheter och på det transatlantiska samarbetet i rättsliga och inrikes frågor (2013/2188(INI))

(2017/C 378/14)

Europaparlamentet utfärdar denna resolution

— med beaktande av fördraget om Europeiska unionen (EU-fördraget), särskilt artiklarna 2, 3, 4, 5, 6, 7, 10, 11 och 21,

— med beaktande av fördraget om Europeiska unionens funktionssätt (EUF-fördraget), särskilt artiklarna 15, 16 och 218 samt avdelning V,

— med beaktande av protokoll 36 om övergångsbestämmelser och artikel 10 i detta samt förklaring nr 50 om detta protokoll,

— med beaktande av Europeiska unionens stadga om de grundläggande rättigheterna, särskilt artiklarna 1, 3, 6, 7, 8, 10, 11, 20, 21, 42, 47, 48 och 52,

— med beaktande av Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (nedan kallad Europakonventionen), särskilt artiklarna 6, 8, 9, 10 och 13 samt protokollen till denna,

— med beaktande av den allmänna förklaringen om de mänskliga rättigheterna, särskilt artiklarna 7, 8, 10, 11, 12 och 14 ([1]),

— med beaktande av Internationella konventionen om medborgerliga och politiska rättigheter, särskilt artiklarna 14, 17, 18 och 19,

— med beaktande av Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (ETS nr 108) och tilläggsprotokollet av den 8 november 2001 till denna konvention om tillsynsmyndigheter och gränsöverskridande flöden av personuppgifter (ETS nr 181),

— med beaktande av Wienkonventionen om diplomatiska förbindelser, särskilt artiklarna 24, 27 och 40,

— med beaktande av Europarådets konvention om it-brottslighet (ETS nr 185),

— med beaktande av den rapport från FN:s särskilda rapportör om främjande och skydd av mänskliga grundläggande fri- och rättigheter i samband med terrorismbekämpning som lades fram den 17 maj 2010 ([2]),

— med beaktande av kommissionens meddelande ”Internetpolitik och förvaltning av internet – Europas roll i utformningen av framtidens internetförvaltning” (COM(2014)0072),

— med beaktande av den rapport från FN:s särskilda rapportör om främjande och skydd av åsikts- och yttrandefriheten som lades fram den 17 april 2013 ([3]),

— med beaktande av de riktlinjer beträffande mänskliga rättigheter och kampen mot terrorism som antogs av Europarådets ministerkommitté den 11 juli 2002,

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

— med beaktande av Brysseldeklarationen av den 1 oktober 2010, som antogs vid de parlamentariska utskottens sjätte konferens om kontroll av underrättelse- och säkerhetstjänsterna i Europeiska unionens medlemsstater,

— med beaktande av resolution nr 1954 (2013) från Europarådets parlamentariska församling om nationell säkerhet och tillgång till information,

— med beaktande av den rapport om demokratisk kontroll av säkerhetstjänster som antogs av Venedigkommissionen den 11 juni 2007 ([1]), samt i väntan på och med stort intresse för uppdateringen av denna rapport som ska vara klar våren 2014,

— med beaktande av vittnesmålen från företrädarna för tillsynskommittéerna om Belgiens, Nederländernas, Danmarks och Norges underrättelsetjänster,

— med beaktande av de ärenden som lagts fram inför fransk ([2]), polsk och brittisk ([3]) domstol samt inför Europeiska domstolen för de mänskliga rättigheterna ([4]), med avseende på system för massövervakning,

— med beaktande av konventionen, upprättad av rådet på grundval av artikel 34 i fördraget om Europeiska unionen, om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater ([5]), särskilt avdelning III i denna,

— med beaktande av kommissionens beslut 2000/520/EG av den 26 juli 2000 om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (Safe Harbour Privacy Principles) i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat,

— med beaktande av kommissionens utvärderingsrapporter av den 13 februari 2002 (SEC(2002)0196) och av den 20 oktober 2004 (SEC(2004)1323) om genomförandet av principerna om integritetsskydd (Safe Harbour Privacy Principles),

— med beaktande av kommissionens meddelande av den 27 november 2013 om hur principerna om integritetsskydd (safe harbour) fungerar när det gäller EU:s medborgare och företag som är etablerade i EU (COM(2013)0847) samt av kommissionens meddelande av den 27 november 2013 om återskapande av förtroendet för dataflöden mellan EU och Förenta staterna (COM(2013)0846),

— med beaktande av sin resolution av den 5 juli 2000 om utkastet till kommissionens beslut om huruvida Förenta staternas safe harbour-principer ger ett adekvat skydd samt tillhörande frågor och svar som utfärdats av Förenta staternas handelsministerium, som ansåg att det inte kunde bekräftas om systemet var adekvat eller inte ([6]), samt av yttrandena från artikel 29-gruppen, särskilt yttrande nr 4/2000 av den 16 maj 2000 ([7]),

— med beaktande av avtalen mellan Amerikas förenta stater och Europeiska unionen om användning och överföring av passageraruppgifter (PNR-avtalen) från 2004, 2007 ([8]) och 2012 ([9]),

— med beaktande av den gemensamma översynen av genomförandet av avtalet mellan Europeiska unionen och Amerikas förenta stater om behandling av passageraruppgifter (PNR) och överföring av dessa till Förenta staternas Department of Homeland Security (DHS) ([10]) – följedokument till rapporten från kommissionen till Europaparlamentet och rådet om den gemensamma översynen (COM(2013)0844),

---

([1]) http://www.venice.coe.int/webforms/documents/CDL-AD(2007)016.aspx
([2]) La Fédération Internationale des Ligues des Droits de l'Homme och La Ligue française pour la défense des droits de l'Homme et du Citoyen mot X; Tribunal de Grande Instance i Paris.
([3]) Målen Privacy International och Liberty i Investigatory Powers Tribunal (domstol med utredningsbefogenheter).
([4]) De förenade målen på grundval av artikel 34, Big Brother Watch, Open Rights Group, English Pen Dr Constanze Kurz (kärande) mot Förenade kungariket (svarande).
([5]) EGT C 197, 12.7.2000, s. 1.
([6]) EGT C 121, 24.4.2001, s. 152.
([7]) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp32en.pdf
([8]) EUT L 204, 4.8.2007, s. 18.
([9]) EUT L 215, 11.8.2012, s. 5.
([10]) SEC(2013)0630, 27.11.2013.

Onsdagen den 12 mars 2014

— med beaktande av generaladvokat Pedro Cruz Villalóns ståndpunkt att hela direktiv 2006/24/EG om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät är oförenligt med artikel 52.1 i Europeiska unionens stadga om de grundläggande rättigheterna samt att artikel 6 i direktivet är oförenlig med artiklarna 7 och 52.1 i stadgan ([1]),

— med beaktande av rådets beslut 2010/412/EU av den 13 juli 2010 om ingående av avtalet mellan Europeiska unionen och Amerikas förenta stater om behandling och överföring av uppgifter om finansiella betalningsmeddelanden från Europeiska unionen till Förenta staterna i enlighet med programmet för att spåra finansiering av terrorism (TFTP) ([2]), samt de bifogade förklaringarna från kommissionen och rådet,

— med beaktande av avtalet om ömsesidig rättslig hjälp mellan Europeiska unionen och Amerikas förenta stater ([3]),

— med beaktande av de pågående förhandlingarna om ett internationellt ramavtal mellan EU och Förenta staterna om skydd av personuppgifter som överförs och behandlas för att förebygga, utreda, avslöja eller lagföra brott, inklusive terrorism, inom ramen för polissamarbete och straffrättsligt samarbete (paraplyavtalet),

— med beaktande av rådets förordning (EG) nr 2271/96 av den 22 november 1996 om skydd mot följderna av tillämpning av extraterritoriell lagstiftning som antas av ett tredje land, och åtgärder som grundar sig på eller är en följd av denna lagstiftning ([4]),

— med beaktande av det uttalande som presidenten för Förbundsrepubliken Brasilien gjorde vid öppnandet av FN:s generalförsamlings 68:e session den 24 september 2013 och det utförda arbetet i det parlamentariska utskott för spioneriutredning som inrättats av Brasiliens senat,

— med beaktande av USA PATRIOT Act, som undertecknades av president George W. Bush den 26 oktober 2001,

— med beaktande av Foreign Intelligence Surveillance Act (FISA) från 1978 och ändringsakten till denna från 2008,

— med beaktande av dekret nr 12333, som utfärdades av Förenta staternas president 1981 och som ändrades 2008,

— med beaktande av den amerikanska presidentens policydirektiv (Presidential Policy Directive, PPD-28) om signalspaning, utfärdat av Förenta staternas president Barack Obama den 17 januari 2014,

— med beaktande av de lagstiftningsförslag som för närvarande utreds i Förenta staternas kongress, inklusive utkastet till Förenta staternas Freedom Act, utkastet till Intelligence Oversight and Surveillance Reform Act, med flera,

— med beaktande av de översyner som genomförts av tillsynsnämnden på området personlig integritet och medborgerliga fri- och rättigheter (Privacy and Civil Liberties Oversight Board), Förenta staternas nationella säkerhetsråd och presidentens grupp för tillsyn av underrättelse- och kommunikationsteknik, särskilt den sistnämndas rapport *Liberty and Security in a Changing World* av den 12 december 2013,

— med beaktande av amerikanska District of Columbias distriktsdomstols dom av den 16 december 2013 i civilmål nr 13-0851, Klayman m.fl. mot Obama m.fl., och med beaktande av avgörandet från den amerikanska distriktsdomstolen för Southern District of New York i målet ACLU m.fl. mot James R. Clapper m.fl. (civilmål nr 13-3994 av den 11 juni 2013),

— med beaktande av rapporten från EU:s medordförande i den tillfälliga EU–USA-arbetsgruppen om dataskydd av den 27 november 2013 ([5]),

---

([1]) Yttrande från generaladvokat Pedro Cruz Villalón av den 12 december 2013 i mål C-293/12.
([2]) EUT L 195, 27.7.2010, s. 3.
([3]) EUT L 181, 19.7.2003, s. 34.
([4]) EGT L 309, 29.11.1996, s. 1.
([5]) Rådets dokument 16987/2013.

— med beaktande av sina resolutioner av den 5 september 2001 ([1]) och 7 november 2002 ([2]) om det världsomfattande systemet för avlyssning av privatpersoner och företag (avlyssningssystemet Echelon),

— med beaktande av sin resolution av den 21 maj 2013 om EU-stadgan: standarder för mediefrihet i EU ([3]),

— med beaktande av sin resolution av den 4 juli 2013 om den amerikanska säkerhetsmyndigheten NSA:s övervakningsprogram och övervakningsorgan i olika medlemsstater och konsekvenserna för EU-medborgarnas integritet ([4]), i vilken utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor uppmanas att göra en ingående utredning av frågan,

— med beaktande av arbetsdokument 1 om Förenta staternas och EU:s övervakningsprogram och deras inverkan på EU-medborgarnas grundläggande rättigheter,

— med beaktande av arbetsdokument 3 om förhållandet mellan övervakningsmetoder i EU och Förenta staterna samt EU:s bestämmelser om uppgiftsskydd,

— med beaktande av arbetsdokument 4 om Förenta staternas övervakning av data och uppgifter inom EU och eventuella juridiska konsekvenser för transatlantiska avtal och samarbeten,

— med beaktande av arbetsdokument 5 om demokratisk översyn av medlemsstaternas underrättelsetjänster och av EU:s underrättelseorgan,

— med beaktande av AFET-utskottets arbetsdokument om de utrikespolitiska aspekterna av granskningen av den elektroniska massövervakningen av EU:s medborgare,

— med beaktande av sin resolution av den 23 oktober 2013 om organiserad brottslighet, korruption och penningtvätt: rekommendationer med avseende på de åtgärder och initiativ som ska vidtas ([5]),

— med beaktande av sin resolution av den 23 oktober 2013 om tillfälligt upphävande av TFTP-avtalet till följd av NSA:s övervakning ([6]),

— med beaktande av sin resolution av den 10 december 2013 om att frigöra de molnbaserade datortjänsternas potential i Europa ([7]),

— med beaktande av det interinstitutionella avtalet mellan Europaparlamentet och rådet om överförande till och hantering inom Europaparlamentet av säkerhetsskyddsklassificerade uppgifter som innehas av rådet vilka rör andra frågor än de som omfattas av den gemensamma utrikes- och säkerhetspolitiken ([8]),

— med beaktande av bilaga VIII till arbetsordningen,

— med beaktande av artikel 48 i arbetsordningen,

— med beaktande av betänkandet från utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor (A7-0139/2014), och av följande skäl:

Effekten av massövervakningen

A. Skyddet av personuppgifter och privatliv hör till de grundläggande rättigheterna. Säkerhetsåtgärder, även åtgärder för att bekämpa terrorism, måste därför utformas så att de är förenliga med rättsstatsprincipen och underkastade skyldigheterna avseende de grundläggande rättigheterna, inklusive sådana som avser privatlivet och skyddet av personuppgifter.

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

Onsdagen den 12 mars 2014

B. Informationsflöden och uppgifter som i dag präglar vardagslivet och ingår i varje individs personliga sfär måste vara lika intrångsskyddade som privata hem.

C. Banden mellan Europa och Amerikas förenta stater bygger på en anda av och principerna om demokrati, rättsstatlighet, frihet, rättvisa och solidaritet.

D. Samarbetet mellan Förenta staterna och Europeiska unionen och dess medlemsstater i kampen mot terrorismen är alltjämt avgörande för båda parternas säkerhet och trygghet.

E. Ömsesidig tillit och förståelse är viktiga faktorer i den transatlantiska dialogen och det transatlantiska partnerskapet.

F. Efter 11 september 2001 blev kampen mot terrorism en av huvudprioriteringarna för de flesta regeringar. Avslöjandena i de dokument som läckts ut av f.d. NSA-konsulten Edward Snowden innebar att politiska ledare blev skyldiga att ta itu med utmaningarna med att övervaka och kontrollera underrättelseorganens övervakningsverksamhet och bedöma hur deras verksamhet påverkar de grundläggande rättigheterna och rättsstatsprincipen i ett demokratiskt samhälle.

G. De avslöjanden som skett sedan juni 2013 har väckt många frågor inom EU när det gäller

— de avslöjade övervakningssystemens omfattning i både Förenta staterna och EU:s medlemsstater,

— överträdelserna av EU:s rättsliga normer, grundläggande rättigheter och standarder för uppgiftsskydd,

— graden av tillit i det transatlantiska samarbetet mellan EU och Förenta staterna,

— omfattningen av vissa EU-medlemsstaters grad av samarbete och deltagande i Förenta staternas övervakningsprogram eller likvärdiga nationella program som avslöjats av medierna,

— de amerikanska politiska myndigheternas och vissa EU-medlemsstaters brist på kontroll och effektiv tillsyn över sina underrättelseorgan,

— risken för att dessa massövervakningsoperationer används för andra ändamål än nationell säkerhet och bekämpning av terrorism i egentlig mening, t.ex. ekonomiskt spionage, industrispionage eller politiskt motiverad profilering,

— undergrävandet av pressfriheten och av kommunikationer med medlemmar i yrkesgrupper som omfattas av tystnadsplikt, bl.a. advokater och läkare,

— underrättelseorganens och de privata it- och telekomföretagens respektive roller och grad av deltagande,

— de allt suddigare gränserna mellan brottsbekämpning och underrättelseverksamhet som leder till att varje medborgare behandlas som misstänkt och övervakas, samt

— hoten mot den personliga integriteten i den digitala tidsåldern och massövervakningens konsekvenser för medborgarna och samhällena.

H. Det spionerі som avslöjats är av en aldrig tidigare skådad omfattning och måste utredas grundligt av Förenta staternas myndigheter, EU-institutionerna och medlemsstaternas regeringar, nationella parlament och rättsliga myndigheter.

I. Förenta staternas myndigheter har förnekat en del av de avslöjade uppgifterna, men inte den stora merparten av dem. Avslöjandena har väckt en omfattande offentlig debatt i Förenta staterna och i vissa EU-medlemsstater, men alltför många av regeringarna och parlament i EU håller tyst och inleder inte adekvata undersökningar.

J. President Obama har nyligen tillkännagett att NSA och dess övervakningsprogram ska reformeras.

K. I jämförelse med åtgärder som vidtagits av både EU:s institutioner och vissa medlemsstater har Europaparlamentet tagit sin plikt på stort allvar att sprida ljus över avslöjandena om den urskillningslösa verksamheten med att massövervaka EU:s medborgare, och i sin resolution av den 4 juli 2013 om den amerikanska säkerhetsmyndigheten NSA:s övervakningsprogram och övervakningsorgan i olika medlemsstater och konsekvenserna för EU-medborgarnas integritet, uppmanade parlamentet sitt utskott för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor att göra en ingående utredning av frågan.

