Programul de supraveghere al Agenţiei Naţionale de Securitate (NSA) a SUA, organismele de supraveghere din diferite state membre şi impactul acestora asupra drepturilor fundamentale ale cetăţenilor UE

Rezoluţia Parlamentului European din 12 martie 2014 referitoare la programul de supraveghere al Agenției Naționale de Securitate (NSA) a SUA, la organismele de supraveghere din diferite state membre și la impactul acestora asupra drepturilor fundamentale ale cetățenilor UE și asupra cooperării transatlantice în materie de justiție și de afaceri interne (2013/2188(INI))

Parlamentul European,

– având în vedere Tratatul privind Uniunea Europeană (TUE), în special articolele 2, 3, 4, 5, 6, 7, 10, 11 și 21,

– având în vedere Tratatul privind funcționarea Uniunii Europene (TFUE), în special articolele 15, 16 și 218, precum și titlul V,

– având în vedere Protocolul nr. 36 privind dispozițiile tranzitorii, în special articolul 10, precum și Declarația nr. 50 anexată la acest protocol,

– având în vedere Carta drepturilor fundamentale a Uniunii Europene, în special articolele 1, 3, 6, 7, 8, 10, 11, 20, 21, 42, 47, 48 și 52,

– având în vedere Convenția europeană a drepturilor omului, în special articolele 6, 8, 9, 10 și 13, precum și protocoalele aferente,

– având în vedere Declarația Universală a Drepturilor Omului, în special articolele 7, 8, 10, 11, 12 și 14[1],

– având în vedere Pactul internațional cu privire la drepturile civile și politice, în special articolele 14, 17, 18 și 19,

– având în vedere Convenția Consiliului Europei privind protecția datelor (ETS nr. 108) și Protocolul adițional din 8 noiembrie 2001 la Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, cu privire la autoritățile de control și fluxul transfrontalier al datelor (ETS nr. 181),

– având în vedere Convenția de la Viena privind relațiile diplomatice, în special articolele 24, 27 și 40,

– având în vedere Convenția Consiliului Europei privind criminalitatea informatică (ETS nr. 185),

– având în vedere Raportul prezentat la 17 mai 2010 de raportorul special al ONU pentru promovarea și protecția drepturilor omului și a libertăților fundamentale în cadrul luptei

[1] http://www.un.org/en/documents/udhr/

împotriva terorismului[1],

– având în vedere Comunicarea Comisiei intitulată „Guvernanța și politica în domeniul internetului – Rolul Europei în modelarea viitorului guvernanței internetului”(COM(2014)0072);

– având în vedere Raportul prezentat la 17 aprilie 2013 de raportorul special al ONU pentru promovarea și protejarea dreptului la libertatea de opinie și de exprimare[2],

– având în vedere Orientările privind drepturile omului și lupta împotriva terorismului adoptate de Comitetul de Miniștri al Consiliului Europei la 11 iulie 2002,

– având în vedere Declarația de la Bruxelles, din 1 octombrie 2010, adoptată la Cea de a șasea conferință a comisiilor parlamentare pentru supravegherea serviciilor de informații și de securitate ale statelor membre ale Uniunii Europene,

– având în vedere Rezoluția nr. 1954/2013 a Adunării Parlamentare a Consiliului Europei privind securitatea națională și accesul la informații,

– având în vedere Raportul referitor la supravegherea democratică a serviciilor de securitate, adoptat de Comisia de la Veneția la 11 iunie 2007[3], și a cărui versiune actualizată este așteptată cu mare interes în primăvara anului 2014,

– având în vedere declarațiile reprezentanților comisiilor de supraveghere a serviciilor de informații din Belgia, Țările de Jos, Danemarca și Norvegia,

– având în vedere cauzele înaintate instanțelor din Franța[4], Polonia și Regatul Unit[5], precum și Curții Europene a Drepturilor Omului[6], în legătură cu sistemele de supraveghere în masă,

– având în vedere Convenția elaborată de Consiliu în conformitate cu articolul 34 din Tratatul privind Uniunea Europeană referitoare la asistența judiciară reciprocă în materie penală între statele membre ale Uniunii Europene[7], în special titlul III,

– având în vedere Decizia 2000/520/CE a Comisiei din 26 iulie 2000 privind caracterul adecvat al protecției oferite de principiile „sferei de siguranță” privind protecția vieții private și întrebările de bază aferente, publicate de Departamentul Comerțului al SUA,

– având în vedere Rapoartele de evaluare ale Comisiei privind punerea în aplicare a

---

1 http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G10/134/10/PDF/G1013410.pdf?OpenElement

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

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

4 Federația Internațională a Ligilor pentru Drepturile Omului și Liga franceză pentru apărarea drepturilor omului și cetățeanului/ X; Tribunal de Grande Instance din Paris.

5 Cauzele înaintate de Privacy International și Liberty către Tribunalul privind competențele de cercetare (Investigatory Powers Tribunal).

6 Cerere comună în temeiul articolului 34 în cauza Big Brother Watch, Open Rights Group, English PEN și Dr. Constanze Kurz (reclamanți)/ Regatul Unit (pârât).

7 JO C 197, 12.7.2000, p. 1.

principiilor „sferei de siguranță” privind viața privată din 13 februarie 2002 (SEC(2002)0196) și din 20 octombrie 2004 (SEC(2004)1323),

– având în vedere Comunicarea Comisiei din 27 noiembrie 2013 privind funcționarea sferei de siguranță din punctul de vedere al cetățenilor UE și al întreprinderilor stabilite în UE (COM(2013)0847) și Comunicarea Comisiei din 27 noiembrie 2013 privind restabilirea încrederii în fluxurile de date dintre UE și SUA (COM(2013)0846),

– având în vedere Rezoluția Parlamentului European din 5 iulie 2000 referitoare la proiectul de decizie a Comisiei privind caracterul adecvat al protecției oferite de principiile „sferei de siguranță” privind protecția vieții private și întrebările de bază aferente, publicate de Departamentul Comerțului al SUA[1], potrivit căreia caracterul adecvat al sistemului nu a putut fi confirmat, și avizele Grupului de lucru „Articolul 29”, în special avizul nr. 4/2000 din 16 mai 2000[2],

– având în vedere acordurile dintre Statele Unite ale Americii și Uniunea Europeană privind utilizarea și transferul de date din registrele cu numele pasagerilor (acordul PNR) din 2004, 2007[3] și 2012[4],

– având în vedere Examinarea comună a punerii în aplicare a Acordului dintre UE și SUA privind prelucrarea și transferul de date din registrele cu numele pasagerilor către Departamentul pentru Securitate Internă al SUA[5], care însoțește Raportul Comisiei către Parlamentul European și Consiliu privind examinarea comună (COM(2013)0844),

– având în vedere concluziile avocatului general Cruz Villalón conform căruia Directiva 2006/24/CE privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicații electronice accesibile publicului sau de rețele de comunicații publice este incompatibilă în întregime cu articolul 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene, iar articolul 6 din aceeași directivă este incompatibil cu articolul 7 și articolul 52 alineatul (1) din Cartă[6],

– având în vedere Decizia 2010/412/UE a Consiliului din 13 iulie 2010 privind încheierea Acordului dintre Uniunea Europeană și Statele Unite ale Americii privind prelucrarea și transferul datelor de mesagerie financiară din Uniunea Europeană către Statele Unite ale Americii în cadrul Programului de urmărire a finanțărilor în scopuri teroriste (TFTP)[7] și declarațiile însoțitoare ale Comisiei și ale Consiliului,

– având în vedere Acordul privind asistența judiciară reciprocă între Uniunea Europeană și Statele Unite ale Americii[8],

– având în vedere negocierile în curs referitoare la un acord-cadru între UE și SUA privind protecția datelor cu caracter personal în momentul transferării și prelucrării în scopul