L. Det är EU-institutionernas skyldighet att se till att EU-lagstiftningen genomförs fullständigt för EU-medborgarnas skull och att EU-fördragens rättsverkan inte undergrävs av ett undergivet godtagande av de extraterritoriella effekterna av tredjeländers standarder eller insatser.

Utvecklingen när det gäller Förenta staternas reform av underrättelsetjänsten

M. Distriktsdomstolen i District of Columbia fastslog i sitt avgörande av den 16 december 2013 att NSA:s massinsamling av metadata strider mot fjärde tillägget i Förenta staternas konstitution ([1]). Distriktsdomstolen i Southern District of New York fastslog dock i sitt avgörande av den 27 december 2013 att denna insamling var laglig.

N. Enligt ett avgörande av distriktsdomstolen i Eastern District of Michigan innebär det fjärde tillägget att det krävs rimlighet vid all spaning, förhandstillstånd för all rimlig spaning, tillstånd grundade på befintliga sannolika skäl och likaså noggrannhet när det gäller personer, platser och föremål samt att det finns en neutral instans mellan de tjänstemän som får i uppdrag att utföra spaningen och medborgarna ([2]).

O. Presidentens grupp för tillsyn av underrättelse- och kommunikationsteknik lägger i sin rapport av den 12 december 2013 fram 46 rekommendationer till Förenta staternas president. I rekommendationerna framhålls behovet av att samtidigt skydda den nationella säkerheten, den personliga integriteten och de medborgerliga fri- och rättigheterna. I detta avseende uppmanas den amerikanska regeringen att så snart som möjligt upphöra med massupptagningen av amerikaners telefonsamtal i enlighet med avsnitt 215 i USA PATRIOT Act, att göra en ingående översyn av den rättsliga ramen för NSA och Förenta staternas underrättelseverksamhet för att se till att rätten till personlig integritet respekteras, att avsluta insatserna för att underminera kommersiell programvara eller göra den sårbar (genom bakdörrar och sabotageprogram), att öka användningen av kryptering, särskilt när det gäller data som överförs, och att inte undergräva insatserna för att skapa krypteringsstandarder, att utse en advokat för allmänintresset som kan företräda den personliga integriteten och de medborgerliga fri- och rättigheterna inför Foreign Intelligence Surveillance Court, att ge tillsynsnämnden på området personlig integritet och medborgerliga fri- och rättigheter befogenhet att övervaka underrättelseorganens verksamhet för utländska underrättelseändamål och inte bara för terrorismbekämpning, samt att ta emot klagomål från visselblåsare, att använda avtalen om ömsesidig rättslig hjälp för att erhålla elektronisk information och att inte använda övervakning för att stjäla industri- eller företagshemligheter.

P. Enligt en öppen promemoria som lades fram för president Obama av före detta höga chefer i NSA/Veteran Intelligence Professionals for Sanity (VIPS) den 7 januari 2014 ([3]) förbättrar inte massinsamlingen av data förmågan att förhindra framtida terroristattacker. Författarna betonar att den massövervakning som utförs av NSA har fått som resultat att inte en enda attack har förhindrats och att miljarder dollar har lagts ner på program som är mindre effektiva och som inkräktar oerhört mycket mer på medborgarnas personliga integritet än en intern teknik med benämningen Thinthread som skapades 2001.

Q. När det gäller underrättelseverksamhet avseende andra personer än ”US persons” (dvs. Förenta staternas medborgare och personer som lagligt befinner sig i landet) i enlighet med avsnitt 702 i FISA rekommenderas Förenta staternas president att beakta den grundläggande principen om respekt för den personliga integriteten och människors värdighet som ingår i artikel 12 i den allmänna förklaringen om de mänskliga rättigheterna och i artikel 17 i Internationella konventionen om medborgerliga och politiska rättigheter. Det görs dock ingen rekommendation om att bevilja andra personer än ”US persons” samma rättigheter och skydd som ”US persons”.

([1]) Dom av den 16 december 2013 i civilmål nr 13-0851, Klayman m.fl. mot Obama m.fl.
([2]) Dom av den 17 augusti 2006 i mål nr 06-CV-10204, ACLU mot NSA.
([3]) http://consortiumnews.com/2014/01/07/nsa-insiders-reveal-what-went-wrong.

Onsdagen den 12 mars 2014

R. I sitt policydirektiv om signalspaning av den 17 januari 2014 och det tillhörande talet slog Förenta staternas president Barack Obama fast att Förenta staterna behöver elektronisk massövervakning för att skydda den nationella säkerheten, landets medborgare och medborgarna i Förenta staternas allierade länder och partnerländer, såväl som för att främja amerikanska utrikespolitiska intressen. Detta policydirektiv innehåller vissa principer om insamling, användning och delning av signalspaning liksom vissa säkerhetsanordningar för andra personer än ”US persons”. Policydirektivet föreskriver delvis behandling som är likvärdig med den som amerikanska medborgare åtnjuter, inklusive säkerhetsanordningar för personuppgifter för alla enskilda individer, oberoende av deras nationalitet eller hemvist. President Obama efterlyste dock inte några konkreta förslag, framför allt inte när det gäller förbudet mot massövervakning och införandet av administrativ och rättslig prövning för andra personer än ”US persons”.

Rättslig ram

Grundläggande rättigheter

S. Rapporten från EU:s medordförande i den tillfälliga EU–USA-arbetsgruppen om dataskydd ger en överblick över rättsläget i Förenta staterna men har inte kunnat fastställa fakta om Förenta staternas övervakningsprogram. Ingen information ges om arbetsgruppen för det så kallade andra spåret, där medlemsstaterna för bilaterala diskussioner med Förenta staternas myndigheter om frågor som rör nationell säkerhet.

T. De grundläggande fri- och rättigheterna, främst yttrandefriheten, pressfriheten, tankefriheten, samvetsfriheten, religionsfriheten och föreningsfriheten samt rätten till personlig integritet, uppgiftsskydd, ett effektivt rättsmedel, oskuldspresumtion, en opartisk domstol och icke-diskriminering, är demokratins grundpelare och fastställs i Europeiska unionens stadga om de grundläggande rättigheterna och i Europakonventionen. Massövervakning av människor är oförenlig med dessa grundpelare.

U. I alla medlemsstater skyddar lagen mot utlämnande av information som har överförts i förtroende mellan advokat och klient, en princip som har erkänts av Europeiska unionens domstol ([1]).

V. I sin resolution av den 23 oktober 2013 om organiserad brottslighet, korruption och penningtvätt uppmanade parlamentet kommissionen att lägga fram ett lagstiftningsförslag om ett verkningsfullt och heltäckande europeiskt skyddsprogram för visselblåsare för att skydda EU:s ekonomiska intressen och dessutom utreda om en sådan framtida lagstiftning även bör omfatta andra områden där unionen är behörig.

Unionens behörighet på säkerhetsområdet

W. Enligt artikel 67.3 i EUF-fördraget ska EU ”verka för att säkerställa en hög säkerhetsnivå”. Bestämmelserna i fördraget (särskilt artikel 4.2 i EU-fördraget samt artiklarna 72 och 73 i EUF-fördraget) innebär att EU har vissa behörigheter i frågor som rör unionens kollektiva säkerhet. EU har behörighet när det gäller inre säkerhet (artikel 4 j i EUF-fördraget) och har utövat denna behörighet genom att besluta om ett antal lagstiftningsinstrument och ingå internationella avtal (PNR- och TFTP-avtalen) i syfte att bekämpa allvarlig brottslighet och terrorism och genom att upprätta en strategi för inre säkerhet och myndigheter som verkar på detta område.

X. Fördraget om Europeiska unionens funktionssätt fastställer att ”medlemsstaterna får inbördes och på eget ansvar organisera sådana former för samarbete och samordning som de finner lämpliga mellan de behöriga avdelningarna vid sina administrationer med ansvar för att skydda den nationella säkerheten” (artikel 73 i EUF-fördraget).

Y. Artikel 276 i EUF-fördraget fastställer att ”när Europeiska unionens domstol utövar sina befogenheter med avseende på bestämmelserna i tredje delen avdelning V kapitlen 4 och 5 om ett område med frihet, säkerhet och rättvisa, är den inte behörig att pröva giltigheten eller proportionaliteten av insatser som polis eller andra brottsbekämpande organ gör i en medlemsstat eller av medlemsstaternas utövning av sitt ansvar för att upprätthålla lag och ordning och skydda den inre säkerheten”.

([1]) Dom av den 18 maj 1982 i mål C-155/79, AM & S Europe Limited mot Europeiska gemenskapernas kommission.

Z. Begreppen ”nationell säkerhet”, ”inre säkerhet”, ”EU:s inre säkerhet” och ”internationell säkerhet” överlappar varandra. Wienkonventionen om traktaträtten, principen om lojalt samarbete mellan EU:s medlemsstater samt människorättslagstiftningens princip om att tolka eventuella undantag restriktivt tyder på en restriktiv tolkning av begreppet ”nationell säkerhet” och innebär att medlemsstaterna måste avstå från att inkräkta på EU:s befogenheter.

AA. EU:s fördrag ger kommissionen rollen som väktare av fördragen, och av denna anledning har kommissionen det rättsliga ansvaret för att undersöka alla eventuella brott mot EU:s lagstiftning.

AB. I enlighet med artikel 6 i EU-fördraget, där det hänvisas till EU:s stadga om de grundläggande rättigheterna och Europakonventionen, måste medlemsstaternas myndigheter och även privata parter som verkar på området nationell säkerhet respektera de rättigheter som fastställs i denna konvention, oavsett om rättigheterna gäller de egna medborgarna eller medborgare med annan statstillhörighet.

Extraterritorialitet

AC. Om ett tredjeland tillämpar sina lagar, förordningar och andra rättsliga eller verkställande instrument extraterritoriellt i situationer som omfattas av EU:s eller EU-medlemsstaternas jurisdiktion, kan detta inverka på den gällande rättsordningen och rättsstatsprincipen, eller till och med strida mot internationell lagstiftning eller EU-lagstiftningen, inbegripet fysiska och juridiska personers rättigheter, beroende på omfattningen av och det angivna eller verkliga syftet med en sådan tillämpning. Under dessa omständigheter är det nödvändigt att vidta åtgärder på unionsnivå för att se till att EU:s värden som föreskrivs i artikel 2 i EU-fördraget, i EU-stadgan om de grundläggande rättigheterna och i Europakonventionens bestämmelser om grundläggande rättigheter, demokrati och rättsstatsprincipen samt fysiska och juridiska personers rättigheter som föreskrivs i den sekundärrätt som tillämpar dessa grundläggande rättigheter respekteras inom EU, till exempel genom att utplåna, neutralisera, stoppa eller på annat sätt motarbeta effekterna av den utländska lagstiftningen i fråga.

Internationella överföringar av uppgifter

AD. Om EU:s institutioner, organ, avdelningar eller myndigheter eller medlemsstaterna överför personuppgifter till Förenta staterna för brottsbekämpande ändamål utan tillräcklig garanti om och skydd av respekten för EU-medborgarnas grundläggande rättigheter, särskilt rätten till personlig integritet och skyddet av personuppgifter, innebär det att institutionen, organet, avdelningen, myndigheten eller medlemsstaten i fråga enligt artikel 340 i EUF-fördraget eller EU-domstolens rättspraxis ([1]), överträder EU-lagstiftningen, som även omfattar all eventuell kränkning av de grundläggande rättigheter som fastställs i EU-stadgan.

AE. Överföring av data är inte geografiskt begränsad och särskilt i samband med den ökande globaliseringen och de världsomspännande kommunikationerna möter EU:s lagstiftare nya utmaningar med avseende på skydd av personuppgifter och personlig kommunikation. Det är därför av den yttersta vikt att främja rättsliga ramar för allmänna standarder.

AF. Massinsamlingen av personuppgifter för kommersiella ändamål och i kampen mot terrorism och allvarlig gränsöverskridande brottslighet äventyrar EU-medborgarnas rättigheter avseende personuppgifter och personlig integritet.

Överföringar till Förenta staterna som grundas på Safe Harbour-avtalet

AG. Förenta staternas rättsliga ram för uppgiftsskydd garanterar inte ett lämpligt skydd för EU-medborgare.

AH. För att göra det möjligt för registeransvariga för uppgifter i EU att överföra personuppgifter till en enhet i Förenta staterna har kommissionen i sitt beslut 2000/520/EG förklarat lämpligheten i det skydd som ges genom principerna om integritetsskydd och de relaterade ”frågor och svar” som har offentliggjorts av Förenta staternas handelsministerium för personuppgifter som överförts från EU till organisationer som är belägna i Förenta staterna och som deltar i Safe Harbour-avtalet.

([1]) Se framför allt domstolens dom av den 19 november 1991 i de förenade målen C-6/90 och C-9/90, Francovich m.fl. mot Italien.

Onsdagen den 12 mars 2014

AI. I sin resolution av den 5 juli 2000 uttryckte parlamentet tveksamheter och farhågor avseende lämpligheten av Safe Harbour-avtalet och uppmanade kommissionen att i god tid granska beslutet mot bakgrund av erfarenheter och eventuell lagstiftningsmässig utveckling.

AJ. I parlamentets arbetsdokument 4 om Förenta staternas övervakningsverksamhet med avseende på EU-uppgifter och dess möjliga rättsliga följder för transatlantiska avtal och transatlantiskt samarbete av den 12 december 2013 uttryckte föredragandena tvivel och oro för Safe Harbour-principernas tillräcklighet och uppmanade kommissionen att häva beslutet om Safe Harbour-principernas tillräcklighet och finna nya rättsliga lösningar.

AK. Enligt kommissionens beslut 2000/520/EG får medlemsstaternas behöriga myndigheter utöva sina befogenheter att tillfälligt förbjuda överföringen av uppgifter till en organisation som genom självcertifiering förbinder sig att följa Safe Harbour-principerna för att skydda individer när det gäller behandling av deras personuppgifter i de fall då det är i hög grad sannolikt att principerna överträds eller en fortsatt överföring av uppgifterna skulle innebära en överhängande risk för allvarlig skada för registrerade.

AL. I kommissionens beslut 2000/520/EG anges även att kommissionen, om det finns bevis för att någon som är ansvarig för att garantera förenligheten med principerna inte fullgör sin uppgift, måste underrätta Förenta staternas handelsministerium om detta och vid behov föreslå åtgärder i syfte att helt eller tills vidare upphäva detta beslut eller begränsa dess tillämpningsområde.

AM. I sina första två rapporter om genomförandet av Safe Harbour-avtalet, offentliggjorda 2002 och 2004, påtalade kommissionen flera brister avseende det lämpliga genomförandet av avtalet och avgav en rad rekommendationer till de amerikanska myndigheterna så att de skulle korrigera dessa brister.

AN. I sin tredje genomföranderapport från den 27 november 2013, nio år efter den andra rapporten och utan att någon av de brister som uppmärksammades i den rapporten hade åtgärdats, påtalade kommissionen ytterligare allvarliga svagheter och brister i Safe Harbour-avtalet och drog slutsatsen att det rådande genomförandet inte kunde fortsätta. Kommissionen har betonat att en långtgående tillgång för amerikanska underrättelsebyråer till uppgifter som har överförts till Förenta staterna genom Safe Harbour-certifierade enheter väcker ytterligare allvarliga frågor vad gäller det fortsatta skyddet av uppgifter om registrerade i EU. Kommissionen riktade 13 rekommendationer till de amerikanska myndigheterna och åtog sig att senast till sommaren 2014 ange, tillsammans med de amerikanska myndigheterna, lösningar som ska genomföras så snart som möjligt, vilka utgör grunden för en fullständig översyn av Safe Harbour-principerna och deras funktionssätt.

AO. Den 28–31 oktober 2013 sammanträdde en delegation från Europaparlamentets utskott för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor (LIBE) i Washington D.C. med Förenta staternas handelsministerium och Förenta staternas federala handelskommission. Handelsministeriet erkände att organisationer hade påstått att de följde Safe Harbour-principerna, men att denna status var inaktuell, dvs. att företaget inte uppfyller kraven i Safe Harbour-avtalet trots att de fortsatte att få personuppgifter från EU. Den federala handelskommissionen medgav att Safe Harbour-avtalet borde ses över så att man kunde förbättra det, särskilt vad gäller klagomål och alternativa tvistlösningssystem.

AP. Safe Harbour-principerna kan vara begränsade till ”vad som är nödvändigt för att uppfylla krav i fråga om nationell säkerhet, allmänintresset eller rättsefterlevnaden”. Som ett undantag för en grundläggande rättighet måste ett sådant undantag alltid tolkas restriktivt och begränsas till vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle, och lagstiftningen måste tydligt ange villkoren och säkerhetsbestämmelserna för att göra denna begränsning legitim. Tillämpningsområdet för ett sådant undantag borde ha tydliggjorts av Förenta staterna och av EU, i synnerhet av kommissionen, för att undvika tolkningar eller tillämpningar som i allt väsentligt upphäver bland annat den grundläggande rätten till personlig integritet och uppgiftsskydd. Ett sådant undantag bör följaktligen aldrig användas på ett sätt som undergräver eller upphäver det skydd som ges av EU-stadgan om de grundläggande rättigheterna, Europakonventionen, EU: s lagstiftning om uppgiftsskydd och Safe Harbour-principerna. Om undantaget för nationell säkerhet åberopas måste man specificera under vilken nationell lag det åberopas.

AQ. De amerikanska underrättelsebyråernas omfattande tillträde till uppgifter har allvarligt undergrävt det transatlantiska förtroendet och påverkat förtroendet negativt när det gäller amerikanska organisationer med verksamhet i EU. Detta har förvärrats ytterligare genom bristen på rättslig och administrativ prövning för EU-medborgare enligt amerikansk lagstiftning, särskilt vad gäller övervakningsverksamhet i underrättelsesyfte.

Överföringar till tredjeländer med beslutet om adekvat skydd

AR. Enligt den information som har avslöjats och slutsatserna av den utredning som har utförts av LIBE-utskottet har Nya Zeelands, Kanadas och Australiens säkerhetsmyndigheter deltagit i en omfattande massövervakning av elektronisk kommunikation och haft ett aktivt samarbete med Förenta staterna enligt det s.k. Five eyes-programmet, och kan ha utväxlat med varandra andra personuppgifter från EU-medborgare som har överförts från EU.

AS. Kommissionen har i sina beslut 2013/65/EU ([1]) och 2002/2/EG ([2]) förklarat att de skyddsnivåer som garanteras av Nya Zeelands uppgiftsskyddslag respektive Kanadas Personal Information Protection and Electronic Documents Act är lämpliga. De tidigare nämnda avslöjandena påverkar också allvarligt förtroendet för rättssystemen i dessa länder när det gäller det fortsatta skydd som ges till EU-medborgare. Kommissionen har inte undersökt denna aspekt.

Överföringar på grundval av avtalsklausuler och andra instrument

AT. I direktiv 95/46/EG anges att internationella överföringar till ett tredjeland även får ske genom särskilda instrument med vars hjälp den registeransvarige åberopar lämpliga säkerhetsbestämmelser med hänsyn till skyddet av integritets- och grundläggande rättigheter och friheter för personer och med hänsyn till utövandet av de motsvarande rättigheterna.

AU. Sådana säkerhetsbestämmelser kan särskilt framgå av lämpliga avtalsklausuler.

AV. Direktiv 95/46/EG ger kommissionen befogenhet att besluta att särskilda standardavtalsklausuler ger den tillräckliga säkerhet som krävs enligt direktivet, och på grundval av detta har kommissionen antagit tre modeller för standardavtalsklausuler för överföringar till registeransvariga och registerförare (och underentreprenörer) i tredjeländer.

AW. I kommissionens beslut om upprättande av standardavtalsklausuler anges att de behöriga myndigheterna i medlemsstaterna får utöva sina befintliga befogenheter att avbryta uppgiftsöverföringar om det har fastställts att den lagstiftning som gäller för uppgiftsimportören eller underentreprenören ålägger dem sådana krav att göra undantag från den tillämpliga uppgiftsskyddslagstiftningen som är mer långtgående än de begränsningar som är nödvändiga i ett demokratiskt samhälle enligt artikel 13 i direktiv 95/46/EG, då dessa krav sannolikt kommer att få en avsevärd negativ effekt på de garantier som ges genom den tillämpliga uppgiftsskyddslagstiftningen och standardavtalsklausulerna, eller då det finns en avsevärd sannolikhet att standardavtalsklausulerna i bilagan inte följs eller inte kommer att följas och den fortsatta överföringen skulle skapa en överhängande risk för att de registrerade lider allvarlig skada.

AX. De nationella dataskyddsmyndigheterna har utarbetat bindande företagsbestämmelser för att underlätta internationella överföringar inom ett multinationellt företag, med lämpliga säkerhetsbestämmelser när det gäller skyddet av den personliga integriteten och av personers grundläggande rättigheter och friheter, och när det gäller utövandet av de motsvarande rättigheterna. Innan de används måste de bindande företagsbestämmelserna godkännas av medlemsstaternas behöriga myndigheter efter det att de har bedömt om reglerna är förenliga med EU:s uppgiftsskyddslagstiftning. Bindande företagsbestämmelser för uppgiftsbehandlare har förkastats i LIBE-utskottets rapport om den allmänna förordningen om uppgiftsskydd, eftersom de skulle göra så att registeransvariga och registrerade personer lämnades utan någon som helst kontroll över den jurisdiktion i vilken deras uppgifter behandlas.

([1]) EUT L 28, 30.1.2013, s. 12.
([2]) EGT L 2, 4.1.2002, s. 13.

Onsdagen den 12 mars 2014

AY. Mot bakgrund av dess behörighet som fastställs i artikel 218 i EUF-fördraget har Europaparlamentet ansvaret för att kontinuerligt övervaka värdet av de internationella avtal som det har godkänt.

Överföringar grundade på TFTP- och PNR-avtalen

AZ. I sin resolution av den 23 oktober 2013 uttryckte parlamentet djup oro över avslöjandena rörande NSA:s verksamhet avseende direkt tillgång till finansiella betalningsmeddelanden och relaterade uppgifter, vilket skulle innebära en klar överträdelse av TFTP-avtalet, särskilt artikel 1 i detta.

BA. Spårande av terrorismfinansiering är ett avgörande verktyg i kampen mot terrorismfinansiering och grova brott, och bidrar till att terrorismbekämpare kan hitta kopplingar mellan personer som undersöks och andra misstänkta å ena sidan och bredare terroristnätverk som misstänks för att finansiera terrorism å andra sidan.

BB. Parlamentet uppmanade kommissionen att tillfälligt upphäva avtalet och begärde att all relevant information och alla dokument omedelbart skulle tillgängliggöras för parlamentets överläggningar. Kommissionen har inte gjort något av detta.

BC. Till följd av de påståenden som publicerats i medierna beslutade kommissionen att inleda samråd med Förenta staterna i enlighet med artikel 19 i TFTP-avtalet. Den 27 november 2013 informerade kommissionsledamot Cecilia Malmström LIBE-utskottet om att kommissionen, efter att ha sammanträtt med de amerikanska myndigheterna och med tanke på de amerikanska myndigheternas svar i sina skrivelser och under sina sammanträden, hade beslutat att inte fortsätta samråden på grund av att det inte fanns något som visade att Förenta staternas regering hade handlat i strid mot avtalets bestämmelser, och att Förenta staterna har tillhandahållit en skriftlig försäkran om att det inte har skett någon direkt uppgiftsinsamling i strid mot TFTP-avtalets bestämmelser. Det står inte klart om de amerikanska myndigheterna har kringgått avtalet genom att få tillgång till sådana uppgifter på andra sätt, som antyddes i brevet av den 18 september 2013 från de amerikanska myndigheterna ([1]).

BD. Under sitt besök i Washington den 28–31 oktober 2013 sammanträdde LIBE-delegationen med det amerikanska finansministeriet. Finansministeriet meddelade att det sedan TFTP-avtalets ikraftträdande inte hade haft någon tillgång till uppgifter från Swift i EU, förutom inom ramen för TFTP-avtalet. Det amerikanska finansministeriet vägrade att kommentera huruvida någon annan amerikansk myndighet hade fått tillgång till Swift-uppgifter utanför ramen för TFTP-avtalet eller om den amerikanska statsförvaltningen kände till NSA:s massövervakningsverksamhet. Den 18 december 2013 meddelade Glenn Greenwald inför LIBE-utskottets utredning att NSA och den brittiska signalspaningsmyndigheten GCHQ hade riktade Swift-nätverk.

BE. De belgiska och nederländska dataskyddsmyndigheterna beslutade den 13 november 2013 att utföra en gemensam utredning om säkerheten hos Swifts betalningsnätverk för att bekräfta huruvida tredje parter kunde få icke-auktoriserad eller olaglig tillgång till europeiska medborgares bankuppgifter ([2]).

BF. Enligt den gemensamma översynen av genomförandet av avtalet mellan Europeiska unionen och Amerikas förenta stater om behandling av passageraruppgifter (PNR) gjorde Förenta staternas Department of Homeland Security (DHS) 23 utlämnanden av PNR-uppgifter. Detta gjordes från fall till fall, som stöd för ärenden om bekämpning av terrorism, i enlighet med avtalets särskilda villkor.

BG. Den gemensamma översynen nämner dock inte det faktum att i de fall personuppgifter behandlas för underrättelseverksamhet, ger Förenta staternas lagstiftning inte några rättsliga eller administrativa möjligheter för personer som inte är medborgare i Förenta staterna att skydda sina rättigheter, och det konstitutionella skyddet omfattar enbart ”US persons”. Denna brist på rättsliga eller administrativa rättigheter undergräver det skydd för EU-medborgare som har angetts i det befintliga PNR-avtalet.

([1]) I brevet uppges att ”den amerikanska regeringen söker efter och erhåller finansiell information … [som] insamlas genom rättsliga och diplomatiska kanaler samt brottsbekämpnings- och underrättelsekanaler, såväl som genom utbyte med våra utländska partner … Den amerikanska regeringen använder TFTP-avtalet för att få tillgång till Swift-uppgifter som vi inte kan få tillgång till från andra källor”.

([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

Överföringar grundade på avtalet mellan EU och Förenta staterna om ömsesidig rättslig hjälp i brottmål

BH. Avtalet mellan EU och Förenta staterna om ömsesidig rättslig hjälp i brottmål av den 6 juni 2003 ([1]) trädde i kraft den 1 februari 2010 och syftar till att underlätta EU:s och Förenta staternas samarbete när det gäller att effektivare bekämpa brott och samtidigt ta hänsyn till individens rättigheter och rättsstatsprincipen.

Ramavtalet om uppgiftsskydd på området för polissamarbete och rättsligt samarbete (”paraplyavtalet”)

BI. Syftet med detta ramavtal är att upprätta den rättsliga ramen för alla överföringar av personuppgifter mellan EU och Förenta staterna för att förebygga, utreda, avslöja eller lagföra brott, inklusive terrorism, inom ramen för polissamarbete och straffrättsligt samarbete. Rådet bemyndigade förhandlingarna den 2 december 2010. Detta avtal är av yttersta vikt och skulle fungera som grund för att underlätta överföringen av uppgifter inom ramen för polissamarbete och straffrättsligt samarbete.

BJ. Detta avtal bör tillhandahålla klara och tydliga och rättsligt bindande principer om uppgiftsbehandling och bör särskilt erkänna EU-medborgarnas rätt till laglig tillgång till, rättelse eller radering av sina personuppgifter i Förenta staterna, såväl som rätten till en effektiv administrativ och juridisk prövning för EU-medborgare i Förenta staterna och oberoende utvärdering av uppgiftsbehandlingsverksamheten.

BK. I sitt meddelande av den 27 november 2013 angav kommissionen att ”paraplyavtalet” borde resultera i en hög skyddsnivå för medborgarna på båda sidor av Atlanten och stärka européernas förtroende för uppgiftsutbytet mellan EU och Förenta staterna, och tillhandahålla en grund på vilken det säkerhetsmässiga samarbetet och partnerskapet mellan EU och Förenta staterna kan utvecklas ytterligare.

BL. Förhandlingarna om avtalet har inte gett några resultat på grund av den amerikanska regeringens envetna motstånd mot att erkänna EU-medborgarnas rätt till en effektiv administrativ och juridisk prövning och på grund av syftet att tillhandahålla omfattande undantag för de uppgiftsskyddsprinciper som finns i avtalet, t.ex. ändamålsbegränsning, datalagring eller vidare överföringar antingen inrikes eller utomlands.

Reform av uppgiftsskyddet

BM. EU:s rättsliga ram för uppgiftsskydd ses för närvarande över, i syfte att upprätta ett övergripande, konsekvent, modernt och kraftfullt system för all uppgiftsbehandlingsverksamhet i EU. I januari 2012 lade kommissionen fram ett paket med lagstiftningsförslag: en allmän förordning om uppgiftsskydd ([2]), som kommer att ersätta direktiv 95/46/EG och upprätta en enhetlig lag i hela EU, och ett direktiv ([3]) som kommer att fastställa en harmoniserad ram för all uppgiftsbehandlingsverksamhet vid de brottsbekämpande myndigheterna i brottsbekämpande syfte och minska de nuvarande skillnaderna mellan de nationella lagarna.

BN. Den 21 oktober 2013 antog LIBE-utskottet sina lagstiftningsbetänkanden om de båda förslagen och ett beslut om att inleda förhandlingar med rådet i syfte att få de rättsliga instrumenten antagna under innevarande valperiod.

BO. Trots att Europeiska rådet den 24–25 oktober 2013 efterlyste ett snabbt antagande av en kraftfull allmän EU-ram för uppgiftsskydd i syfte att främja medborgarnas och företagens förtroende för den digitala ekonomin, har rådet efter två års överläggningar fortfarande inte kunnat komma överens om ett allmänt förhållningssätt till den allmänna förordningen om uppgiftsskydd och till direktivet ([4]).

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

Onsdagen den 12 mars 2014

It-säkerhet och datormoln

BP. I parlamentets ovannämnda resolution av den 10 december 2013 betonas ”datormolnföretagens” eventuella betydelse för tillväxten och sysselsättningen. Uppskattningsvis kommer det samlade ekonomiska värdet av molntjänsterna att uppgå till 207 miljarder US-dollar om året senast 2016. Värdet kommer med andra ord att vara dubbelt så högt som 2012.

BQ. Nivån på uppgiftsskyddet i en datormolnmiljö får inte vara sämre än den som krävs i något annat sammanhang avseende uppgiftsbehandling. Eftersom EU:s lagstiftning om uppgiftsskydd är tekniskt neutral gäller den redan fullt ut för datormolntjänster som är verksamma i EU.

BR. Massövervakningsverksamhet ger underrättelsemyndigheter tillgång till personuppgifter som har lagrats eller på annat sätt behandlats av individer i EU enligt avtal om molntjänster med större datormolnleverantörer i Förenta staterna. Underrättelsemyndigheter i Förenta staterna har haft tillgång till personuppgifter som har lagrats eller på annat sätt behandlats på servrar som finns på EU:s territorium, genom att de har tagit sig in i Yahoos och Googles interna nätverk. Sådan verksamhet utgör en överträdelse av internationella åtaganden och av europeiska standarder för grundläggande rättigheter, inklusive rätten till privat- och familjeliv, telehemlighet vid kommunikation, oskuldspresumtion, yttrandefrihet, informationsfrihet, mötesfrihet, föreningsfrihet och näringsfrihet. Det är inte uteslutet att även information som har lagrats i molntjänster av medlemsstaternas offentliga myndigheter eller företag och institutioner har varit åtkomlig för underrättelsemyndigheter.

BS. Förenta staternas underrättelseorgan har som policy att systematiskt undergräva kryptoprotokoll och krypto-produkter för att kunna avlyssna även krypterade kommunikationer. Förenta staternas National Security Agency har insamlat ett ofantligt antal s.k. ”zero-day exploits” – brister i it-säkerheten som varken allmänheten eller produktens säljare ännu känner till. Sådan verksamhet undergräver i mycket hög grad de globala insatserna för att förbättra it-säkerheten.

BT. Det faktum att underrättelseorganen har haft tillgång till personuppgifter för användare av onlinetjänster har allvarligt skadat medborgarnas förtroende för sådana tjänster och har därför en negativ effekt på företag som investerar i utvecklingen av nya tjänster som använder stora datamängder och nya tillämpningar, såsom sakernas internet.

BU. It-säljare levererar ofta produkter som inte har testats ordentligt med avseende på it-säkerhet eller som ibland till och med har bakdörrar som avsiktligt har installerats av säljaren. Bristen på ansvarsregler för mjukvarusäljare har lett till denna situation, vilken i sin tur utnyttjas av underrättelseorgan, men som även gör att risken för attacker av andra enheter kvarstår.

BV. Det är ytterst viktigt för företag som tillhandahåller sådana nya tjänster och tillämpningar att respektera reglerna för uppgiftsskydd och den personliga integriteten för registrerade personer vars uppgifter insamlas, behandlas och analyseras för att upprätthålla en hög förtroendenivå bland medborgarna.