---

1 JO C 121, 24.4.2001, p. 152.
2 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp32en.pdf
3 JO L 204, 4.8.2007, p. 18.
4 JO L 215, 11.8.2012, p. 5.
5 SEC(2013)0630, 27.11.2013.
6 Concluziile avocatului general Cruz Villalón din 12 decembrie 2013 în cauza C-293/12.
7 JO L 195, 27.7.2010, p. 3.
8 JO L 181, 19.7.2003, p. 34.

prevenirii, anchetării, identificării sau urmăririi penale a infracțiunilor, inclusiv infracțiunea de terorism, în cadrul cooperării polițienești și judiciare în materie penală („acordul-cadru”),

– având în vedere Regulamentul (CE) nr. 2271/96 al Consiliului din 22 noiembrie 1996 de protecție împotriva efectelor aplicării extrateritoriale a unei legislații adoptate de către o țară terță, precum și a acțiunilor întemeiate pe aceasta sau care rezultă din aceasta[1],

– având în vedere declarația președintelui Republice Federative a Braziliei la deschiderea celei de a 68-a sesiuni a Adunării Generale a ONU din 24 septembrie 2013 și lucrările Comisiei parlamentare de anchetă privind activitățile de spionaj înființate de Senatul federal al Braziliei,

– având în vedere Legea „USA PATRIOT” a SUA semnată de președintele George W. Bush la 26 octombrie 2001,

– având în vedere Legea privind supravegherea activităților străine de spionaj (FISA) din 1978 și Actul de modificare a FISA din 2008,

– având în vedere Ordinul executiv nr. 12333, emis de președintele SUA în 1981 și modificat în 2008,

– având în vedere Directiva prezidențială (PPD-28) privind activitățile de colectare de informații pe baza semnalelor electromagnetice, emisă de președintele SUA, Barack Obama, la 17 ianuarie 2014,

– având în vedere propunerile legislative în curs de examinare în Congresul SUA, inclusiv proiectul de lege al SUA *Freedom Act*, proiectul de lege privind reforma activităților de supraveghere și monitorizare ale serviciilor de informații și altele,

– având în vedere evaluările realizate de Comitetul de supraveghere a vieții private și a libertăților civile, de Consiliul Național de Securitate al SUA și de grupul de analiză al președintelui privind serviciile de informații și tehnologia comunicațiilor, în special raportul prezentat de acest grup la 12 decembrie 2013 și intitulat „Libertate și securitate într-o lume în schimbare”,

– având în vedere hotărârea Curții districtuale a SUA din districtul Columbia, Klayman și alții/Obama și alții, cauza civilă nr. 13-0851 din 16 decembrie 2013 și hotărârea Curții districtuale a SUA din districtul New York Sud, ACLU și alții/James R. Clapper și alții, cauza civilă nr. 13-3994 din 11 iunie 2013,

– având în vedere Raportul referitor la concluziile copreședinților UE ai Grupului de lucru *ad hoc* UE-SUA privind protecția datelor din 27 noiembrie 2013[2],

– având în vedere Rezoluțiile sale din 5 septembrie 2001[3] și din 7 noiembrie 2002[4] privind existența unui sistem global de interceptare a comunicațiilor private și comerciale

---

1 JO L 309, 29.11.1996, p. 1.
2 Documentul 16987/2013 al Consiliului.
3 JO C 72 E, 21.3.2002, p. 221.
4 JO C 16 E, 22.1.2004, p. 88.

(sistemul de interceptare ECHELON),

– având în vedere Rezoluția sa din 21 mai 2013 privind Carta UE: norme standard pentru libertatea mass-mediei în UE[1],

– având în vedere Rezoluția sa din 4 iulie 2013 referitoare la programul de supraveghere al Agenției Naționale de Securitate din SUA, serviciile de informații din diferitele state membre și impactul asupra vieții private a cetățenilor UE[2], în urma căreia Parlamentul European a solicitat Comisiei pentru libertăți civile, justiție și afaceri interne să realizeze o anchetă aprofundată pe această temă,

– având în vedere Documentul de lucru nr. 1 referitor la programele de supraveghere ale SUA și UE și impactul acestora asupra drepturilor fundamentale ale cetățenilor UE,

– având în vedere Documentul de lucru nr. 3 referitor la relația dintre practicile de supraveghere din UE și din SUA și dispozițiile UE privind protecția datelor,

– având în vedere Documentul de lucru nr. 4 referitor la activitățile de supraveghere efectuate de SUA în ceea ce privește datele UE și posibilele implicații juridice ale acestora asupra acordurilor și a cooperării transatlantice,– având în vedere Documentul de lucru nr. 5 referitor la supravegherea democratică a serviciilor de informații ale statelor membre și a organismelor de informații ale UE,

– având în vedere documentul de lucru al Comisiei AFET intitulat „Aspecte ale politicii externe din cadrul anchetei privind supravegherea electronică în masă a cetățenilor UE”;

– având în vedere Rezoluția sa din 23 octombrie 2013 referitoare la crima organizată, corupția și spălarea de bani: recomandări cu privire la acțiunile și inițiativele care se impun[3],

– având în vedere Rezoluția sa din 23 octombrie 2013 referitoare la suspendarea Acordului TFTP ca urmare a supravegherii Agenției Naționale de Securitate a SUA[4],

– având în vedere Rezoluția sa din 10 decembrie 2013 referitoare la valorificarea potențialului *cloud computingului* în Europa[5],

– având în vedere Acordul interinstituțional între Parlamentul European și Consiliu privind transmiterea și prelucrarea de către Parlamentul European a informațiilor clasificate deținute de Consiliu în alte chestiuni decât cele vizate de domeniul politicii externe și de securitate comune[6],

– având în vedere anexa VIII la Regulamentul său de procedură,

– având în vedere articolul 48 din Regulamentul său de procedură,

---

1 Texte adoptate, P7_TA(2013)0203.
2 Texte adoptate, P7_TA(2013)0322.
3 Texte adoptate, P7_TA(2013)0444.
4 Texte adoptate, P7_TA(2013)0449.
5 Texte adoptate, P7_TA(2013)0535.
6 JO C 353 E, 3.12.2013, p. 156.

– având în vedere Raportul Comisiei pentru libertăți civile, justiție și afaceri interne (A7-0139/2014),

Impactul supravegherii în masă

A. întrucât protecția datelor și viața privată sunt drepturi fundamentale; întrucât măsurile de securitate, inclusiv măsurile de combatere a terorismului, trebuie, prin urmare, să fie aplicate respectându-se statul de drept și obligațiile în materie de drepturi fundamentale, printre care se numără și viața privată și protecția datelor;

B. întrucât fluxurile de informații și datele care domină în prezent viața de zi cu zi și care fac parte din integritatea oricărei persoane trebuie să fie la fel de bine protejate împotriva eventualelor intruziuni ca locuințele private;

C. întrucât relațiile dintre Europa și Statele Unite ale Americii se bazează pe spiritul și principiile democrației și statului de drept, ale libertății, dreptății și solidarității;

D. întrucât cooperarea dintre Statele Unite ale Americii și Uniunea Europeană și statele sale membre în lupta împotriva terorismului este în continuare crucială pentru securitatea și siguranța ambilor parteneri;

E. întrucât încrederea și înțelegerea reciproce sunt factori-cheie în dialogul și parteneriatul transatlantice;

F. întrucât, după evenimentele din 11 septembrie 2001, combaterea terorismului a devenit una dintre prioritățile absolute pentru majoritatea guvernelor; întrucât dezvăluirile bazate pe scurgerile de informații datorate lui Edward Snowden, fost contractant al NSA, i-au obligat pe liderii politici să abordeze provocările legate de supravegherea și controlul serviciilor de informații și de evaluarea impactului activităților acestora asupra drepturilor fundamentale și asupra statului de drept într-o societate democratică;

G. întrucât dezvăluirile făcute începând din iunie 2013 au cauzat numeroase îngrijorări la nivelul UE în legătură cu:

– amploarea sistemelor de supraveghere făcute cunoscute atât în SUA, cât și în statele membre ale UE;