Demokratisk tillsyn över underrättelsetjänster

BW. Underrättelsetjänsterna i demokratiska samhällen ges särskilda befogenheter och särskild förmåga att skydda grundläggande rättigheter, demokrati och rättsstatsprincipen, medborgarnas rättigheter och staten mot inre och yttre hot och är underställda demokratisk ansvarsskyldighet och rättslig tillsyn. De har fått särskilda befogenheter och särskild behörighet uteslutande för att uppnå detta mål. Dessa befogenheter bör användas inom de lagstadgade gränser som åläggs av de grundläggande rättigheterna, demokratin och rättsstatsprincipen, och tillämpningen av dem bör noggrant granskas eftersom de annars förlorar legitimitet och riskerar att urholka demokratin.

BX. Även om en viss sekretessnivå beviljas för underrättelsetjänster – för att undvika att äventyra pågående operationer, avslöja arbetsmetoder eller sätta agenters liv på spel – kan inte denna sekretess åsidosätta eller utesluta regler rörande demokratisk granskning och rättslig prövning samt granskning av deras verksamhet, såväl som regler rörande öppenhet, i synnerhet i förhållande till de grundläggande rättigheterna och rättsstatsprincipen, som alla är hörnstenar i ett demokratiskt samhälle.

BY. De flesta av de befintliga nationella tillsynsmekanismerna och tillsynsorganen infördes eller moderniserades på 1990-talet och har inte alltid anpassats till det senaste årtiondets snabba tekniska och rättsliga utveckling som har lett till ökat internationellt underrättelsesamarbete, även genom ett utbyte av personuppgifter, vilket ofta har suddat ut gränserna mellan underrättelseverksamhet och brottsbekämpning.

BZ. Den demokratiska tillsynen över underrättelseverksamheten utförs fortfarande endast på nationell nivå, trots att informationsutbytet mellan EU:s medlemsstater och mellan medlemsstaterna och tredjeländer har ökat. Det finns en växande klyfta mellan nivån på det internationella samarbetet å ena sidan och den nationella tillsynskapaciteten å andra sidan, vilket leder till otillräcklig och ineffektiv demokratisk kontroll.

CA. Nationella tillsynsorgan har ofta inte full tillgång till upplysningar som erhållits från en utländsk underrättelsetjänst, vilket kan leda till luckor inom vilka internationellt utbyte av uppgifter kan förekomma utan tillräcklig tillsyn. Detta problem förvärras ytterligare av den s.k. tredjepartsregeln eller principen om upphovsmannens kontroll, vilken har utformats för att göra det möjligt för upphovsmannen att behålla kontrollen över den ytterligare spridningen av känslig information, men som tyvärr ofta tolkas som att gälla även för tillsyn av mottagartjänsterna.

CB. Privata och offentliga reforminitiativ för insyn är mycket viktiga för att säkerställa allmänhetens förtroende för underrättelsetjänsternas verksamhet. Rättsliga system bör inte förhindra företag från att avslöja uppgifter till allmänheten om hur de handskas med alla typer av förfrågningar från staten och domstolsbeslut rörande tillgång till användaruppgifter, inklusive möjligheten att avslöja sammanställd information om antalet förfrågningar och beslut som godkänts och avvisats.

Huvudsakliga slutsatser

1. Europaparlamentet anser att den senaste tidens avslöjanden i medierna från visselblåsare och journalister – tillsammans med den bevisning som experter har lämnat under denna utredning, myndigheternas medgivanden och de otillräckliga svaren på dessa påståenden – har gett övertygande bevis för att det finns långtgående, komplexa och avancerade högteknologiska system som utformats av Förenta staternas och vissa medlemsstaters underrättelsetjänster för att samla in, lagra och analysera kommunikationsinformation, inklusive innehållsdata, lokaliseringsinformation och metadata om alla invånare runtom i världen i oöverträffad skala och på ett sätt som är urskillningslöst och inte bygger på brottsmisstankar.

2. Europaparlamentet framhäver särskilt amerikanska NSA:s underrättelseprogram, som möjliggör massövervakning av EU:s invånare genom direkt tillgång till centrala servrar hos ledande amerikanska internetföretag (Prismprogrammet), analys av innehåll och metadata (Xkeyscore-programmet), kringgående av onlinekryptering (Bullrun) samt tillgång till data- och telefonnätverk, lokaliseringsinformation och den brittiska underrättelsetjänsten GCHQ:s system, såsom övervakningsverksamheten i den tidiga kommunikationsfasen (Temporaprogrammet), dekrypteringsprogrammet (Edgehill), riktade ”man in the middle”-angrepp på informationssystem (Quantumtheory- och Foxaidprogrammen) samt insamlingen och lagringen av 200 miljoner sms per dag (Dishfireprogrammet).

3. Europaparlamentet noterar anklagelserna mot den brittiska underrättelsetjänsten GCHQ om intrång, s.k. hackning, i Belgacoms system. Parlamentet konstaterar att Belgacom meddelade att företaget varken kunde bekräfta eller dementera att EU-institutionerna hade utsatts eller påverkats, och att det sabotageprogram som användes var ytterst komplext och att dess utveckling och användning måste ha krävt betydande ekonomiska resurser och personalresurser som privatpersoner eller hackare inte kan tänkas ha tillgång till.

4. Europaparlamentet framhåller att förtroendet har fått sig en allvarlig törn: förtroendet mellan de båda transatlantiska partnerna, förtroendet mellan medborgarna och deras regeringar, förtroendet för de demokratiska institutionerna på båda sidorna om Atlanten, förtroendet för respekten för rättsstatsprincipen och förtroendet för it-tjänsternas säkerhet. För att återuppbygga förtroendet på alla dessa områden behövs det omgående en omfattande åtgärdsplan med en rad åtgärder som omfattas av en offentlig kontroll.

5. Europaparlamentet konstaterar att flera regeringar påstår att dessa massövervakningsprogram är nödvändiga för kampen mot terrorismen. Parlamentet fördömer med kraft terrorismen, men är av den bestämda åsikten att kampen mot terrorismen aldrig kan rättfärdiga urskillningslösa, hemliga eller till och med olagliga massövervakningsprogram. Sådana program är oförenliga med nödvändighets- och proportionalitetsprinciperna i ett demokratiskt samhälle.

Onsdagen den 12 mars 2014

6. Europaparlamentet påminner om EU:s bestämda uppfattning att det måste finnas rätt balans mellan säkerhetsåtgärder och skyddet av medborgerliga friheter och grundläggande rättigheter, samtidigt som man ser till att den personliga integriteten och uppgiftsskyddet åtnjuter största möjliga respekt.

7. Europaparlamentet anser att uppgiftsinsamling i en sådan stor skala ger upphov till stora tvivel om huruvida denna verksamhet endast motiveras av kampen mot terrorism, eftersom den omfattar insamling av alla möjliga slags uppgifter om samtliga invånare. Parlamentet menar därför att det kan tänkas finnas andra ändamål, t.ex. politiskt och ekonomiskt spionage, och att alla misstankar om sådana ändamål måste kunna avfärdas.

8. Europaparlamentet ifrågasätter om vissa medlemsstaters massiva ekonomiska spionage är förenligt med EU:s inremarknads- och konkurrenslagstiftning i enlighet med avdelningarna I och VII i EUF-fördraget. Parlamentet vill påminna om principen om lojalt samarbete, som fastställs i artikel 4.3 i EU-fördraget, och principen att medlemsstaterna ska ”avstå från varje åtgärd som kan äventyra fullgörandet av unionens mål”.

9. Europaparlamentet konstaterar att internationella avtal, EU:s och Förenta staternas lagstiftning samt de nationella tillsynsmekanismerna har misslyckats med att skapa nödvändiga kontroll- och maktdelningssystem eller ett demokratiskt ansvarsutkrävande.

10. Europaparlamentet fördömer den omfattande och systemiska övergripande inhämtningen av oskyldiga människors personuppgifter, inklusive information av en högst personlig natur. Parlamentet betonar att underrättelsetjänsternas urskillningslösa massövervakning är en allvarlig överträdelse av medborgarnas grundläggande rättigheter. Parlamentet understryker att ett privatliv inte är ett lyxigt privilegium, utan en hörnsten i ett fritt och demokratiskt samhälle. Vidare menar parlamentet att massövervakningen kan komma att få allvarliga effekter för press-, tanke- och yttrandefriheten samt mötes- och föreningsfriheten och att det även finns en betydande risk för att de upplysningar som samlats in missbrukas för att komma åt politiska motståndare. Parlamentet betonar att massövervakningen dessutom medför olagliga handlingar från underrättelsetjänsternas sida och att den väcker frågor om den nationella lagstiftningens extraterritoriella tillämplighet.

11. Europaparlamentet anser att det är mycket viktigt att tystnadsplikten för advokater, journalister, läkare och andra reglerade yrken skyddas mot massövervakningsverksamhet. Parlamentet betonar framför allt att all ovisshet om sekretesskyddet för korrespondens mellan advokater och deras klienter skulle kunna inverka negativt på unionsmedborgarnas rätt till juridisk rådgivning och tillgång till rättslig prövning samt deras rätt till en rättvis rättegång.

12. Europaparlamentet anser att övervakningsprogrammen är ytterligare ett steg mot inrättandet av en fullfjädrad förebyggande stat, där den vedertagna modellen för straffrätt i demokratiska samhällen, enligt vilken varje inskränkning av misstänktas grundläggande rättigheter måste godkännas av en domare eller åklagare på grundval av skälig misstanke och regleras i lag, ändras, och där man i stället främjar en blandning av brottsbekämpning och underrättelseverksamhet med försvagat rättsskydd, som ofta är oförenligt med demokratiska kontroll- och maktdelningssystem och grundläggande rättigheter, särskilt oskuldspresumtionen. I detta sammanhang uppmärksammar parlamentet en dom i Tysklands federala författningsdomstol ([1]) om ett förbud mot användandet av förebyggande polisinsatser (”präventive Rasterfahndung”) såvida det inte föreligger bevis om konkret fara för andra viktiga lagstadgade rättigheter. Det räcker inte med en allmän hotsituation eller internationella spänningar för att motivera sådana åtgärder.

13. Europaparlamentet är övertygat om att hemliga lagar och domstolar bryter mot rättsstatsprincipen. Parlamentet påpekar att inga domar i en domstol och inga beslut från en administrativ myndighet i en stat utanför EU som direkt eller indirekt tillåter överföring av personuppgifter får erkännas eller tillämpas på något vis, såvida det inte finns ett avtal om ömsesidig rättslig hjälp eller ett gällande internationellt avtal mellan det begärande tredjelandet och unionen eller en medlemsstat och ett förhandsgodkännande av en behörig tillsynsmyndighet. Parlamentet påminner om att alla utslag av en hemlig domstol och alla beslut av en administrativ myndighet i en stat utanför EU som i hemlighet direkt eller indirekt ger tillstånd till övervakningsverksamheter inte ska erkännas eller tillämpas.

([1]) Nr 1 BvR 518/02 av den 4 april 2006.

14. Europaparlamentet påpekar att de ovannämnda farhågorna förvärras av den snabba utvecklingen av tekniken och samhället, eftersom internet och mobila enheter finns överallt i vår moderna värld och eftersom de flesta internetföretags affärsmodell bygger på behandling av personuppgifter. Parlamentet anser att detta problem är av en helt oöverträffad storlek. Detta kan skapa en situation där infrastruktur för insamling och behandling av uppgifter i stor skala skulle kunna missbrukas vid politiska regimskiften.

15. Europaparlamentet konstaterar att det inte finns någon garanti, vare sig för EU:s offentliga institutioner eller för medborgarna, att deras it-säkerhet eller privatliv kan skyddas från angrepp av välutrustade obehöriga, och att det därmed inte finns någon 100-procentig it-säkerhet. För att uppnå största möjliga it-säkerhet måste EU:s invånare vara villiga att bidra med tillräckliga resurser, både vad gäller personal och finanser, för att slå vakt om Europas oberoende och självständighet på it-området.

16. Europaparlamentet förkastar med kraft idén om att alla frågor om massövervakningsprogram bara rör den nationella säkerheten och därför helt faller under de individuella medlemsstaternas ansvar. Parlamentet vidhåller att medlemsstaterna till fullo måste respektera EU-lagstiftningen och Europakonventionen när de vidtar åtgärder för att säkerställa sin nationella säkerhet. Parlamentet påminner om en ny dom i Europeiska unionens domstol enligt vilken ”blotta omständigheten att ett beslut rör statens säkerhet [inte kan] leda till att unionsrätten inte är tillämplig, även om det ankommer på medlemsstaterna att vidta åtgärder som är lämpliga för att säkerställa medlemsstaternas inre och yttre säkerhet” ([1]). Parlamentet understryker även att skyddet av samtliga EU-medborgares privatliv står på spel, såväl som säkerheten och tillförlitligheten hos EU:s alla kommunikationsnätverk. Därför anser parlamentet att diskussioner och åtgärder på EU-nivå inte bara är berättigade, utan att frågan även gäller EU:s självständighet.

17. Europaparlamentet välkomnar det stöd som olika institutioner och experter har bidragit med under denna utredning. Parlamentet beklagar emellertid djupt att myndigheterna i flera medlemsstater inte har samarbetat under den utredning som Europaparlamentet har genomfört på medborgarnas vägnar. Parlamentet välkomnar den öppenhet som många kongressledamöter och nationella parlament har visat.

18. Europaparlamentet är medvetet om att det på grund av en mycket pressad tidsfrist inte har kunnat göra mer än en preliminär utredning om alla de frågor som varit aktuella sedan juli 2013. Parlamentet konstaterar att de avslöjanden som föranlett utredningen är mycket omfattande och att de är av pågående karaktär. Därför tillämpar parlamentet en framåtsyftande metod, bestående av ett antal särskilda förslag och en mekanism för uppföljningsåtgärder under parlamentets nästa valperiod, som syftar till att säkerställa att utredningens resultat fortsatt hamnar högt på EU:s politiska agenda.

19. Europaparlamentet har för avsikt att kräva omfattande politiska åtgärder från den nya kommission som kommer att utses efter Europaparlamentsvalet i maj 2014, så att den genomför förslagen och rekommendationerna som härrör från denna utredning.

Rekommendationer

20. Europaparlamentet uppmanar Förenta staternas myndigheter och EU:s medlemsstater att förbjuda urskillningslös massövervakning om de inte redan gjort detta.

21. Europaparlamentet uppmanar alla medlemsstater, särskilt dem som deltar i de s.k. 9-eyes- och 14-eyes-programmen ([2]), att ingående utvärdera och vid behov se över sin nationella lagstiftning och sin styrning av sina underrättelsetjänster för att säkerställa att de står under parlamentarisk och rättslig uppsikt och omfattas av offentlig kontroll, att de respekterar principerna om laglighet, nödvändighet, proportionalitet, rättssäkerhet, användarinformation och insyn, i överensstämmelse med FN:s sammanställning av god praxis och Venedigkommissionens rekommendationer, samt att de är förenliga med Europakonventionen och uppfyller medlemsstaternas skyldigheter i fråga om grundläggande rättigheter såsom dataskydd, privatliv och oskuldspresumtion.

([1]) Domstolens dom av den 4 juni 2013 i mål C-300/11, ZZ mot Secretary of State for the Home Department.

([2]) Det s.k. 9-eyes-programmet omfattar Förenta staterna, Förenade kungariket, Kanada, Australien, Nya Zeeland, Danmark, Frankrike, Norge och Nederländerna, medan det s.k. 14-eyes-programmet omfattar även Tyskland, Belgien, Italien, Spanien och Sverige.

Onsdagen den 12 mars 2014

22. Europaparlamentet uppmanar samtliga EU-medlemsstater och i synnerhet – när det gäller dess resolution av den 4 juli 2013 och sammanträden för bevisupptagning – Förenade kungariket, Frankrike, Tyskland, Sverige, Nederländerna och Polen att se till att deras nuvarande eller framtida lagstiftningsramar och tillsynsmekanismer för underrättelseorganens verksamhet är förenliga med Europakonventionen och EU:s uppgiftsskyddslagstiftning. Dessa medlemsstater uppmanas att bringa klarhet i anklagelserna om massövervakningsverksamhet, inklusive massövervakning av gränsöverskridande telekommunikation, oriktad övervakning av kabelbundna kommunikationer, eventuella överenskommelser mellan underrättelsetjänster och telekommunikationsföretag om tillgång till och utbyte av personuppgifter och tillgång till transatlantiska kablar, Förenta staternas underrättelsepersonal och utrustning på EU:s territorium utan tillsyn över övervakningsverksamhet och deras förenlighet med EU-lagstiftningen. De nationella parlamenten i dessa länder uppmanas att öka de egna ländernas underrättelseorgans samarbete på europeisk nivå.

23. Med tanke på mediernas omfattande rapportering om massövervakning av underrättelseorganet GCHQ uppmanar Europaparlamentet framför allt Förenade kungariket att se över sin nuvarande lagstiftningsram, som består av ett komplext samspel mellan tre olika lagar: ”Human Rights Act” från 1998, ”Intelligence Services Act” från 1994 och ”Regulation of Investigatory Powers Act” från 2000.