– încălcarea standardelor juridice, a drepturilor fundamentale și a standardelor în materie de protecție a datelor din UE;

– nivelul de încredere dintre UE și SUA în calitate de parteneri transatlantici;

– gradul de cooperare și de implicare al unor state membre ale UE în programele de supraveghere ale SUA sau în programe echivalente de la nivel național conform dezvăluirilor din mass-media;

– lipsa controlului și a supravegherii efective exercitate de autoritățile politice americane și de unele state membre ale UE asupra serviciilor lor de informații;

– posibilitatea ca aceste acțiuni de supraveghere în masă să fie utilizate pentru alte motive decât securitatea națională și lupta împotriva terorismului în sensul strict al cuvântului, ca de exemplu pentru spionaj economic și industrial sau pentru

stabilirea de profiluri pe motive politice;

– subminarea libertății presei și a comunicațiilor dintre membrii anumitor profesii care se bucură de privilegiul confidențialității, cum sunt, printre alții, avocații și medicii;

– rolurile serviciilor de informații și ale companiilor private din domeniul IT și al comunicațiilor, precum și gradul de implicare al acestora;

– liniile de demarcare din ce în ce mai neclare dintre aplicarea legii și activitățile de spionaj, care fac ca fiecare cetățean să fie tratat ca suspect și să fie supravegheat;

– amenințările la adresa vieții private în era digitală și impactul supravegherii de masă asupra cetățenilor și a societății;

H. întrucât amploarea nemaiîntâlnită a activităților de spionaj scoase la iveală necesită o investigare aprofundată din partea autorităților SUA, a instituțiilor europene și a guvernelor, a parlamentelor naționale și a autorităților judiciare din statele membre;

I. întrucât autoritățile americane au negat o parte din informațiile dezvăluite, fără a contesta însă cea marea majoritate a acestora; întrucât dezbaterea publică s-a desfășurat la scară largă în SUA și în anumite state membre ale UE; întrucât, de prea multe ori, guvernele și parlamentele din UE păstrează tăcerea și nu lansează investigațiile care se impun;

J. întrucât președintele Obama a anunțat recent o reformă a NSA și a programelor sale de supraveghere;

K. întrucât, comparativ cu acțiunile întreprinse atât de instituțiile UE, cât și de unele state membre, Parlamentul European și-a luat foarte în serios obligația de a face lumină asupra dezvăluirilor privind practicile nediscriminante de supraveghere în masă a cetățenilor UE și, prin Rezoluția sa din 4 iulie 2013 referitoare la programul de supraveghere al Agenției Naționale de Securitate a SUA, organismele de supraveghere din diferitele state membre și impactul acestora asupra cetățenilor UE, a solicitat Comisiei pentru libertăți civile, justiție și afaceri interne să realizeze o anchetă aprofundată pe această temă;

L. întrucât instituțiilor europene le revine responsabilitatea de a se asigura că legislația UE este pusă pe deplin în aplicare în interesul cetățenilor europeni și că forța juridică a tratatelor UE nu este subminată de o acceptare indiferentă a efectelor extrateritoriale ale standardelor sau acțiunilor unor țări terțe;

Evoluții ale reformei serviciilor de informații din SUA

M. întrucât Curtea districtuală a Districtului Columbia, în hotărârea sa din 16 decembrie 2013, a decis că colectarea de metadate în masă de către NSA încalcă Al patrulea amendament al Constituției Statelor Unite ale Americii[1]; întrucât, în hotărârea sa din 27 decembrie 2013, Curtea districtuală a Districtului New York Sud a statuat, cu toate acestea, că respectiva colectare este legală;

N. întrucât o hotărâre a Curții districtuale a Districtului de Est din Michigan a decis că Al

[1] Klayman și alții/Obama și alții, cauza civilă nr. 13-0851, 16 decembrie 2013.

patrulea amendament impune o abordare rezonabilă în toate percheziţiile, mandate prealabile pentru toate percheziţiile, mandate bazate pe o cauză probabilă anterioară, precum şi o abordare specifică persoanelor, locurilor şi lucrurilor şi interpunerea unui magistrat neutru între agenţii responsabili cu aplicarea legii şi cetăţeni[1];

O. întrucât, în raportul său din 12 decembrie 2013, grupul de analiză al preşedintelui privind serviciile de informaţii şi tehnologia comunicaţiilor propune 46 de recomandări preşedintelui Statelor Unite ale Americii; întrucât aceste recomandări subliniază nevoia de a proteja atât securitatea naţională, cât şi viaţa privată şi libertăţile civile; întrucât, în acest sens, raportul invită administraţia americană: să pună capăt colectării în masă a înregistrărilor convorbirilor telefonice ale cetăţenilor Statelor Unite în temeiul secţiunii 215 din Legea *PATRIOT* a SUA cât de curând posibil; să realizeze o analiză aprofundată a cadrului juridic al NSA şi al serviciilor de informaţii ale SUA, pentru a asigura respectarea dreptului la viaţa privată; să pună capăt eforturilor de subminare sau de vulnerabilizare a produselor software comerciale (*backdoors* şi *malware*); să recurgă din ce în ce mai des la criptare, în special pentru datele aflate în tranzit, şi să nu submineze eforturile de creare a unor standarde de criptare; să instituie un Avocat al interesului public, care să reprezinte viaţa privată şi libertăţile civile în faţa Tribunalului pentru Serviciile de Informaţii Externe; să confere Comisiei de supraveghere a respectării dreptului la viaţă privată şi a libertăţilor civile competenţa de a monitoriza activităţile comunităţii de informaţii în scopul colectării de informaţii externe, şi nu doar în scopul combaterii terorismului; şi să primească plângeri din partea denunţătorilor, să utilizeze tratatele de asistenţă judiciară pentru a obţine comunicaţii electronice şi să nu recurgă la supravegheri pentru a fura secrete industriale sau comerciale;

P. întrucât, potrivit unui memorandum deschis prezentat preşedintelui Obama de foşti înalţi funcţionari ai NSA/*Veteran Intelligence Professionals for Sanity* (VIPS) la 7 ianuarie 2014[2], colectarea masivă de date nu sporeşte capacitatea de prevenire a viitoarelor atacuri teroriste; întrucât autorii memorandumului subliniază că supravegherea în masă efectuată de NSA a avut drept rezultat prevenirea a zero atacuri şi că s-au cheltuit miliarde de dolari pentru programe care sunt mai puţin eficace şi mult mai intruzive asupra vieţii private a cetăţenilor decât o tehnologie internă denumită THINTHREAD, creată în 2001;

Q. întrucât, în ceea ce priveşte activităţile de spionaj implicând persoane din afara SUA în baza secţiunii 702 din FISA, recomandările preşedintelui SUA recunosc principiul fundamental al respectării vieţii private şi demnităţii umane consacrat la articolul 12 din Declaraţia Universală a Drepturilor Omului şi la articolul 17 din Pactul internaţional cu privire la drepturile civile şi politice; întrucât acestea nu recomandă acordarea aceloraşi drepturi şi aceleiaşi protecţii pentru persoanele din afara SUA ca cele de care beneficiază cetăţenii americani;

R. întrucât, în Directiva prezidenţială din 17 ianuarie 2014 privind activităţile de colectare de informaţii pe baza semnalelor electromagnetice şi în discursul aferent, preşedintele american Barack Obama a afirmat că supravegherea electronică în masă este necesară pentru Statele Unite în scopul protejării securităţii naţionale, a cetăţenilor săi, a cetăţenilor aliaţilor şi partenerilor SUA, precum şi pentru promovarea intereselor sale în materie de

---

1 ACLU/ NSA nr. 06-CV-10204, 17 august 2006.

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

politică externă; întrucât această directivă de politică conține o serie de principii privind colectarea, utilizarea și partajarea informațiilor obținute pe baza semnalelor electromagnetice și extinde unele garanții la persoanele din afara SUA, prevăzând parțial un tratament egal cu cel aplicat cetățenilor americani, inclusiv garanții privind informațiile personale ale tuturor cetățenilor, indiferent de naționalitate sau de locul de reședință; întrucât, cu toate acestea, președintele Obama nu a anunțat nicio propunere concretă, în special în ceea ce privește interzicerea activităților de supraveghere în masă și introducerea unor căi de atac administrative și judiciare pentru persoanele din afara SUA;

Cadrul juridic

Drepturile fundamentale

S. întrucât raportul privind concluziile copreședinților UE ai Grupului de lucru *ad hoc* UE-SUA privind protecția datelor oferă o vedere de ansamblu a situației juridice din SUA, dar nu reușește să stabilească faptele concrete legate de programele de supraveghere ale SUA; întrucât nu a fost dată publicității nicio informație în legătură cu așa-numitul Grup de lucru „secundar”, în cadrul căruia statele membre poartă discuții bilaterale cu autoritățile americane pe marginea unor chestiuni de securitate națională;

T. întrucât drepturile fundamentale, în special libertatea de exprimare, libertatea presei, libertatea de gândire, libertatea de conștiință, libertatea religioasă și de asociere, viață privată, protecția datelor, precum și dreptul la o cale de atac eficientă, prezumția de nevinovăție și dreptul la un proces echitabil și la nediscriminare, astfel cum sunt consacrate în Carta drepturilor fundamentale a Uniunii Europene și în Convenția Europeană a Drepturilor Omului, sunt pietre de temelie ale democrației; întrucât supravegherea în masă a persoanelor este incompatibilă cu aceste pietre de temelie;

U. întrucât, în toate statele membre, legea asigură protecție împotriva dezvăluirii de informații comunicate în cadrul relației de încredere dintre avocat și client, un principiu care a fost recunoscut de Curtea de Justiție a Uniunii Europene[1];

V. întrucât, în Rezoluția sa din 23 octombrie 2013 referitoare la crima organizată, corupție și spălare de bani, Parlamentul a solicitat Comisiei să prezinte o propunere legislativă de instituire a unui program european de protecție eficace și globală a denunțărilor, în vederea protejării intereselor financiare ale UE, și să continue să examineze măsura în care o astfel de legislație viitoare ar trebui să vizeze și alte domenii de competență ale Uniunii;

Competențele Uniunii în materie de securitate

W. întrucât, în conformitate cu articolul 67 alineatul (3) din TFUE, UE „acționează pentru a asigura un înalt nivel de securitate”; întrucât dispozițiile tratatului [în special articolul 4 alineatul (2) din TUE, articolele 72 și 73 din TFUE] sugerează că UE dispune de anumite competențe în chestiuni legate de securitatea comună a Uniunii; întrucât UE deține competențe în chestiuni de securitate internă [articolul 4 litera (j) din TFUE] și și-a exercitat aceste competențe prin luarea unor decizii cu privire la o serie de instrumente legislative și prin încheierea de acorduri internaționale (PNR, TFTP) care vizează combaterea infracțiunilor grave și a terorismului, precum și prin instituirea unei strategii

[1] Hotărârea din 18 mai 1982, AM & S Europe Limited/Comisia Comunităților Europene, C-155/79.

de securitate internă și a unor agenții cu activitate în acest domeniu;

X. întrucât Tratatul privind funcționarea Uniunii Europene stipulează că „statele membre au libertatea de a organiza între ele și sub autoritatea lor forme de cooperare și de coordonare pe care le consideră oportune, între serviciile competente ale administrațiilor acestora care răspund de asigurarea securității naționale” (articolul 73 din TFUE);

Y. întrucât articolul 276 din TFUE stipulează că „în exercitarea atribuțiilor sale privind dispozițiile părții a treia titlul V capitolele 4 și 5, referitoare la spațiul de libertate, securitate și justiție, Curtea de Justiție a Uniunii Europene nu este competentă să verifice legalitatea sau proporționalitatea operațiunilor efectuate de poliție sau de alte servicii de aplicare a legii într-un stat membru și nici să hotărască cu privire la exercitarea responsabilităților care le revin statelor membre în vederea menținerii ordinii publice și a apărării securității interne”;

Z. întrucât conceptele de „securitate națională”, „securitate internă”, „securitate internă a UE” și „securitate internațională” se suprapun; întrucât Convenția de la Viena privind dreptul tratatelor, principiul cooperării sincere între statele membre ale UE și principiul drepturilor omului conform căruia toate scutirile se interpretează în sensul cel mai strict duc înspre o interpretare restrictivă a noțiunii de „securitate națională” și impune statelor membre să nu își suprapună acțiunile peste competențele UE;

AA. întrucât tratatele europene conferă Comisiei Europene rolul de „gardian al tratatelor” și, prin urmare, acesteia îi revine responsabilitatea juridică de a investiga orice posibilă încălcare a legislației UE;

AB. întrucât, în conformitate cu articolul 6 din TUE, care face trimitere la Carta drepturilor fundamentale a Uniunii Europene și la Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale, agențiile din statele membre și chiar și actorii privați care activează în domeniul securității naționale trebuie, de asemenea, să respecte drepturile consacrate în aceste documente, indiferent dacă drepturile în cauză le aparțin propriilor cetățeni sau cetățenilor altor state;

Extrateritorialitate

AC. întrucât aplicarea extrateritorială de către o țară terță a propriilor legii, regulamente și a altor instrumente legislative sau norme de aplicare în situații care intră sub jurisdicția UE sau a statelor membre ale UE poate avea un impact asupra cadrului legislativ deja existent și a statului de drept și poate conduce chiar la încălcarea dreptului internațional sau a dreptului UE, inclusiv la încălcarea drepturilor persoanelor fizice și juridice, având în vedere sfera de aplicare a acestor dispoziții și scopul, declarat sau real, al aplicării lor; întrucât, în aceste condiții, este necesar să se ia măsuri la nivelul Uniunii pentru a se asigura respectarea, în cadrul UE, a valorilor europene consacrate la articolul 2 din TUE, în Carta drepturilor fundamentale, în Convenția CEDO referitoare la drepturile fundamentale, la democrație și la statul de drept, precum și a drepturilor persoanelor fizice și juridice, consacrate în legislația secundară de aplicare a acestor principii fundamentale, de pildă prin îndepărtarea, neutralizarea, blocarea sau contracararea prin alte mijloace a efectelor dispozițiilor legislative străine în cauză;

Transferurile internaționale de date

AD. întrucât, prin transferul de date cu caracter personal de către instituțiile, organismele, birourile sau agențiile UE sau de către statele membre ale UE către SUA în scopuri legate de aplicarea legii, în lipsa unor garanții și protecții adecvate pentru respectarea drepturilor fundamentale ale cetățenilor UE, în special drepturile la viață privată și la protecția datelor cu caracter personal, instituția, organismul, biroul sau agenția UE sau statul membru în cauză s-ar face vinovate, în baza articolului 340 din TFUE sau a jurisprudenței consacrate a CJUE[1], de încălcarea legislației UE – care include orice încălcare a drepturilor fundamentale consacrate în Carta UE;

AE. întrucât transferul de date nu este limitat din punct de vedere geografic și, în special în contextul intensificării globalizării și a comunicațiilor la nivel mondial, legiuitorul UE se confruntă cu provocări noi în ceea ce privește protecția datelor cu caracter personal și a comunicațiilor; întrucât este, prin urmare, extrem de important să se promoveze introducerea unor cadre juridice bazate pe standarde comune;

AF. întrucât colectarea în masă a datelor cu caracter personal în scopuri comerciale și pentru combaterea terorismului și a infracțiunilor transnaționale grave pune în pericol drepturile cetățenilor UE în materie de date cu caracter personal și de confidențialitate;