24. Europaparlamentet noterar översynen av den nederländska underrättelse- och säkerhetslagen från 2002 (betänkandet från Dessens-kommissionen av den 2 december 2013). Parlamentet stöder de rekommendationer från översynskommissionen som syftar till att stärka insynen i och kontrollen och tillsynen över de nederländska underrättelsetjänsterna. Parlamentet uppmanar Nederländerna att avstå från att utsträcka underrättelsetjänsternas befogenheter på ett sådant sätt att oriktad och storskalig övervakning även kan ske av oskyldiga medborgares kabelbundna kommunikationer, särskilt med hänsyn till att en av världens största knutpunkter för internettrafik (AMS-IX) är belägen i Amsterdam. Parlamentet uppmanar till försiktighet vid fastställandet av den nya JSCU-enhetens (Joint Sigint Cyber Unit) uppdrag och möjligheter, samt till försiktighet när det gäller amerikansk underrättelsepersonals närvaro och verksamhet på nederländskt territorium.

25. Europaparlamentet uppmanar medlemsstaterna, även när de företräds av sina underrättelsetjänster, att neka att motta uppgifter från tredjeländer som har samlats in på olaglig väg och att inte ge tillstånd till underrättelseverksamhet på sitt territorium utförd av tredjeländers regeringar eller organ som är olagliga enligt den nationella lagstiftningen eller som inte uppfyller de krav på rättsskydd som fastställs i instrument på internationell nivå eller EU-nivå, inbegripet skyddet för mänskliga rättigheter enligt EU-fördraget, Europakonventionen och EU:s stadga om de grundläggande rättigheterna.

26. Europaparlamentet begär att alla säkerhetstjänster ska upphöra med massövervakning och massbearbetning av webbkamerabilder. Medlemsstaterna uppmanas att grundligt utreda om, hur och i vilken utsträckning deras respektive säkerhetstjänster har varit delaktiga i massövervakningen och massbearbetningen av webbkamerabilder och att radera alla bilder som lagrats med hjälp av sådana massövervakningsprogram.

27. Europaparlamentet uppmanar medlemsstaterna att omgående uppfylla sin positiva skyldighet enligt Europakonventionen att skydda sina invånare från onödig övervakning, inklusive när målet med denna är att skydda den nationella säkerheten, som utförs av tredjeländer eller deras egna underrättelsetjänster samt att se till att rättsstaten inte försvagas till följd av extraterritoriell tillämpning av ett tredjelands lagstiftning.

28. Europaparlamentet uppmanar Europarådets generalsekreterare att inleda förfarandet enligt artikel 52, vilken lyder på följande sätt: ”På anmodan av Europarådets generalsekreterare skall varje hög fördragsslutande part tillhandahålla upplysningar om det sätt på vilket dess inhemska lagstiftning säkerställer en effektiv tillämpning av bestämmelserna i denna konvention.”

29. Europaparlamentet uppmanar medlemsstaterna att omedelbart vidta lämpliga åtgärder, inklusive genom talan vid domstol, mot den överträdelse av deras suveränitet, och därigenom av den allmänna folkrätten, som begåtts genom massövervakningsprogrammen. Parlamentet uppmanar vidare medlemsstaterna att utnyttja alla tillgängliga internationella medel för att försvara EU-medborgarnas grundläggande rättigheter, framför allt genom att använda det mellanstatliga klagomålsförfarandet enligt artikel 41 i Internationella konventionen om medborgerliga och politiska rättigheter (ICCPR).

30. Europaparlamentet uppmanar medlemsstaterna att införa effektiva mekanismer som säkerställer att de som är ansvariga för (mass)övervakningsprogram som strider mot rättsstatsprincipen och medborgarnas grundläggande rättigheter ställs till svars för detta maktmissbruk.

31. Europaparlamentet uppmanar Förenta staterna att utan dröjsmål se över sin lagstiftning för att göra den förenlig med internationell rätt, att erkänna EU-medborgarnas rätt till privatliv och övriga rättigheter, att ge EU-medborgarna möjlighet till rättsligt överklagande, att se till att EU-medborgarna får samma rättigheter som de amerikanska medborgarna och att underteckna det fakultativa protokollet som möjliggör klagomål från enskilda personer inom ramen för ICCPR.

32. Europaparlamentet välkomnar i detta sammanhang kommentarerna från och det presidentdirektiv som USA:s president Barack Obama utfärdade den 17 januari 2014 som ett steg mot att begränsa de amerikanska underrättelseorganens tillstånd att använda övervakning och databehandling för nationella säkerhetsändamål och mot lika behandling av alla människors personuppgifter, oberoende av deras nationalitet eller hemvist. Parlamentet förväntar sig dock att ytterligare uttryckliga steg ska tas i förbindelserna mellan EU och Förenta staterna och framför allt för att stärka förtroendet för transatlantiska dataöverföringar och ge bindande garantier för att EU-medborgare har rätt till rättslig prövning, så som närmare beskrivs i detta betänkande.

33. Europaparlamentet framhåller sin starka oro över arbetet inom Europarådets kommitté för konventionen om it-brottslighet angående tolkningen av artikel 32 i konventionen om it-brottslighet av den 23 november 2001 (Budapestkonventionen) om gränsöverskridande åtkomst till lagrade datoruppgifter med medgivande eller om uppgifterna är offentligt tillgängliga. Parlamentet invänder mot ingåendet av ett tilläggsprotokoll eller vägledning i syfte att bredda tillämpningen av denna bestämmelse utöver den nuvarande ordning som upprättats genom konventionen, som redan är ett stort undantag från territorialitetsprincipen eftersom detta skulle kunna leda till att brottsbekämpande myndigheter får ohejdad fjärråtkomst till servrar och datorer som finns i andra jurisdiktioner utan hänvisning till avtal om ömsesidig rättslig hjälp och andra instrument för rättsligt samarbete som införts för att garantera den enskildes grundläggande rättigheter, inklusive uppgiftsskydd och rättssäkerhet, särskilt Europarådets konvention 108.

34. Europaparlamentet uppmanar kommissionen att före juli 2014 genomföra en bedömning av tillämpligheten av rådets förordning (EG) nr 2271/96 på fall av lagkonflikt vid överföringar av personuppgifter.

35. Europaparlamentet uppmanar Europeiska unionens byrå för grundläggande rättigheter att ingående studera skyddet av de grundläggande rättigheterna i samband med övervakning och att framför allt titta närmare på den aktuella rättsliga situationen för EU-medborgarna när det gäller de rättsmedel som de har tillgång till i samband med denna verksamhet.

Internationella överföringar av uppgifter

Den amerikanska rättsliga ramen för uppgiftsskydd och de amerikanska Safe Harbour-principerna

36. Europaparlamentet konstaterar att de företag som pekats ut i medierna som inblandade i amerikanska NSA:s storskaliga massövervakning av registrerade inom EU är företag som har självcertifierat att de följer Safe Harbour-principerna, och att Safe Harbour är det rättsliga instrument som används för överföring av personuppgifter från EU till Förenta staterna (till exempel Google, Microsoft, Yahoo!, Facebook, Apple, LinkedIn). Parlamentet framför sin oro över att dessa organisationer inte har krypterat uppgifts- och kommunikationsflöden mellan sina datacentraler och därigenom gjort det möjligt för underrättelsetjänster att avlyssna information. Parlamentet välkomnar vissa amerikanska företags uttalanden om att de kommer att påskynda planerna att kryptera dataflödena mellan sina globala datacentraler.

37. Europaparlamentet anser att storskalig åtkomst för amerikanska underrättelseorgan till personuppgifter från EU som behandlas enligt Safe Harbour-principerna inte uppfyller kriterierna för undantag på grund av ”nationell säkerhet”.

Onsdagen den 12 mars 2014

38. Europaparlamentet anser att eftersom Safe Harbour-principerna under de nuvarande omständigheterna inte ger adekvat skydd för EU-medborgare bör dessa överföringar göras inom ramen för andra instrument, såsom avtalsklausuler eller bindande företagsbestämmelser, förutsatt att dessa instrument fastställer särskilda garantier och skyddsmekanismer och inte kringgås av andra lagstiftningsramar.

39. Europaparlamentet anser att kommissionen har underlåtit att vidta åtgärder för att avhjälpa de välkända bristerna i det nuvarande genomförandet av Safe Harbour.

40. Europaparlamentet uppmanar kommissionen att lägga fram åtgärder för ett omedelbart tillfälligt upphävande av kommissionens beslut 2000/520/EG, där Safe Harbour-principerna om integritetsskydd och de frågor och svar som Förenta staternas handelsministerium utfärdat i samband med detta förklarades adekvata. Förenta staternas myndigheter uppmanas därför att lägga fram ett förslag om ett nytt system för överföring av personuppgifter från EU till Förenta staterna. Detta nya system måste vara förenligt med unionslagstiftningens uppgiftsskyddskrav och uppfylla kraven på tillräcklig skyddsnivå.

41. Europaparlamentet uppmanar medlemsstaternas behöriga myndigheter, särskilt uppgiftsskyddsmyndigheterna, att utnyttja sina befintliga befogenheter och omedelbart stoppa dataflöden till alla organisationer som har självcertifierat att de följer de amerikanska Safe Harbour-principerna, samt att kräva att sådana dataflöden endast sker inom ramen för andra instrument och på villkor att dessa instrument omfattar nödvändiga skyddsmekanismer och garantier för personlig integritet och enskilda individers grundläggande fri- och rättigheter.

42. Europaparlamentet uppmanar kommissionen att senast i december 2014 lägga fram en heltäckande bedömning av det amerikanska regelverket för integritetsskydd som omfattar kommersiell verksamhet, brottsbekämpning och underrättelseverksamhet samt konkreta rekommendationer som bygger på att det saknas en allmän dataskyddslag i Förenta staterna. Kommissionen uppmanas att samarbeta med Förenta staternas regering för att fastställa en lagstiftningsram som medför en hög skyddsnivå för enskilda individer när det gäller skyddet av deras personuppgifter då de överförs till Förenta staterna och säkerställa överensstämmelsen mellan EU:s och Förenta staternas regelverk för integritetsskydd.

Överföring till tredjeland med beslut om adekvat skydd

43. Europaparlamentet påminner om att det i direktiv 95/46/EG fastställs att överföring av personuppgifter till tredjeland endast får ske om det aktuella tredjelandet säkerställer en adekvat skyddsnivå, utan att detta påverkar tillämpningen av de nationella bestämmelser som antagits till följd av de andra bestämmelserna i direktivet. Syftet med denna bestämmelse är att säkerställa fortsatt skydd enligt EU:s uppgiftsskyddslagstiftning när personuppgifter överförs till länder utanför EU.

44. Europaparlamentet påminner om att det i direktiv 95/46/EG även fastställs att bedömningen av huruvida ett tredjelands skyddsnivå är adekvat ska göras med hänsyn till alla de omständigheter som har samband med en överföring eller en grupp av överföringar. Parlamentet påminner även om att kommissionen genom detta direktiv förses med genomförandebefogenheter att förklara att ett tredjeland säkerställer en adekvat skyddsnivå mot bakgrund av de kriterier som fastställs i direktiv 95/46/EG. Kommissionen ges genom direktiv 95/46/EG även befogenhet att förklara att ett tredjeland inte säkerställer en adekvat skyddsnivå.

45. Europaparlamentet påminner om att medlemsstaterna i det senare fallet måste vidta de åtgärder som är nödvändiga för att hindra överföring av uppgifter av samma slag till tredjelandet i fråga. Kommissionen bör inleda förhandlingar för att avhjälpa den situation som uppstått.

46. Europaparlamentet uppmanar kommissionen och medlemsstaterna att utan dröjsmål bedöma om skyddsnivåerna i Nya Zeelands uppgiftsskyddslag och i den kanadensiska lagen om elektroniska handlingar och skydd för personuppgifter (Personal Information Protection and Electronic Documents Act), som förklarades adekvata i kommissionens beslut 2013/65/EU och 2002/2/EG, har påverkats av dessa länders nationella underrättelseorgans medverkan till massövervakningen av EU-medborgare och att vid behov vidta lämpliga åtgärder för att tillfälligt upphäva eller återkalla besluten om adekvat skydd. Parlamentet uppmanar också kommissionen att utvärdera situationen för andra länder vars skydd har bedömts vara adekvat. Parlamentet förväntar sig att kommissionen avlägger rapport till parlamentet om sina resultat beträffande de ovannämnda länderna senast i december 2014.

Överföringar på grundval av avtalsklausuler och andra instrument

47. Europaparlamentet påminner om att nationella dataskyddsmyndigheter har uppgett att varken standardavtalsklausuler eller bindande företagsbestämmelser är skrivna med tanke på situationer där åtkomst till personuppgifter sker i massövervakningssyfte, och att sådan åtkomst inte skulle ligga i linje med de undantagsklausuler till avtalsklausuler eller bindande företagsbestämmelser som avser exceptionella undantag på grund av legitima intressen i ett demokratiskt samhälle när detta är nödvändigt och proportionerligt.

48. Europaparlamentet uppmanar medlemsstaterna att förbjuda eller avbryta dataflöden till tredjeländer på grundval av standardavtalsklausuler, avtalsklausuler eller bindande företagsbestämmelser som godkänts av de nationella behöriga myndigheterna om det är troligt att den lagstiftning som gäller uppgiftsmottagarna ställer krav på dessa som överstiger de begränsningar som är strikt nödvändiga, adekvata och proportionerliga i ett demokratiskt samhälle och som sannolikt kommer att ha en skadlig inverkan på de garantier som ges genom den tillämpliga uppgiftsskyddslagstiftningen och standardavtalsklausulerna, eller för att fortsatt överföring skulle medföra en risk för allvarlig skada för de registrerade.

49. Europaparlamentet uppmanar artikel 29-gruppen att utfärda riktlinjer och rekommendationer om de garantier och skydd som ska ingå i avtalsmässiga instrument för internationell överföring av personuppgifter från EU för att säkerställa skydd för den personliga integriteten och för enskilda individers grundläggande fri- och rättigheter, med särskild hänsyn till tredjelandets lagstiftning om underrättelseverksamhet och nationell säkerhet och till om företag som mottar data i ett tredjeland medverkar till ett tredjelands underrättelseorgans massövervakningsverksamhet.

50. Europaparlamentet uppmanar kommissionen att omgående granska de standardavtalsklausuler den har upprättat för att bedöma om de ger nödvändigt skydd när det gäller åtkomst till personuppgifter som överförts enligt klausulerna i underrättelsesyften och, om nödvändigt, att se över dem.

Överföringar på grundval av avtalet om ömsesidig rättslig hjälp

51. Europaparlamentet uppmanar kommissionen att före slutet av 2014 genomföra en djupgående bedömning av det befintliga avtalet om ömsesidig rättslig hjälp, i enlighet med artikel 17 i detta avtal, för att kontrollera hur det genomförts i praktiken och i synnerhet om Förenta staterna har utnyttjat avtalet effektivt för att erhålla information eller bevis i EU och om avtalet har kringgåtts för att förvärva information direkt i EU, samt att bedöma konsekvenserna för individers grundläggande rättigheter. En sådan bedömning bör inte enbart förlita sig på amerikanska officiella uttalanden som tillräcklig grund för analysen, utan även bygga på särskilda EU-utvärderingar. Denna djupgående översyn bör också omfatta följderna av tillämpningen av unionens konstitutionella struktur på detta instrument för att göra det förenligt med unionslagstiftningen, med särskild hänsyn till protokoll 36 och artikel 10 i avtalet och förklaring 50 om detta protokoll. Parlamentet uppmanar också rådet och kommissionen att utvärdera de bilaterala avtalen mellan medlemsstaterna och Förenta staterna för att se till att de stämmer överens med de avtal som EU har ingått eller beslutar ingå med Förenta staterna.

Ömsesidig rättslig hjälp i brottmål inom EU

52. Europaparlamentet uppmanar rådet och kommissionen att informera parlamentet om medlemsstaternas faktiska användning av konventionen om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater, särskilt avdelning III om avlyssning av telemeddelanden. Parlamentet uppmanar kommissionen att i enlighet med förklaring 50 lägga fram ett förslag om protokoll 36, såsom begärts, före slutet av 2014 för att anpassa protokollet till Lissabonfördragets ramar.

Överföringar baserade på TFTP- och PNR-avtalen

53. Europaparlamentet anser att den information som lämnats av kommissionen och Förenta staternas finansministerium inte klargör om Förenta staternas underrättelseorgan har tillgång till finansiella Swift-uppgifter i EU genom att avlyssna Swift-nätverk eller bankers operativsystem eller kommunikationsnät, ensamt eller i samarbete med EU:s nationella underrättelsetjänster och utan att använda sig av befintliga bilaterala kanaler för ömsesidig rättslig hjälp och rättsligt samarbete.

Onsdagen den 12 mars 2014

54. Europaparlamentet påminner om sin resolution av den 23 oktober 2013 och uppmanar kommissionen att upphäva TFTP-avtalet.

55. Europaparlamentet uppmanar kommissionen att reagera på farhågorna om att tre av de största databokningssystem som används av flygbolag i hela världen är baserade i Förenta staterna samt att PNR-uppgifter sparas i molnsystem som drivs på Förenta staternas mark enligt Förenta staternas lagstiftning, som inte erbjuder ett adekvat uppgiftsskydd.

Ramavtal om uppgiftsskydd på området för polissamarbete och rättsligt samarbete (”paraplyavtalet”)

56. Europaparlamentet anser att en tillfredsställande lösning enligt ”paraplyavtalet” är en förutsättning för att fullt förtroende mellan de transatlantiska parterna ska kunna återupprättas.

57. Europaparlamentet anser att förhandlingarna med Förenta staterna om ”paraplyavtalet” omedelbart bör återupptas, vilket bör medföra att unionsmedborgarnas rättigheter likställs med de rättigheter som medborgarna i Förenta staterna åtnjuter. Parlamentet betonar dessutom att detta avtal bör bana väg för effektiva och genomförbara administrativa och rättsliga åtgärder för alla EU-medborgare i Förenta staterna utan någon diskriminering.

58. Europaparlamentet uppmanar kommissionen och rådet att inte ta initiativ till några nya separata avtal eller överenskommelser om överföring av personuppgifter i brottsbekämpande syfte med Förenta staterna innan ”paraplyavtalet” har trätt i kraft.

59. Europaparlamentet uppmanar med kraft kommissionen att i detalj rapportera om de olika punkterna i förhandlingsmandatet och om det aktuella läget senast i april 2014.

Reform av uppgiftsskyddet

60. Europaparlamentet uppmanar rådets ordförandeskap och medlemsstaterna att påskynda sitt arbete med hela uppgiftsskyddspaketet så att det kan antas 2014. Syftet med detta är att EU-medborgarna ska omfattas av en hög uppgiftsskyddsnivå inom en mycket snar framtid. Ett starkt engagemang och helhjärtat stöd från rådets sida är en nödvändig förutsättning för att man ska visa trovärdighet och tyngd gentemot tredjeländer.

61. Europaparlamentet understryker att både uppgiftsskyddsförordningen och dataskyddsdirektivet är nödvändiga för att skydda enskilda personers grundläggande rättigheter. Båda dessa rättsakter måste därför behandlas som ett paket och antas samtidigt, så att all uppgiftsbehandlingsverksamhet i EU alltid har ett starkt skydd. Parlamentet betonar att det inte kommer att vidta några ytterligare samarbetsåtgärder i brottsbekämpningssyfte förrän rådet har inlett förhandlingar med parlamentet och kommissionen om uppgiftsskyddspaketet.

62. Europaparlamentet påminner om att koncepten ”inbyggt integritetsskydd” och ”integritetsskydd som standard” stärker uppgiftsskyddet och bör ha status som riktlinjer för alla produkter, tjänster och system som erbjuds på internet.

63. Europaparlamentet anser att större öppenhet och bättre säkerhetsstandarder för internet och telekommunikation är en nödvändig princip för ett bättre uppgiftsskyddssystem. Kommissionen uppmanas därför att lägga fram ett lagstiftningsförslag om standardiserade allmänna villkor och bestämmelser för internet- och telekommunikationstjänster och att ge ett tillsynsorgan i uppdrag att övervaka efterlevnaden av dessa allmänna villkor och bestämmelser.

Datormolntjänster

64. Europaparlamentet noterar att ovannämnda metoder har påverkat förtroendet för amerikanska leverantörer av molntjänster och molnleverantörer negativt. Parlamentet betonar därför att det är mycket viktigt att utveckla europeiska datormoln och it-lösningar för att skapa tillväxt och sysselsättning samt förtroende för molntjänster och molnleverantörer, och för att säkerställa ett starkt skydd av personuppgifter.

65. Europaparlamentet uppmanar alla offentliga organ i unionen att inte använda sig av molntjänster som eventuellt omfattas av annan lagstiftning än EU-lagstiftning.

66. Europaparlamentet upprepar sin allvarliga oro över det obligatoriska direkta utlämnandet av EU-medborgares personuppgifter och information som behandlats inom ramen för molnavtal till myndigheter i tredjeländer från molnleverantörer som omfattas av tredjeländers lagstiftning eller använder lagringsservrar i tredjeländer, liksom sin allvarliga oro över direkt fjärrtillträde till personuppgifter och information som behandlas av brottsbekämpande myndigheter och underrättelsetjänster i tredjeländer.

67. Europaparlamentet beklagar djupt att sådant tillträde vanligen sker genom att myndigheter i tredjeländer direkt verkställer sina egna rättsliga bestämmelser utan att använda sig av de internationella instrumenten när det gäller rättsligt samarbete, såsom avtal om ömsesidig rättslig hjälp eller andra former av rättsligt samarbete.

68. Europaparlamentet uppmanar kommissionen och medlemsstaterna att påskynda arbetet för att upprätta Europeiska partnerskapet för molntjänster och göra det civila samhället och det tekniska samfundet, exempelvis Internet Engineering Task Force (IETF), fullt delaktigt i detta samt införliva uppgiftsskyddsaspekter.

69. Europaparlamentet uppmanar eftertryckligen kommissionen att i samband med förhandlingarna om internationella avtal som inbegriper behandling av personuppgifter särskilt beakta de risker och utmaningar som molntjänster innebär för de grundläggande rättigheterna, särskilt – men inte uteslutande – rätten till privatliv och skydd av personuppgifter, i enlighet med artiklarna 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Vidare uppmanas kommissionen eftertryckligen att notera förhandlingspartnerns nationella bestämmelser om brottsbekämpande myndigheters och underrättelsetjänsters åtkomst till personuppgifter som behandlas genom molntjänster, särskilt genom att kräva att åtkomst kan beviljas till sådana uppgifter enbart med full respekt för vederbörliga rättsliga förfaranden och på en entydig rättslig grund samt att det specificeras exakt vilka villkor som ska gälla för åtkomst, vad syftet är med åtkomsten, vilka säkerhetsåtgärder som ska vidtas när uppgifterna överlämnas, vilka rättigheter som ska gälla för den enskilda personen samt vilka bestämmelser som ska gälla för tillsyn och en effektiv prövningsmekanism.

70. Europaparlamentet påminner om att alla företag som tillhandahåller tjänster inom EU alltid, undantagslöst, måste följa EU-lagstiftningen och kan hållas ansvariga för överträdelser av den. Parlamentet framhåller vikten av effektiva, proportionerliga och avskräckande administrativa sanktioner som kan sättas in mot leverantörer av datormolntjänster som inte följer EU:s standarder för uppgiftsskydd.

71. Europaparlamentet uppmanar kommissionen och medlemsstaternas behöriga myndigheter att bedöma i vilken omfattning EU:s bestämmelser om personlig integritet och uppgiftsskydd har överträtts genom samarbetet mellan EU:s rättsliga enheter och säkerhetstjänster eller genom att domstolsbeslut har godtagits från myndigheter i tredjeländer med begäran om personuppgifter gällande EU-medborgare, i strid med EU:s uppgiftsskyddslagstiftning.

72. Europaparlamentet uppmanar företag som tillhandahåller nya tjänster med hjälp av storskaliga datavolymer (”Big Data”) och nya tillämpningar, till exempel ”Sakernas Internet”, att integrera uppgiftsskyddsåtgärder redan under utvecklingsstadiet i syfte att upprätthålla ett starkt förtroende hos medborgarna.

Avtal om det transatlantiska partnerskapet för handel och investeringar

73. Europaparlamentet erkänner att EU och Förenta staterna förhandlar om ett transatlantiskt partnerskap för handel och investeringar, som är av stor strategisk betydelse för att skapa fortsatt ekonomisk tillväxt

74. Europaparlamentet betonar kraftfullt – med hänsyn till den digitala ekonomins betydelse i förhållandet och för att återupprätta förtroendet mellan EU och Förenta staterna – att parlamentets samtycke till det slutliga avtalet om det transatlantiska partnerskapet för handel och investeringar skulle kunna äventyras så länge den urskillningslösa massövervakningen liksom avlyssningen av EU-institutioner och diplomatiska representationer inte har stoppas helt och hållet och så länge man inte hittar en lämplig lösning i fråga om EU-medborgarnas rätt till uppgiftsskydd, inbegripet

administrativ och rättslig prövning. Parlamentet betonar att det endast kan samtycka till det slutliga avtalet om det transatlantiska partnerskapet för handel och investeringar under förutsättning att avtalet fullt ut respekterar bland annat de grundläggande rättigheter som fastställs i EU:s stadga samt att skyddet av enskilda personers privatliv i samband med behandling och spridning av personuppgifter även i fortsättningen regleras av artikel XIV i Gats. Parlamentet betonar att EU:s uppgiftsskyddslagstiftning inte kan anses vara ett ”medel för godtycklig eller oberättigad diskriminering” vid tillämpningen av artikel XIV i Gats.

Demokratisk tillsyn över underrättelsetjänster

75. Europaparlamentet betonar att tillsynen över underrättelsetjänsternas verksamhet bör grundas på såväl demokratisk legitimitet (kraftfull rättslig ram, förhandsgodkännande och efterhandskontroll) som lämplig teknisk behörighet och expertis. Större delen av EU:s och Förenta staternas aktuella tillsynsorgan lider dock stor brist på bådadera, i synnerhet teknisk behörighet.

76. Europaparlamentet uppmanar – som det tidigare gjort i fråga om Echelon – alla de nationella parlament som ännu inte har gjort det att inrätta en meningsfull tillsyn över underrättelseverksamhet och i detta sammanhang engagera parlamentsledamöter eller expertorgan med rättsliga utredningsbefogenheter. Parlamentet uppmanar de nationella parlamenten att se till att sådana tillsynskommittéer eller tillsynsorgan har tillräckliga resurser, teknisk expertis och rättsliga medel, inbegripet rätten att göra platsbesök, för att kunna kontrollera underrättelsetjänsterna effektivt.

77. Europaparlamentet begär att det tillsätts en grupp bestående av ledamöter och experter som, på ett transparent sätt och i samarbete med de nationella parlamenten, ska granska rekommendationerna för en ökad demokratisk tillsyn, inklusive parlamentarisk tillsyn, av underrättelsetjänsterna samt ett ökat tillsynssamarbete inom EU, särskilt när det gäller dess gränsöverskridande dimension. Parlamentet anser att gruppen framför allt bör granska möjligheten till europeiska minimistandarder eller riktlinjer för (föregående eller efterföljande) tillsyn över underrättelsetjänsterna på grundval av bästa praxis och rekommendationer från internationella organ (FN, Europarådet), inklusive frågan om tillsynsorgan som betraktas som tredjeparter enligt ”tredjepartsregeln”, eller principen om ”upphovsmannens kontroll”, när det gäller tillsyn och ansvarsskyldighet i fråga om underrättelser från främmande länder, kriterier för ökad insyn utifrån den allmänna principen om tillgång till information och de så kallade Tshwane-principerna ([1]) samt principer för hur länge och i vilken omfattning en övervakning får pågå, i syfte att säkerställa att övervakningen är proportionerlig och begränsad till ändamålet.

78. Europaparlamentet uppmanar denna grupp att utarbeta en rapport till, och hjälpa till med förberedelserna inför, en konferens som parlamentet ska anordna med nationella tillsynsorgan, antingen parlamentariska eller oberoende, senast i början av 2015.

79. Europaparlamentet uppmanar medlemsstaterna att utnyttja bästa praxis för att förbättra tillsynsorganens tillgång till information om underrättelseverksamhet (inbegripet sekretessbelagd information och information från andra tjänster) samt införa befogenhet att göra platsbesök och fastställa omfattande förhörsbefogenheter, tillräckliga resurser och teknisk expertis, ett fullständigt oberoende gentemot sina respektive regeringar samt en rapporteringsskyldighet till sina respektive parlament.

80. Europaparlamentet uppmanar medlemsstaterna att utveckla samarbetet mellan tillsynsorganen, särskilt inom European Network of National Intelligence Reviewers (ENNIR).

81. Europaparlamentet uppmanar eftertryckligen vice ordföranden för kommissionen/unionens höga representant för utrikes frågor och säkerhetspolitik att för parlamentets ansvariga organ regelbundet redovisa verksamheten vid EU:s underrättelseanalyscentrum (EU Intcen), som är en del av Europeiska utrikestjänsten, bland annat dess fulla efterlevnad av de grundläggande rättigheterna och EU:s tillämpliga uppgiftsskyddsregler, som gör det möjligt för parlamentet att förbättra sin tillsyn över EU-politikområdenas externa dimension. Kommissionen och vice ordföranden/den höga representanten uppmanas eftertryckligen att lägga fram ett förslag till rättslig grund för verksamheten vid IntCen, om det planeras några operationer eller framtida befogenheter på underrättelseområdet eller någon egen uppgiftsinsamling som kan inverka på EU:s strategi för inre säkerhet.

([1]) The Global Principles on National Security and the Right to Information, juni 2013.

82. Europaparlamentet uppmanar kommissionen att senast i december 2014 lägga fram ett förslag till förfarande för EU:s säkerhetsprövning av alla EU:s tjänstemän, eftersom det i det aktuella systemet, som bygger på den säkerhetsprövning som genomförs av den medlemsstat där de är medborgare, fastställs olika krav och längd på förfarandena inom de nationella systemen, vilket leder till olika behandlingar av parlamentsledamöter och deras personal beroende på deras nationalitet.

83. Europaparlamentet påminner om bestämmelserna i det interinstitutionella avtalet mellan Europaparlamentet och rådet om överförande till och hantering inom parlamentet av säkerhetsskyddsklassificerade uppgifter som innehas av rådet vilka rör andra frågor än de som omfattas av den gemensamma utrikes- och säkerhetspolitiken, som bör användas för att förbättra tillsynen på EU-nivå.

EU-organ

84. Europaparlamentet uppmanar den gemensamma tillsynsmyndigheten för Europol och nationella uppgiftsskyddsmyndigheter att genomföra en gemensam tillsyn före utgången av 2014 i syfte att klarlägga om den information och de personuppgifter som delas med Europol har förvärvats av nationella myndigheter enligt lag, i synnerhet om informationen eller uppgifterna ursprungligen förvärvades av underrättelsetjänsterna i EU eller ett tredjeland och om lämpliga åtgärder har vidtagits för att förhindra att sådan information eller sådana uppgifter används eller sprids vidare. Parlamentet anser inte att Europol bör behandla någon information eller några uppgifter som har erhållits i strid med grundläggande rättigheter som skyddas enligt stadgan om de grundläggande rättigheterna.

85. Europaparlamentet uppmanar Europol att till fullo utnyttja sitt mandat till att begära att medlemsstaternas behöriga myndigheter inleder brottsutredningar i fråga om stora it-angrepp och it-brott med potentiellt gränsöverskridande följder. Europols mandat bör utökas så att byrån kan inleda sina egna utredningar vid misstanke om ett fientligt angrepp mot nät- och informationssystemet i två eller fler medlemsstater eller unionsorgan ([1]). Kommissionen uppmanas att se över Europeiska it-brottscentrumet, som sorterar under Europol, och vid behov lägga fram ett förslag till ett heltäckande ramverk för att stärka dess befogenheter.

Yttrandefrihet

86. Europaparlamentet uttrycker stark oro över de ökande hoten mot pressfriheten och den avskräckande effekten på journalister genom hot från statliga myndigheter, i synnerhet när det gäller meddelarskyddet för journalisters källor. Parlamentet upprepar uppmaningarna från sin resolution av den 21 maj 2013 om ”EU-stadgan: Standarder för mediefrihet i EU”.

87. Europaparlamentet noterar fängslandet av David Miranda och de brittiska myndigheternas beslagtagande av hans material enligt förteckning 7 i Terrorism Act 2000 (och dessutom uppmaningen till The Guardian att förstöra eller överlämna materialet) och är bekymrat över att detta kan utgöra en allvarlig kränkning av rätten till yttrandefrihet och mediefrihet enligt artikel 10 i Europakonventionen och artikel 11 i EU:s stadga och att lagstiftning för att bekämpa terrorism kan missbrukas i dessa fall.