Transferuri de date către SUA în baza „sferei de siguranță” din SUA

AG. întrucât cadrul juridic al SUA privind protecția datelor nu asigură un nivel adecvat de protecție în ceea ce-i privește pe cetățenii UE;

AH. întrucât, pentru a le permite operatorilor de date europeni să transfere date cu caracter personal către o entitate din SUA, Comisia a constatat, în Decizia sa 2000/520/CE, caracterul adecvat al protecției oferite de principiile „sferei de siguranță” privind protecția vieții private și întrebările de bază aferente, publicate de Departamentul Comerțului al SUA, în ceea ce privește datele transferate dinspre Uniune către organizații situate în SUA care au aderat la „sfera de siguranță”;

AI. întrucât, în Rezoluția sa din 5 iulie 2000, Parlamentul European și-a exprimat îndoielile și preocupările cu privire la caracterul adecvat al „sferei de siguranță” și a solicitat Comisiei să reevalueze decizia în timp util, ținând cont de ultimele experiențe și de schimbările legislative recente;

AJ. întrucât, în Documentul de lucru nr. 4 al Parlamentului din 12 decembrie 2013 referitor la activitățile de supraveghere ale SUA în ceea ce privește datele UE și posibilele implicații juridice ale acestora asupra acordurilor și a cooperării transatlantice, raportorii și-au exprimat îndoiala și îngrijorarea față de caracterul adecvat al „sferei de siguranță” și au solicitat Comisiei să abroge decizia privind caracterul adecvat al „sferei de siguranță” și să găsească soluții juridice noi;

AK. întrucât Decizia 2000/520/CE a Comisiei prevede că autoritățile competente din statele membre se pot folosi de atribuțiile de care dispun pentru a suspenda fluxurile de date către o organizație care și-a autodeclarat adeziunea la principiile „sferei de siguranță”, în vederea protejării persoanelor fizice cu privire la prelucrarea datelor lor cu caracter personal în cazurile în care există o probabilitate ridicată ca principiile „sferei de

[1] A se vedea în special hotărârea din 28 mai 1991, Francovich și alții/ Italia, C-6/90 și C-9/90.

siguranță” să fie încălcate sau dacă continuarea transferului de date ar genera un risc iminent de atingere gravă adusă persoanelor ale căror date sunt transferate;

AL. întrucât Decizia 2000/520/CE a Comisiei prevede, de asemenea, că în cazurile în care se demonstrează că un organism însărcinat cu asigurarea respectării principiilor nu își îndeplinește eficient rolul, Comisia trebuie să informeze Departamentul Comerțului al SUA și, în cazul în care este necesar, să prezinte măsuri în vederea abrogării sau suspendării deciziei ori a limitării domeniului de aplicare al acesteia;

AM. întrucât, în primele sale două rapoarte referitoare la punerea în aplicare a „sferei de siguranță”, publicate în 2002 și 2004, Comisia a identificat mai multe deficiențe în ceea ce privește aplicarea corectă a „sferei de siguranță” și a prezentat o serie de recomandări autorităților americane în vederea remedierii acestora;

AN. întrucât, în al treilea raport referitor la stadiul de punere în aplicare, din 27 noiembrie 2013, publicat la nouă ani după al doilea raport și fără ca vreo deficiență identificată în raportul anterior să fi fost remediată, Comisia a identificat și alte puncte slabe și neajunsuri de amploare în „sfera de siguranță” și a decis că punerea în aplicare nu poate continua în forma actuală; întrucât Comisia a subliniat că accesul extins al serviciilor de informații din SUA la datele transferate către SUA prin intermediul unor entități certificate ca făcând parte din „sfera de siguranță” dă naștere la noi întrebări grave legate de continuitatea protecției datelor referitoare la cetățenii UE; întrucât Comisia a adresat 13 recomandări autorităților SUA și s-a angajat să identifice, până în vara anului 2014, împreună cu autoritățile SUA, soluții care să fie aplicate cât mai repede și care să reprezinte baza unei revizuiri depline a funcționării principiilor „sferei de siguranță”;

AO. întrucât, în perioada 28-31 octombrie 2013, o delegație a Comisiei pentru libertăți civile, justiție și afaceri interne a Parlamentului European (Comisia LIBE) s-a întâlnit la Washington D.C. cu Departamentul Comerțului al SUA și cu Comisia Federală pentru Comerț a SUA; întrucât Departamentul Comerțului a recunoscut existența unor organizații care și-au autodeclarat adeziunea la principiile „sferei de siguranță”, dar care în mod clar au un „statut neactualizat”, ceea ce înseamnă că nu îndeplinesc cerințele „sferei de siguranță”, deși continuă să primească date cu caracter personal din partea UE; întrucât Comisia Federală pentru Comerț a recunoscut că „sfera de siguranță” ar trebui revizuită în vederea ameliorării, în special în ceea ce privește plângerile și sistemele de soluționare alternativă a litigiilor;

AP. întrucât principiile „sferei de siguranță” pot fi limitate la „ceea ce este necesar pentru respectarea securității naționale, a interesului public sau a cerințelor de aplicare a legii”; întrucât, ca excepție de la un drept fundamental, o astfel de excepție trebuie întotdeauna să fie interpretată în mod restrictiv și să fie limitată la ceea ce este necesar și proporțional într-o societate democratică, iar legislația trebuie să prevadă în mod clar condițiile și garanțiile care să asigure legitimitatea acestor limitări; întrucât domeniul de aplicare al acestei excepții ar fi trebuit să fie clarificat de SUA și de UE, îndeosebi de Comisie, pentru a se evita orice interpretare sau implementare care anulează, în fond, dreptul fundamental la viață privată și la protecția datelor, printre altele; întrucât, prin urmare, o astfel de excepție nu ar trebui să fie utilizată într-un mod care să submineze sau să anuleze protecția asigurată de Carta drepturilor fundamentale, de CEDO, de legislația UE privind protecția datelor și de principiile „sferei de siguranță”; insistă asupra faptului că, în cazul în care este invocată excepția pe motivul securității naționale, trebuie să se

precizeze în temeiul cărei legislații naționale;

AQ. întrucât accesul pe scară largă al serviciilor de informații ale SUA a erodat serios încrederea transatlantică și a avut un impact negativ asupra încrederii în organizațiile SUA cu activitate în UE; întrucât acest lucru este exacerbat și mai mult de lipsa unor căi de atac judiciare și administrative pentru cetățenii UE în temeiul legislației SUA, în special în cazul activităților de supraveghere utilizate în scopul colectării de informații;

Transferuri către țări terțe în baza deciziei privind caracterul adecvat

AR. întrucât, potrivit informațiilor dezvăluite și concluziilor anchetei desfășurate de Comisia LIBE, agențiile de securitate națională din Noua Zeelandă, Canada și Australia au fost implicate pe scară largă în activități de supraveghere în masă a comunicațiilor electronice și au cooperat în mod activ cu SUA în cadrul așa-numitului program *Five Eyes* (Cinci ochi) și este posibil să fi efectuat între ele schimburi de date cu caracter personal ale cetățenilor Uniunii transferate din UE;

AS. întrucât Comisia a declarat, în deciziile sale nr. 2013/65/UE[1] și 2002/2/CE[2], nivelurile de protecție asigurate de Legea privind protecția vieții private din Noua Zeelandă și de Legea privind protecția informațiilor cu caracter personal și a documentelor electronice din Canada ca fiind adecvate; întrucât dezvăluirile menționate anterior au afectat, de asemenea, în mod grav încrederea în sistemele juridice din aceste țări în ceea ce privește continuitatea protecției asigurate pentru cetățenii UE; întrucât Comisia nu a analizat acest aspect;

Transferuri în baza clauzelor contractuale și a altor instrumente

AT. întrucât Directiva 95/46/CE prevede că transferurile internaționale către o țară terță pot fi realizate, de asemenea, cu ajutorul unor instrumente specifice prin care operatorul de date prezintă garanții adecvate cu privire la protecția vieții private, a drepturilor fundamentale și a libertăților persoanelor fizice, precum și în ceea ce privește exercitarea respectivelor drepturi;