88. Europaparlamentet uppmärksammar den svåra situation som visselblåsare och de personer som stöder dem, bl.a. journalister, hamnar i på grund av deras avslöjanden. Kommissionen uppmanas att utreda huruvida ett framtida lagstiftningsförslag om ett verkningsfullt och heltäckande europeiskt skyddsprogram för visselblåsare, vilket redan efterlysts i parlamentets resolution av den 23 oktober 2013, även bör omfatta andra områden där unionen är behörig. Särskild hänsyn bör här tas till uppgiftslämnandets komplexitet på underrättelseområdet. Medlemsstaterna uppmanas att ingående undersöka möjligheten att ge visselblåsare internationellt skydd mot åtal.

([1]) Europaparlamentets ståndpunkt av den 25 februari 2014 om förslaget till Europaparlamentets och rådets förordning om Europeiska unionens organ för samarbete och fortbildning inom brottsbekämpning (Europol) (Antagna texter, P7_TA(2014)0121).

89. Europaparlamentet uppmanar medlemsstaterna att se till att deras lagstiftning, särskilt när det gäller nationell säkerhet, innebär ett säkert alternativ till tystnad för att avslöja eller rapportera oegentligheter, t.ex. korruption, brott, åsidosättande av rättslig skyldighet, felaktiga domslut och maktmissbruk, vilket också ligger i linje med bestämmelserna i olika internationella instrument (FN och Europarådet) mot korruption, principerna i Europarådets parlamentariska församlings resolution 1729 (2010), Tshwane-principerna etc.

EU:s it-säkerhet

90. Europaparlamentet påpekar att de nyligen inträffade incidenterna tydligt visar på den akuta sårbarheten inom EU – särskilt för EU-institutionerna, de nationella regeringarna och parlamenten, de stora europeiska företagen och de europeiska it-infrastrukturerna och it-nätverken – för avancerade angrepp med komplexa program och sabotageprogram. Parlamentet konstaterar att dessa angrepp kräver sådana ekonomiska och mänskliga resurser att de sannolikt kommer från statliga enheter som agerar för utländska regeringars räkning. Parlamentet ser i detta sammanhang fallet med hackandet av eller intrånget i telekommunikationsföretaget Belgacom som ett oroande exempel på ett angrepp mot EU:s it-kapacitet. Parlamentet understryker att förstärkningar av EU:s it-kapacitet och it-säkerhet också minskar EU:s sårbarhet för it-angrepp som genomförs av stora brottsorganisationer eller terroristgrupper.

91. Europaparlamentet anser att de avslöjanden om massövervakning som har lett till denna kris kan användas som en möjlighet för Europa att ta initiativet till och bygga upp, som en strategisk åtgärd av högsta prioritet, en stark och fristående it-nyckelresurskapacitet. För att återupprätta detta förtroende bör en sådan europeisk it-kapacitet i möjligaste mån baseras på öppna standarder och programvara – och om möjligt maskinvara – med öppen källkod och möjliggöra insyn i och översyn av hela leveranskedjan, från processorns utformning till själva tillämpningen. För att återvinna konkurrenskraften inom den strategiska sektorn för it-tjänster krävs en ny digital reform med gemensamma, storskaliga insatser av EU-institutionerna, medlemsstaterna, forskningsinstituten, näringslivet och det civila samhället. Parlamentet uppmanar kommissionen och medlemsstaterna att använda offentlig upphandling som en hävstång för att ge stöd för en sådan resurskapacitet inom EU genom att göra EU-standarder för säkerhet och integritet till ett grundkrav vid offentlig upphandling av varor och tjänster på it-området. Kommissionen uppmanas därför eftertryckligen att se över de nuvarande upphandlingsmetoderna när det gäller uppgiftsbehandling för att överväga att begränsa anbudsförfarandena till certifierade företag, och eventuellt EU-företag, om säkerhetsintressen eller andra vitala intressen står på spel.

92. Europaparlamentet fördömer starkt att underrättelsetjänster har försökt att sänka it-säkerhetsstandarder och installera bakdörrar i många olika slags it-system. Parlamentet uppmanar kommissionen att lägga fram lagstiftningsförslag om att förbjuda bakdörrar för brottsbekämpande organ. Parlamentet rekommenderar följaktligen att programvara med öppen källkod används i alla miljöer där it-säkerheten är viktig.

93. Europaparlamentet uppmanar alla medlemsstater, kommissionen, rådet och Europeiska rådet att ge sitt fulla stöd, bland annat genom ekonomiska resurser till forskning och utveckling, till utvecklingen av europeisk innovation och teknisk kapacitet hos it-relaterade verktyg, företag och leverantörer (av maskinvara, programvara, tjänster och nät), bland annat i it-säkerhetssyfte samt krypterings- och kryptografiförmåga. Alla ansvariga EU-institutioner och medlemsstater uppmanas att investera i EU-intern lokal och oberoende teknik och att kraftigt utveckla och utöka upptäcksförmågan.

94. Europaparlamentet uppmanar kommissionen, standardiseringsorganen och Enisa att fram till och med december 2014 utveckla minimistandarder och minimiriktlinjer för säkerhet och integritet för it-relaterade system, nät och tjänster, inklusive datormolntjänster, för att bättre skydda EU-medborgarnas personuppgifter och alla it-systems integritet. Parlamentet anser att dessa standarder skulle kunna bli riktmärken för nya globala standarder och bör fastställas i en öppen och demokratisk process, snarare än att drivas igenom av ett enda land, en enda instans eller ett enda multinationellt företag. Även om berättigade hänsyn måste tas till brottsbekämpning och underrättelseverksamhet, får dessa inte leda till en allmän underminering av alla it-systems tillförlitlighet. Parlamentet uttrycker sitt stöd för de beslut som Internet Engineering Task Force (IETF) nyligen fattat om att inkludera regeringar i hotmodellen för internetsäkerhet.

95. Europaparlamentet påpekar att nationella tillsynsmyndigheter på telekomområdet och i vissa fall även telekomföretag tydligt har åsidosatt sina användares och kunders it-säkerhet. Parlamentet uppmanar kommissionen att fullt ut använda alla sina nuvarande befogenheter enligt ramdirektivet om integritet och elektronisk kommunikation och telekommunikation för att stärka skyddet för integriteten i kommunikationen genom att införa åtgärder för att se till att terminalutrustning är kompatibel med användarnas rätt att ha kontroll över och skydda sina personuppgifter, och att säkerställa en hög säkerhetsnivå i nät och tjänster för telekommunikation, även genom krav på avancerad obruten kryptering av kommunikationen.

96. Europaparlamentet stöder EU:s it-strategi men anser att den inte omfattar alla möjliga hot och bör utvidgas till att omfatta aktioner som stater genomför med illvilligt uppsåt. Parlamentet understryker behovet av en bättre it-säkerhet och motståndskraftiga it-system.

97. Europaparlamentet uppmanar kommissionen att senast i januari 2015 presentera en handlingsplan för att ge EU större självständighet inom it-sektorn, med en mer samordnad taktik för att öka Europas tekniska förmåga på it-området (för it-system, utrustning, tjänster, datormolntjänster, kryptering och anonymisering) och för förmågan att skydda viktig it-infrastruktur (även i fråga om ägande och sårbarhet).

98. Europaparlamentet uppmanar kommissionen att inom ramen för nästa arbetsprogram för Horisont 2020-programmet tillföra mer resurser för att stärka Europas forskning, utveckling, innovationer och utbildning på it-området, särskilt när det gäller integritetsförstärkande teknik och infrastruktur, kryptologi, datorsäkerhet, bästa möjliga säkerhetslösningar med öppen källkod och andra tjänster med anknytning till informationssamhället. Kommissionen uppmanas också att främja den inre marknaden för europeisk program- och maskinvara samt krypterade kommunikationsmedel och kommunikationsinfrastruktur, bland annat genom att inom EU utarbeta en omfattande branschstrategi för it-branschen. Parlamentet anser att små och medelstora företag spelar en viktig roll inom forskningen. Parlamentet betonar att inga EU-medel bör beviljas till projekt som har som enda syfte att utveckla verktyg för olaglig åtkomst till it-system.

99. Europaparlamentet uppmanar kommissionen att kartlägga den nuvarande ansvarsfördelningen och att senast i december 2014 utvärdera behovet av ett bredare mandat, bättre samordning och/eller ytterligare resurser och tekniska möjligheter för Enisa, Europols center för it-brottslighet och andra EU-center med specialistkompetens, CERT-EU och EDPS för att göra det möjligt för dem att spela en central roll när det gäller att säkerställa europeiska kommunikationssystem, på ett effektivare sätt förebygga och utreda grova it-brott inom EU och göra (eller hjälpa medlemsstater och EU-organ att göra) tekniska utredningar på plats vid grova it-brott. Kommissionen uppmanas framför allt att överväga att stärka Enisas roll när det gäller att skydda EU-institutionernas interna system och att inom ramen för Enisa inrätta en incidenthanteringsorganisation (Cert) för EU och medlemsstaterna.

100. Europaparlamentet ber kommissionen överväga behovet av en europeisk it-akademi som samlar de bästa oberoende europeiska och internationella experterna på alla relaterade områden och får i uppdrag att ge alla EU:s relevanta institutioner och organ vetenskaplig rådgivning om informationsteknik, inklusive säkerhetsrelaterade strategier.

101. Europaparlamentet uppmanar de behöriga tjänsteenheterna inom parlamentets generalsekretariat att under ansvar av parlamentets talman senast i juni 2015, med en interimsrapport senast i december 2014, göra en utförlig granskning och utvärdering av tillförlitligheten för parlamentets it-säkerhet, med inriktning på följande: budgetresurser, personalresurser, tekniska resurser, intern organisation och alla relevanta element, för att skapa en hög säkerhetsnivå i parlamentets it-system. Parlamentet anser att man i en sådan utvärdering bör ge åtminstone en analys av och information och rekommendationer när det gäller följande:

— Behovet av regelbundna, noggranna och oberoende säkerhetsgranskningar och intrångstester, med ett urval av externa säkerhetsexperter under öppenhet och med garantier för deras kvalifikationer i förhållande till tredjeländer eller andra typer av särintressen.

— Inkluderandet av specifika bästa praxis-baserade krav på it-säkerhet/-integritet i anbudsförfaranden för nya it-system, inklusive möjligheten att ställa krav på programvara med öppen källkod som ett inköpsvillkor eller krav på att betrodda EU-företag deltar i upphandlingen när känsliga, säkerhetsrelaterade områden berörs.

Onsdagen den 12 mars 2014

— Förteckningen över de företag som har avtal med parlamentet på it- och telekomområdena, med hänsyn till all information som uppdagats om deras samarbete med underrättelseorgan (såsom avslöjandena om NSA:s avtal med ett företag som RSA, vars produkter parlamentet använder i det förmenta syftet att förhindra sina ledamöters och sin personals fjärråtkomst till sina uppgifter), inklusive eventuell möjlighet att få samma tjänster från andra, helst europeiska, företag.

— Tillförlitligheten och stabiliteten hos all programvara, särskilt kommersiell programvara som finns i handeln, som EU-institutionerna använder i sina it-system med avseende på intrång från brottsbekämpande myndigheter och underrättelsetjänster inom EU eller från tredjeländer, även med hänsyn till relevanta internationella standarder, principer för bästa praxis för hantering av säkerhetsrisker och efterlevnad av EU:s säkerhetsstandarder för nätverksinformation gällande säkerhetsbrott.

— Användningen av fler system med öppen källkod.

— Insatser och åtgärder för att hantera den ökade användningen av mobila verktyg (t.ex. smarta telefoner och surfplattor, både yrkesmässigt och privat) och dess effekter på systemets it-säkerhet.

— Säkerheten i kommunikationen mellan parlamentets olika arbetsplatser och i de it-system som används inom parlamentet.

— Användningen och placeringen av servrar och it-center för parlamentets it-system och konsekvenserna för systemens säkerhet och integritet.

— Den praktiska tillämpningen av de befintliga reglerna för säkerhetsöverträdelser och den omedelbara anmälan av dessa till de behöriga myndigheterna från de operatörer som driver offentliga telenät.

— Parlamentets användning av molnbaserade datortjänster och lagringstjänster, med information om vilka typer av data som lagras i molnet, om hur innehållet och åtkomsten till det skyddas och var molnservrarna finns, med ett klargörande av det tillämpliga regelverket för det dataskydd och underrättelser, samt med en bedömning av möjligheten att endast använda molnservrar som är baserade på EU:s territorium.

— En plan som möjliggör användning av fler tekniska krypteringslösningar, särskilt autentiserad obruten kryptering för alla it- och kommunikationstjänster såsom datormolntjänster, e-post, snabbmeddelanden och telefoni.

— Användningen av elektroniska signaturer i e-post.

— En plan för att använda en standardkrypteringsmetod, såsom GNU Privacy Guard, för e-post, vilket samtidigt skulle möjliggöra användning av digitala signaturer.

— Möjligheten att skapa en säker tjänst för snabbmeddelanden inom parlamentet, som möjliggör en säker kommunikation där endast krypterat innehåll är tillgängligt på servern.

102. Europaparlamentet uppmanar alla EU:s institutioner och organ, i synnerhet Europeiska rådet, rådet, Europeiska utrikestjänsten (inklusive EU-delegationerna), kommissionen, Europeiska unionens domstol och Europeiska centralbanken, att i samarbete med Enisa, Europol och Cert vidta liknande åtgärder senast i juni 2015, med en interimsrapport senast i december 2014. Medlemsstaterna uppmanas att genomföra liknande bedömningar.

103. Europaparlamentet understryker att det bör göras bedömningar av budgetbehoven för EU:s yttre åtgärder, att inledande åtgärder utan dröjsmål bör vidtas för Europeiska utrikestjänsten samt att lämpliga medel behöver anslås i budgetförslaget för 2015.

104. Europaparlamentet anser att de storskaliga it-system som används inom området med frihet, säkerhet och rättvisa, såsom Schengens informationssystem II, Informationssystemet för viseringar, Eurodac och eventuella framtida system såsom EU-ESTA, bör utvecklas och drivas på ett sådant sätt att uppgifter inte kan komma att äventyras till följd av förfrågningar från myndigheter i tredjeländer. Parlamentet uppmanar eu-LISA att före utgången av 2014 återrapportera till parlamentet om de befintliga systemens tillförlitlighet.

105. Europaparlamentet uppmanar kommissionen och Europeiska utrikestjänsten att vidta åtgärder på internationell nivå, framför allt tillsammans med FN, och i samarbete med berörda partner genomföra en EU-strategi för demokratisk styrning av internet i syfte att förhindra otillbörlig påverkan av ICANN:s och IANA:s verksamhet från en enskild enhet eller ett enskilt företag eller land genom att se till att alla berörda parter företräds på lämpligt sätt i dessa organ. Statlig kontroll, censur samt ”balkanisering” och splittring av internet får dock inte främjas.

106. Europaparlamentet begär att EU ska inta en ledarroll i omformningen av internets allmänna struktur och styrning för att åtgärda de risker som är kopplade till dataflöden och datalagring, där man eftersträvar ökad dataminimering och öppenhet samt minskad central masslagring av obehandlade uppgifter samt en omläggning av internettrafiken eller helt obruten kryptering av all internettrafik så att man undviker riskerna med den trafik som i onödan leds genom länder som inte uppfyller de grundläggande standarderna för grundläggande rättigheter, uppgiftsskydd och personlig integritet.

107. Europaparlamentet uppmanar till främjande av följande:

— EU:s sökmotorer och sociala nätverk, som ett värdefullt steg mot EU:s it-oberoende.

— Europeiska leverantörer av it-tjänster.

— Kryptering av kommunikation i allmänhet, inklusive e-post och sms.

— Europeiska it-nyckelelement, t.ex. lösningar för system med kundservrar där man använder standarder för öppen källkod och utvecklar europeiska element för nätverkskoppling, t.ex. routrar.

108. Europaparlamentet uppmanar kommissionen att lägga fram ett lagstiftningsförslag om ett routingsystem för EU, inklusive hantering inom EU av telefonsamtalsinformation (call detail record/CDR) på EU-nivå, som ska vara en understruktur inom det befintliga internet och inte överskrida EU:s gränser. Alla routingdata och all telefonsamtalsinformation bör hanteras i enlighet med EU:s rättsliga ram.

109. Europaparlamentet uppmanar medlemsstaterna att i samarbete med Enisa, Europols it-brottscentrum, incidenthanteringsorganisationer och nationella uppgiftsskyddsmyndigheter och it-brottsenheter utveckla en kultur av säkerhet och starta en utbildnings- och informationskampanj. En sådan kampanj ska ge medborgarna förutsättningar att göra ett mer välgrundat val när det gäller vilka personuppgifter som ska läggas ut på nätet och hur man skyddar dem bättre, genom exempelvis kryptering och säkra molntjänster. Den plattform för information av allmänintresse som föreskrivs i direktivet om samhällsomfattande tjänster ska då utnyttjas fullt ut.