AU. întrucât astfel de garanții pot decurge în special din clauze contractuale specifice;

AV. întrucât Directiva 95/46/CE acordă Comisiei competența de a hotărî dacă anumite clauze contractuale standard oferă suficiente garanții obligatorii în temeiul directivei și întrucât, pe această bază, Comisia a adoptat trei modele de clauze contractuale standard pentru transferuri către operatorii și persoanele împuternicite de către operator (precum și persoanele secundare împuternicite de către operator) stabiliți în țările terțe;

AW. întrucât deciziile Comisiei de stabilire a clauzelor contractuale standard prevăd că autoritățile competente din statele membre își pot exercita atribuțiile de care dispun pentru a suspenda fluxurile de date în cazul în care se dovedește că legislația care reglementează activitatea importatorului sau a persoanei secundare împuternicite de către operatorul de date îi obligă pe aceștia să facă derogări de la legislația în vigoare privind protecția datelor cu mult peste restricțiile necesare într-o societate democratică, astfel cum este prevăzut la articolul 13 din Directiva 95/46/CE, în cazurile în care aceste cerințe de

[1] JO L 28, 30.1.2013, p. 12.
[2] JO L 2, 4.1.2002, p. 13.

derogare ar putea avea efecte negative considerabile asupra garanțiilor oferite de legislația în vigoare privind protecția datelor și de clauzele contractuale standard sau în cazurile în care este foarte probabil ca aceste clauze contractuale standard din anexă să nu fie respectate sau să urmeze a fi încălcate, generându-se astfel prin continuarea transferului un risc iminent de atingere gravă la adresa persoanelor ale căror date sunt transferate;

AX. întrucât autoritățile naționale de protecție a datelor au elaborat reguli corporatiste obligatorii (BCR) pentru a facilita transferurile internaționale în cadrul unei corporații multinaționale oferind garanții adecvate cu privire la protecția vieții private, a drepturilor fundamentale și a libertăților persoanelor, precum și în ceea ce privește exercitarea drepturilor în cauză; întrucât, înainte de a fi utilizate, BCR trebuie să fie autorizate de autoritățile competente ale statelor membre după ce acestea din urmă au evaluat conformitatea cu legislația Uniunii privind protecția datelor; întrucât BCR pentru agenții care prelucrează datele au fost respinse în raportul Comisiei LIBE referitor la Regulamentul general privind protecția datelor, deoarece ar priva operatorul de date și persoana vizată de orice control asupra jurisdicției în care sunt prelucrate datele acestora;

AY. întrucât Parlamentul European, dată fiind competența sa stipulată la articolul 218 din TFUE, are responsabilitatea de a monitoriza în permanență valoarea acordurilor internaționale asupra cărora și-a dat acordul;

Transferurile realizate pe baza acordurilor TFTP și PNR

AZ. întrucât, în Rezoluția sa din 23 octombrie 2013, Parlamentul European și-a exprimat preocuparea în legătură cu dezvăluirile referitoare la activitățile NSA în ceea ce privește accesul direct la mesaje de plăți financiare și informații conexe, ceea ce ar reprezenta o încălcare clară a acordului TFTP, în special a articolului 1;

BA. întrucât urmărirea finanțărilor în scopuri teroriste este un instrument esențial în lupta împotriva finanțării terorismului și a infracțiunilor grave, permițând anchetatorilor din domeniul combaterii terorismului să descopere legături între țintele anchetelor și alți potențiali suspecți asociați unor rețele teroriste extinse suspectate de finanțarea terorismului;

BB. întrucât Parlamentul European a solicitat Comisiei suspendarea acordului și a cerut ca toate informațiile și documentele pertinente să fie imediat puse la dispoziția Parlamentului în vederea deliberărilor; întrucât Comisia nu s-a conformat niciunei cerințe;

BC. întrucât, ca urmare a afirmațiilor apărute în mass-media, Comisia a hotărât să deschidă un proces de consultare cu SUA în temeiul articolului 19 din Acordul TFTP; întrucât, la 27 noiembrie 2013, comisarul Malmström a informat Comisia LIBE în legătură cu faptul că, după reuniunea cu autoritățile SUA și având în vedere răspunsurile acestora din schimbul de scrisori și din cadrul întâlnirilor, Comisia a hotărât să nu continue consultările pe motiv că nu există elemente care să dovedească faptul că guvernul SUA a acționat în mod contrar dispozițiilor acordului și că SUA a furnizat garanții scrise că nu s-a realizat nicio colectare directă de date care să contravină dispozițiilor Acordului TFTP; întrucât nu este clar dacă autoritățile americane au eludat acordul accesând astfel de date prin alte mijloace, după cum o arată scrisoarea din 18 septembrie 2013 adresată de

autoritățile americane[1];

BD. întrucât, cu ocazia misiunii delegației Comisiei LIBE la Washington din 28-31 octombrie 2013, aceasta a avut întâlniri cu Departamentul Trezoreriei al SUA; întrucât Trezoreria SUA a declarat că, de la intrarea în vigoare a Acordului TFTP, nu a mai avut acces la date SWIFT din UE decât în cadrul Acordului TFTP; întrucât Trezoreria SUA a refuzat să comenteze dacă un alt organism guvernamental sau departament al SUA ar fi avut acces la datele SWIFT în afara Acordului TFTP sau dacă administrația americană a avut cunoștință de activitățile de supraveghere în masă ale NSA; întrucât, la 18 decembrie 2013, dl Glenn Greenwald a declarat înainte de ancheta Comisiei LIBE că NSA și GCHQ vizaseră rețele SWIFT;

BE. întrucât autoritățile belgiene și neerlandeze de protecție a datelor au hotărât, la 13 noiembrie 2013, să efectueze o anchetă comună cu privire la securitatea rețelelor de plăți SWIFT cu scopul de a stabili dacă părți terțe ar putea obține acces neautorizat sau ilegal la datele bancare ale cetățenilor UE[2];

BF. întrucât, în conformitate cu Examinarea comună a Acordului PNR dintre SUA și UE, Departamentul pentru securitate internă (DHS) al SUA a transmis de 23 de ori date din PNR către NSA pentru fiecare caz în parte pentru a oferi asistență în cazuri de combatere a terorismului, în conformitate cu termenii specifici acordului;

BG. întrucât evaluarea comună nu menționează faptul că, în cazul prelucrării datelor cu caracter personal în scopuri de spionaj, conform legislației americane, cetățenii din afara SUA nu beneficiază de niciun instrument judiciar sau administrativ pentru a-și proteja drepturile, protecția constituțională fiind acordată exclusiv cetățenilor americani; întrucât lipsa de drepturi judiciare sau administrative anulează măsurile de protecție a cetățenilor UE prevăzute de Acordul PNR actual;

Transferuri efectuate în baza Acordului privind asistența judiciară reciprocă în materie penală dintre UE și SUA

BH. întrucât Acordul privind asistența juridică reciprocă în materie penală dintre UE și SUA din 6 iunie 2003[3] a intrat în vigoare la 1 februarie 2010 și vizează facilitarea cooperării dintre UE și SUA în vederea combaterii mai eficace a infracțiunilor, cu respectarea drepturilor persoanelor și a statului de drept;

Acordul-cadru privind protecția datelor în domeniul cooperării polițienești și judiciare („acordul-cadru”)

BI. întrucât scopul acestui acord general este de a stabili cadrul juridic pentru transferurile de date cu caracter personal între UE și SUA doar în scopurile prevenirii, anchetării, identificării sau urmăririi penale a infracțiunilor, inclusiv a infracțiunilor teroriste, în

---

1 În scrisoare se afirmă că „guvernul SUA caută și obține informații financiare… [...](care) sunt colectate prin mijloace normative și de aplicare a legii, pe cale diplomatică și prin canale de informații, precum și prin schimburi cu partenerii străini” și că „guvernul SUA utilizează TFTP pentru a obține date SWIFT pe care nu le putem obține din alte surse”.

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

3 JO L 181, 19.7.2003, p. 25.

cadrul cooperării polițienești și judiciare în materie penală; întrucât negocierile au fost autorizate de Consiliu la 2 decembrie 2010; întrucât acest acord este de o importanță crucială și va servi drept bază pentru facilitarea transferului de date în contextul cooperării judiciare și polițienești și în materie penală;

BJ. întrucât acest acord ar trebui să stabilească principii clare și precise, obligatorii din punct de vedere juridic, referitoare la prelucrarea datelor și ar trebui să recunoască, în special, dreptul cetățenilor UE la acces judiciar, la rectificarea și la ștergerea datelor lor cu caracter personal care din SUA, dreptul la o cale eficace de atac administrativă și judiciară pentru cetățenii UE din SUA, precum și la o supraveghere independentă a activităților de prelucrare a datelor;

BK. întrucât, în Comunicarea sa din 27 noiembrie 2013, Comisia a afirmat că „acordul-cadru” ar trebui să genereze un nivel ridicat de protecție a cetățenilor de ambele părți ale Oceanului Atlantic și să consolideze încrederea europenilor în schimburile de date dintre UE și SUA, constituind o bază pentru dezvoltarea cooperării în materie de securitate și de viitoare parteneriate între UE și SUA;

BL. întrucât negocierile privind acordul nu au înregistrat progrese din cauza poziției inflexibile a guvernului SUA, care refuză să recunoască drepturile efective la o cale de atac administrativă și judiciară pentru cetățenii UE și din cauza intenției de a acorda ample derogări de la principiile privind protecția datelor stabilite de acord, ca de exemplu limitarea scopului, păstrarea datelor sau transferarea lor mai departe pe plan intern sau extern;

Reforma privind protecția datelor

BM. întrucât cadrul juridic privind protecția datelor din UE este în curs de revizuire în vederea stabilirii unui sistem cuprinzător, coerent, modern și robust pentru toate activitățile de prelucrare a datelor de la nivelul Uniunii; întrucât, în ianuarie 2012, Comisia a prezentat un pachet de propuneri legislative: un regulament general privind protecția datelor[1], care va înlocui Directiva 95/46/CE și va stabili o legislație uniformă la nivelul întregii Uniuni, și o directivă[2] care va prevedea un cadru armonizat pentru toate activitățile de prelucrare a datelor realizate de autoritățile de aplicare a legii în scopuri de aplicare a legii și va reduce divergențele actuale dintre legislațiile naționale;

BN. întrucât, la 21 octombrie 2013, Comisia LIBE a adoptat rapoartele legislative referitoare la cele două propuneri și o decizie referitoare la deschiderea negocierilor cu Consiliul în vederea adoptării instrumentelor juridice pe perioada prezentei legislaturi;

BO. întrucât, deși Consiliul European din 24-25 octombrie 2013 a cerut adoptarea la timp a unui cadru general solid al UE privind protecția datelor, menit să încurajeze încrederea cetățenilor și a întreprinderilor în economia digitală, după doi ani de deliberări, Consiliul nu a reușit încă să ajungă la o abordare generală în legătură cu Regulamentul general privind protecția datelor și cu Directiva menționate anterior[3];

---

1 COM(2012)0011, 25.1.2012.
2 COM(2012)0010, 25.1.2012.
3 http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf

Securitatea informatică și cloud computingul

BP. întrucât rezoluția Parlamentului din 10 decembrie 2013 menționată mai sus subliniază potențialul economic al *cloud computingului* pentru creșterea economică și ocuparea forței de muncă; întrucât valoarea economică globală a pieței *cloud computingului* se estimează că va atinge 207 miliarde USD anual în 2016, de două ori mai mult față de valoarea înregistrată în 2012;

BQ. întrucât nivelul de protecție a datelor într-un mediu de tip *cloud* nu trebuie să fie inferior nivelului de protecție prevăzut în orice alt context de prelucrare a datelor; întrucât legislația Uniunii privind protecția datelor, neutră din punct de vedere tehnologic, se aplică deja în integralitate serviciilor de *cloud computing* din UE;

BR. întrucât activitățile de supraveghere în masă oferă serviciilor de informații acces la datele cu caracter personal stocate sau prelucrate în alt mod de persoane fizice din UE în cadrul acordurilor pentru servicii de tip *cloud* cu mari furnizori de tehnologie de acest tip din SUA; întrucât serviciile de informații americane au accesat date cu caracter personal stocate sau prelucrate în alt mod pe servere situate pe teritoriul UE prin intruziuni în rețelele interne ale Yahoo și Google; întrucât astfel de acțiuni reprezintă o încălcare a obligațiilor internaționale și a standardelor europene în materie de drepturi fundamentale, inclusiv dreptul la viață privată și dreptul la viața de familie, confidențialitatea comunicațiilor, prezumția de nevinovăție, libertatea de exprimare, libertatea de informare, libertatea de întrunire și de asociere și libertatea de a desfășura o activitate comercială; întrucât nu este exclus ca informațiile stocate în serviciile de tip *cloud* de către autorități sau întreprinderi publice, precum și de instituții ale statelor membre, să fi fost accesate și de serviciile de informații;

BS. întrucât serviciile de informații americane duc o politică de subminare sistematică a protocoalelor și a produselor criptografice pentru a putea intercepta chiar și comunicațiile criptate; întrucât Agenția Națională de Securitate a SUA a înregistrat un număr mare de așa-numite „atacuri în ziua zero” – vulnerabilități de securitate informatică necunoscute încă publicului sau vânzătorului produsului; întrucât astfel de activități subminează puternic eforturile depuse la nivel mondial în vederea îmbunătățirii securității informatice;

BT. întrucât faptul că serviciile de informații au accesat datele cu caracter personal ale utilizatorilor de servicii online a denaturat grav încrederea cetățenilor în aceste servicii și, ca urmare, are un efect negativ asupra întreprinderilor care investesc în dezvoltarea de servicii noi utilizând date voluminoase (*big data*) și aplicații noi precum „internetul obiectelor” (*Internet of Things*);

BU. întrucât vânzătorii de produse informatice livrează adeseori produse care nu au fost testate în mod corespunzător sub aspectul securității informatice sau care au uneori implantate aplicații de tip *backdoor* în mod intenționat de către vânzător; întrucât lipsa unor norme în materie de răspundere pentru vânzătorii de software a condus la o astfel de situație, care este exploatată de serviciile de informații, dar care prezintă și riscul unor atacuri din partea altor entități;

BV. întrucât este esențial ca întreprinderile care furnizează astfel de servicii și aplicații noi să respecte normele privind protecția datelor și viața privată a persoanelor vizate de colectarea, prelucrarea și analizarea datelor, pentru a menține un nivel ridicat de încredere

în rândul cetățenilor;

Supravegherea democratică a serviciilor de informații

BW. întrucât serviciilor de informații din societățile democratice li s-au conferit competențe și puteri speciale pentru a proteja drepturile fundamentale, democrația și statul de drept, drepturile cetățenilor și statul în fața amenințărilor interne și externe și acestea fac obiectul unei supravegheri judiciare și răspund în mod democratic; întrucât competențele și puterile speciale le-au fost conferite exclusiv în acest sens; întrucât aceste competențe ar trebui utilizate în limitele legale impuse de drepturile fundamentale, democrație și statul de drept, iar aplicarea lor ar trebui supravegheată cu strictețe, în caz contrar existând riscul de pierdere a legitimității și de subminare a democrației;