110. Europaparlamentet uppmanar kommissionen att senast i december 2014 lägga fram lagstiftningsförslag som uppmuntrar programvaru- och maskinvarutillverkare att införa ökad säkerhet och integritet i sina produkter genom inbyggt integritetsskydd och olika standardfunktioner, bland annat genom att införa negativa incitament för otillbörlig och oproportionerlig massinsamling av personuppgifter och genom att införa ett rättsligt ansvar för tillverkare när det gäller kända brister som inte har åtgärdats, produkter som är defekta eller brister i säkerhet, eller hemliga inbyggda bakdörrar som möjliggör obehörig tillgång till och behandling av uppgifter. Parlamentet uppmanar i detta avseende kommissionen att bedöma möjligheten att införa ett certifierings- eller valideringssystem för it-maskinvara, bl.a. testförfaranden på EU-nivå, för att säkra produkternas integritet och säkerhet.

Återskapa förtroendet

111. Europaparlamentet anser att utredningen, utöver behovet av lagstiftningsmässiga ändringar, har visat att Förenta staterna behöver återskapa förtroendet hos sina EU-partner, eftersom det i första hand är de amerikanska underrättelsetjänsternas verksamhet som står på spel.

Onsdagen den 12 mars 2014

112. Europaparlamentet påpekar att den förtroendekris som har uppstått även omfattar följande:

— Samarbetsandan inom EU, eftersom viss nationell underrättelseverksamhet kan äventyra möjligheterna att uppnå unionens mål.

— Medborgarna, som inser att det inte enbart är tredjeländer eller multinationella företag som kan spionera på dem, utan även deras egen regering.

— Respekten för grundläggande rättigheter, demokrati och rättsstatsprincipen samt de demokratiska, rättsliga och parlamentariska skyddsmekanismernas trovärdighet och tillsyn, i ett digitalt samhälle.

Mellan EU och Förenta staterna

113. Europaparlamentet erinrar om det viktiga historiska och strategiska partnerskapet mellan EU:s medlemsstater och Förenta staterna, som bygger på en samsyn kring demokrati, rättsstatsprincipen och grundläggande rättigheter.

114. Europaparlamentet anser att Förenta staternas massövervakning av medborgare och spionage på politiska ledare allvarligt har skadat förbindelserna mellan EU och Förenta staterna och har inverkat negativt på förtroendet för amerikanska organisationer med verksamhet i EU. Detta förvärras ytterligare av att det enligt Förenta staternas lagstiftning inte finns några rättsliga eller administrativa möjligheter för EU-medborgare att få tillgång till prövning, i synnerhet inte när det gäller övervakning i underrättelsesyfte.

115. Europaparlamentet inser, med tanke på de globala utmaningar som både EU och Förenta staterna står inför, att det transatlantiska partnerskapet behöver stärkas ytterligare och att det inom terrorismbekämpningen är mycket viktigt med ett fortsatt transatlantiskt samarbete som grundar sig på ett nytt förtroende baserat på en sann gemensam respekt för rättsstatsprincipen och avståndstagande från all typ av urskillningslösa metoder för massövervakning. Parlamentet understryker därför att Förenta staterna behöver vidta tydliga åtgärder för att återskapa förtroendet och på nytt framhålla de gemensamma grundvärderingar som ligger till grund för partnerskapet.

116. Europaparlamentet är redo att aktivt delta i en dialog med de amerikanska motparterna så att rätten till integritet och övriga rättigheter för EU:s medborgare och invånare och för andra personer som omfattas av EU-lagstiftningen liksom rätten till lika information och integritetsskydd i de amerikanska domstolarna, inklusive rätten till rättslig prövning, garanteras genom till exempel en översyn av integritetslagen och lagen om integritet i elektronisk kommunikation och genom ratificering av det första fakultativa protokollet till den internationella konventionen om medborgerliga och politiska rättigheter (ICCPR), så att den nuvarande diskrimineringen inte fortsätter.

117. Europaparlamentet kräver att nödvändiga reformer genomförs och att européerna får effektiva garantier för att säkerställa att utnyttjandet av övervakning och databehandling för utländska underrättelseändamål är proportionerligt, begränsat enligt klart angivna villkor och kopplat till en rimlig misstanke eller sannolik orsak till terroristrelaterad verksamhet. Parlamentet understryker att detta syfte måste omfattas av en öppen rättslig prövning.

118. Europaparlamentet anser att våra amerikanska partner behöver skicka tydliga politiska signaler för att visa att Förenta staterna skiljer mellan bundsförvanter och fiender.

119. Europaparlamentet uppmanar enträget kommissionen och den amerikanska regeringen att behandla frågan om EU-medborgarnas rätt till information och rättslig prövning under de pågående förhandlingarna om ett paraplyavtal mellan EU och Förenta staterna om dataöverföring i brottsbekämpande syfte, samt att slutföra dessa förhandlingar före sommaren 2014 i enlighet med det åtagande som gjordes vid ministermötet mellan EU och Förenta staterna om rättsliga och inrikes frågor den 18 november 2013.

120. Europaparlamentet uppmuntrar Förenta staterna att ansluta sig till Europarådets konvention om skydd för enskilda personer vid automatisk behandling av personuppgifter (konvention 108) på samma sätt som man anslöt sig till 2001 års konvention om it-brottslighet, vilket stärkte den gemensamma rättsliga grunden mellan de transatlantiska bundsförvanterna.

121. Europaparlamentet uppmanar EU-institutionerna att undersöka möjligheterna att tillsammans med Förenta staterna upprätta en uppförandekod som skulle garantera att Förenta staterna inte bedriver något spionage mot EU:s institutioner och lokaler.

På EU-nivå

122. Europaparlamentet anser också att EU-medlemsstaternas medverkan och verksamhet har skadat förtroendet, inklusive mellan medlemsstaterna och mellan EU-medborgarna och deras nationella myndigheter. Parlamentet menar att det förtroende som gått förlorat endast kan återskapas genom en fullständig öppenhet kring övervakningens syften och metoder, en offentlig diskussion och slutligen en översyn av lagstiftningen, inklusive ett stopp för massövervakningen och en förstärkning av systemet för rättslig och parlamentarisk tillsyn. Parlamentet understryker att det är svårt att utveckla en heltäckande säkerhetsstrategi för EU när sådan massövervakning pågår och betonar att EU:s princip om lojalt samarbete kräver att medlemsstaterna avstår från att bedriva underrättelseverksamhet på andra medlemsstaters territorium.

123. Europaparlamentet konstaterar att vissa medlemsstater håller på att föra bilaterala samtal med de amerikanska myndigheterna om spionageanklagelserna och att vissa av dem har ingått (Förenade kungariket) eller planerar att ingå (Tyskland, Frankrike) så kallade antispionageavtal. Parlamentet understryker att dessa medlemsstater behöver tillvarata hela EU:s intressen och regelverk fullt ut. Parlamentet bedömer att sådana bilaterala avtal är kontraproduktiva och irrelevanta, då det behövs ett europeiskt förhållningssätt till detta problem. Rådet uppmanas att informera parlamentet om hur det går med medlemsstaternas planer på ett ömsesidigt antispionageavtal inom EU.

124. Europaparlamentet anser att sådana avtal inte får bryta mot EU:s fördrag, framför allt inte principen om lojalt samarbete (artikel 4.3 i EU-fördraget), eller undergräva EU:s politik i största allmänhet och då i synnerhet den inre marknaden, en sund konkurrens samt ekonomisk, industriell och social utveckling. Parlamentet kan besluta att granska sådana avtal för att se om de är förenliga med EU:s lagstiftning och förbehåller sig rätten att använda sig av fördragsförfaranden om sådana avtal skulle visa sig strida mot unionens sammanhållning eller de grundläggande principer som denna sammanhållning bygger på.

125. Europaparlamentet uppmanar medlemsstaterna att göra sitt yttersta för att skapa ett bättre samarbete för att införa skyddsmekanismer mot spionage, i samarbete med EU:s relevanta organ och byråer, för att skydda EU:s medborgare och institutioner, de europeiska företagen, industrin i EU, it-infrastrukturen, it-nätverken och den europeiska forskningen. Parlamentet anser att en aktiv delaktighet för intressenterna i EU är en förutsättning för ett effektivt informationsutbyte. Parlamentet påpekar att säkerhetshoten har blivit mer internationella, utbredda och komplexa och därför kräver ett ökat europeiskt samarbete. Denna utveckling bör bättre återspeglas i fördragen. Därför efterlyser parlamentet en fördragsändring för att stärka principen om lojalt samarbete mellan medlemsstaterna och unionen när det gäller målet att uppnå ett område med säkerhet och för att förhindra ömsesidigt spionage mellan medlemsstaterna inom unionen.

126. Europaparlamentet ser det som en absolut nödvändighet att både kommunikationsvägar (e-post och telekommunikation, däribland fasta telefoner och mobiltelefoner) och mötesrum på alla relevanta EU-institutioner och EU-delegationer ska vara omöjliga att avlyssna. Parlamentet efterlyser därför ett krypterat internt e-postsystem inom EU.

127. Europaparlamentet uppmanar rådet och kommissionen att utan dröjsmål godkänna det förslag som Europaparlamentet antog den 23 maj 2012 om Europaparlamentets förordning om närmare föreskrifter för utövandet av Europaparlamentets undersökningsrätt och om upphävande av Europaparlamentets, rådets och kommissionens beslut 95/167/EG, Euratom, EKSG, som lagts fram på grundval av artikel 226 i EUF-fördraget. Parlamentet efterlyser en fördragsändring för att utvidga denna undersökningsrätt så att den, utan restriktioner eller undantag, omfattar alla unionens befogenhets- eller verksamhetsområden och så att möjligheten till utfrågningar under ed införs.

Internationellt

128. Europaparlamentet uppmanar kommissionen att senast i januari 2015 lägga fram en EU-strategi för demokratisk styrning av internet.

Onsdagen den 12 mars 2014

129. Europaparlamentet uppmanar medlemsstaterna att följa uppmaningen från den 35:e internationella konferensen för uppgiftsskyddsmyndigheter ”att förorda antagandet av ett tilläggsprotokoll till artikel 17 i den internationella konventionen om medborgerliga och politiska rättigheter (ICCPR), som bör grundas på de standarder som har utarbetats och antagits av den internationella konferensen samt bestämmelserna i kommittén för de mänskliga rättigheternas allmänna kommentar nr 16 till konventionen för att upprätta världsomfattande standarder för dataskydd och skyddet av privatlivet i enlighet med rättsstatsprincipen”. Parlamentet uppmanar medlemsstaterna att i samband med detta efterlysa en internationell FN-byrå med särskilt ansvar för att bevaka nya övervakningsverktyg samt reglera och undersöka hur dessa används. Kommissionens vice ordförande/unionens höga representant för utrikes frågor och säkerhetspolitik och Europeiska utrikestjänsten uppmanas att inta en proaktiv hållning.

130. Europaparlamentet uppmanar medlemsstaterna att utarbeta en sammanhållen och stark strategi inom FN, där man framför allt stöder den resolution om rätten till integritet i den digitala tidsåldern som Brasilien och Tyskland tagit initiativ till och som den tredje kommittén i FN:s generalförsamling (kommittén för de mänskliga rättigheterna) antog den 27 november 2013, liksom att också vidta ytterligare åtgärder för att försvara den grundläggande rätten till privatliv och uppgiftsskydd på internationell nivå samtidigt som man undviker att underlätta statlig kontroll eller censur eller splittring av internet, inklusive ett initiativ till ett internationellt fördrag som förbjuder massövervakning och ett organ som ska utöva tillsyn över detta.

Prioriteringsplan: En europeisk digital habeas corpus för att skydda de grundläggande rättigheterna i en digital tidsålder

131. Europaparlamentet beslutar att inför nästa valperiod lägga fram ovannämnda rekommendationer som prioriteringsplan för EU:s medborgare, institutioner och medlemsstater. Kommissionen och EU:s övriga institutioner, organ och byråer enligt denna resolution uppmanas i enlighet med artikel 265 i EUF-fördraget att följa de rekommendationer och uppmaningar som ingår i denna resolution.

132. Europaparlamentet beslutar att lansera ”En europeisk digital habeas corpus för att skydda de grundläggande rättigheterna i en digital tidsålder” på grundval av följande åtta insatser där Europaparlamentet ska övervaka genomförandet:

— Insats 1: Anta uppgiftsskyddspaketet under 2014.

— Insats 2: Ingå paraplyavtalet mellan EU och Förenta staterna, vilket ska säkra medborgarnas grundläggande rättigheter till integritet och uppgiftsskydd och säkerställa att EU-medborgare har reella möjligheter till rättslig prövning om uppgifter överförs från EU till Förenta staterna i brottsbekämpande syfte.

— Insats 3: Avbryta Safe Harbour tills det har gjorts en fullständig översyn och nuvarande kryphål har åtgärdats samt säkerställa att personuppgifter endast kan överföras från unionen till Förenta staterna för kommersiella ändamål om det sker i överensstämmelse med högsta EU-standarder.

— Insats 4: Upphäva TFTP-avtalet tills i) förhandlingarna om paraplyavtalet har slutförts, ii) en grundlig utredning har gjorts på grundval av en EU-analys och alla frågor som togs upp i parlamentets resolution av den 23 oktober 2013 har åtgärdats på vederbörligt sätt.

— Insats 5: Utvärdera alla avtal, mekanismer och utbyten med tredjeländer som omfattar personuppgifter, så att rätten till integritet och skydd av personuppgifter inte överträds genom övervakningsverksamhet, samt vidta nödvändiga uppföljningsåtgärder.

— Insats 6: Skydda rättsstatsprincipen och EU-medborgarnas grundläggande rättigheter (bland annat rätten att slippa hot mot pressfriheten), allmänhetens rätt till opartisk information och tystnadsplikten (bland annat i relationen mellan advokat och klient) samt ett ökat skydd för visselblåsare.

— Insats 7: Utarbeta en europeisk strategi för större it-oberoende (en ny digital reform, inklusive tilldelning av lämpliga resurser på nationell nivå och EU-nivå) för att främja it-branschen och göra det möjligt för europeiska företag att utnyttja EU:s konkurrensfördel när det gäller integritet.

— Insats 8: Utveckla EU som referensaktör för en demokratisk och neutral styrning av internet.

133. Europaparlamentet uppmanar EU-institutionerna och medlemsstaterna att främja ”En europeisk digital habeas corpus för att skydda de grundläggande rättigheterna i en digital tidsålder”. Parlamentet åtar sig att fungera som förespråkare av EU-medborgarnas rättigheter och övervaka genomförandet enligt följande tidsplan:

— April 2014–mars 2015: Övervakningsgrupp som bygger på LIBE:s utredningsteam med ansvar för att övervaka eventuella nya avslöjanden som ligger inom ramen för utredningens uppdrag samt att granska genomförandet av denna resolution.

— Juli 2014 och framåt: Permanent tillsynsmekanism för dataöverföringar och rättslig prövning inom det ansvariga utskottet.

— Våren 2014: Formell uppmaning till Europeiska rådet att integrera ”En europeisk digital habeas corpus för att skydda de grundläggande rättigheterna i en digital tidsålder” i de riktlinjer som ska antas enligt artikel 68 i EUF-fördraget.

— Hösten 2014: Åtagande om att ”En europeisk digital habeas corpus för att skydda de grundläggande rättigheterna i en digital tidsålder” och tillhörande rekommendationer ska utgöra huvudkriterier när nästa kommission ska godkännas.

— 2014: Konferens med europeiska högnivåexperter inom olika områden som främjar it-säkerhet (däribland matematik, kryptografi och integritetsfrämjande teknik) för att bidra till att en it-strategi för EU utvecklas inför nästa valperiod.

— 2014–2015: En grupp med inriktning på förtroende/uppgifter/medborgares rättigheter ska regelbundet sammankalla till möten mellan Europaparlamentet och den amerikanska kongressen samt med andra berörda parlament i tredjeland, däribland Brasilien.

— 2014–2015: Konferens med tillsynsorganen för underrättelseväsendet i de europeiska nationella parlamenten.

o

o o

134. Europaparlamentet uppdrar åt talmannen att översända denna resolution till Europeiska rådet, rådet, kommissionen, medlemsstaternas parlament och regeringar, de nationella uppgiftsskyddsmyndigheterna, Europeiska datatillsynsmannen, eu-LISA, Enisa, EU:s byrå för grundläggande rättigheter, artikel 29-gruppen, Europarådet, Förenta staternas kongress, Förenta staternas regering, Förbundsrepubliken Brasiliens president, regering och parlament samt FN:s generalsekreterare.

135. Europaparlamentet uppdrar åt utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor att ta upp frågan med parlamentet i plenum ett år efter antagandet av denna resolution. Parlamentet anser att det är mycket viktigt att bedöma i vilken utsträckning parlamentets rekommendationer har följts och att analysera de fall då rekommendationerna inte följts.