BX. întrucât faptul că serviciilor de informații li se atribuie un anumit nivel de secretizare, cu scopul de a evita punerea în pericol a operațiunilor în curs de desfășurare, dezvăluirea modurilor de operare sau punerea în pericol a vieților agenților, această secretizare nu poate să se suprapună peste sau să excludă normele privind controlul democratic și judiciar și examinarea activităților acestora, precum și normele privind transparența, în special în ceea ce privește respectarea drepturilor fundamentale și a statului de drept, pietre de temelie ale unei societăți democratice;

BY. întrucât majoritatea mecanismelor și organismelor de supraveghere existente la nivel național au fost înființate sau restructurate în anii 1990 și nu au fost neapărat adaptate la evoluțiile politice și tehnologice rapide din ultimul deceniu care au dus la intensificarea cooperării internaționale în materie de informații, și prin intermediul schimbului pe scară largă de date cu caracter personal, făcând neclară linia de demarcare dintre activitățile de informații și de aplicare a legii;

BZ. întrucât supravegherea democratică a activităților serviciilor de informații se desfășoară încă doar la nivel național, în ciuda intensificării schimbului de informații dintre statele membre ale UE și dintre statele membre și țări terțe; întrucât există un decalaj din ce în ce mai mare între nivelul cooperării internaționale, pe de o parte, și capacitățile de supraveghere limitate la nivel național, pe de altă parte, ceea ce duce la un control democratic insuficient și ineficace,

CA. întrucât organismele naționale de supraveghere nu au adeseori acces deplin la informațiile secrete primite din partea unui serviciu de informații străin, fapt ce poate să genereze lacune, iar schimburile de informații la nivel internațional pot avea loc fără o reexaminare adecvată; întrucât această problemă este agravată și mai mult de așa-numita „regulă a terțului” sau de principiul „controlului exercitat de partea emitentă”, care a fost conceput pentru a permite inițiatorului să mențină controlul asupra diseminării ulterioare a informațiilor sale sensibile, dar care este, din păcate, interpretat adeseori ca aplicându-se și la supravegherea serviciilor beneficiare;

CB. întrucât inițiativele publice și private de reformă în domeniul transparenței sunt esențiale pentru a asigura încrederea publicului în activitățile serviciilor secrete; întrucât sistemele juridice nu ar trebui să împiedice întreprinderile să divulge publicului informații despre modul în care acestea tratează toate tipurile de solicitări guvernamentale și de hotărâri judecătorești pentru accesul la datele utilizatorilor, inclusiv posibilitatea divulgării de informații agregate cu privire la numărul de solicitări și de hotărâri aprobate și respinse,

Constatări principale

1. consideră că dezvăluirile recente din presă ale denunțătorilor și jurnaliștilor, alături de dovezile specializate obținute pe parcursul anchetei, de confirmările autorităților și de lipsa infirmării anumitor acuzații, au contribuit la adunarea de probe care atestă existența unor sisteme vaste, complexe și foarte avansate din punct de vedere tehnologic, concepute de serviciile de informații ale SUA și ale unor state membre, pentru a colecta, a stoca și a analiza date privind comunicațiile, inclusiv date de conținut, date de localizare și metadate ale tuturor cetățenilor din întreaga lume, la o scară nemaiîntâlnită și într-un mod nediscriminant, fără a exista suspiciuni prealabile;

2. indică în special programele de spionaj ale NSA a SUA care au fost utilizate pentru supravegherea în masă a cetățenilor UE prin accesul direct la severele centrale ale principalilor furnizori de internet din SUA (programul PRISM), prin analiza conținutului și a metadatelor (programul Xkeyscore), prin eludarea criptărilor online (BULLRUN), prin accesul la rețelele de computere și telefonie și prin accesul la date privind poziția, precum și sistemele utilizate de serviciile de informații ale Regatului Unit GCHQ, ca de exemplu activitatea de supraveghere în amonte (programul Tempora), programul de decriptare (Edgehill), atacurile de tip *man-in-the-middle* asupra sistemelor de informații (programele Quantumtheory și Foxacid), precum și colectarea și reținerea a 200 de milioane de SMS-uri zilnic (programul Dishfire);

3. ia act de acuzațiile privind actele de piraterie cibernetică sau intruziune în sistemele Belgacom realizate de serviciile de informații din Marea Britanie, GCHQ; ia act de afirmația Belgacom, care nu a putut confirma, nici infirma, dacă instituțiile UE au constituit ținte ale atacurilor sau dacă au fost afectate și care a declarat că programele ostile utilizate (*malware*) erau extrem de complexe și necesitau, pentru a fi dezvoltate și utilizate, importante resurse financiare și umane, care nu ar fi la îndemâna unor entități sau a unor hackeri privați;

4. subliniază faptul că încrederea a fost profund zdruncinată: încrederea dintre cei doi parteneri transatlantici, încrederea dintre cetățeni și guvernele lor, încrederea în funcționarea instituțiilor democratice pe ambele părți ale Atlanticului, încrederea în respectarea statului de drept și încrederea în securitatea serviciilor și a comunicațiilor informatice; consideră că, pentru recâștigarea încrederii pe toate planurile, este nevoie de un plan cuprinzător de reacție rapidă care să conțină o serie de acțiuni ce fac obiectul controlului public;

5. ia act de faptul că sunt guverne care afirmă că aceste programe de supraveghere în masă sunt necesare pentru combaterea terorismului; denunță ferm terorismul, însă este profund convins că lupta împotriva terorismului nu poate justifica în niciun caz programele de supraveghere în masă secrete, fără ținte precise sau chiar ilegale; este de părere că, într-o societate democratică, aceste programe sunt incompatibile cu principiile necesității și proporționalității;

6. reamintește convingerea fermă a UE că este necesară atingerea unui echilibru între măsurile de securitate și protecția libertăților civile și a drepturilor fundamentale, asigurând, în același timp, respectarea absolută a vieții private și a protecției datelor;

7. consideră că o colectare de date de asemenea amploare ridică numeroase semne de întrebare cu privire la măsura în care aceste acțiuni vizează doar lupta împotriva terorismului, având în vedere că presupune colectarea tuturor datelor posibile ale tuturor cetățenilor; prin urmare, atrage atenția asupra existenței posibile a altor motive, printre care spionajul politic și economic, și asupra faptului că trebuie luate măsuri adecvate pentru a îndepărta aceste îndoieli;

8. pune sub semnul întrebării compatibilitatea activităților vaste de spionaj economic ale unor state membre cu legislația care reglementează piața internă și concurența, astfel cum sunt definite la titlurile I și VII din Tratatul privind funcționarea Uniunii Europene; reafirmă principiul cooperării sincere, astfel cum este definit la articolul 4 alineatul (3) din Tratatul privind Uniunea Europeană și principiul conform căruia statele membre „se abțin de la orice măsură care ar putea pune în pericol realizarea obiectivelor Uniunii”;

9. ia act de faptul că tratatele internaționale și legislația UE și a SUA, precum și mecanismele de supraveghere naționale, nu au reușit să asigure echilibrul și controlul necesar și nici răspunderea democratică;

10. condamnă colectarea la scară largă, sistemică și secretă a datelor cu caracter personal ale unor persoane nevinovate, cuprinzând în numeroase rânduri informații strict personale și private; subliniază faptul că sistemele de supraveghere nediferențiată în masă de către serviciile de informații constituie o imixtiune gravă în drepturile fundamentale ale cetățenilor; subliniază că viața privată nu este un drept de lux, ci reprezintă piatra de temelie a unei societăți libere și democratice; în continuare, subliniază că supravegherea în masă poate avea efecte negative grave asupra libertății presei, a libertății de gândire și de exprimare și a libertății de întrunire și de asociere și că poate conduce la cazuri grave de utilizare abuzivă a informațiilor colectate împotriva adversarilor politici; subliniază faptul că aceste activități de supraveghere în masă presupun de asemenea acțiuni ilegale ale serviciilor de informații și ridică probleme legate de extrateritorialitatea legislației naționale;

11. consideră esențială protejarea privilegiului secretului profesional al avocaților, jurnaliștilor, medicilor și al altor persoane care exercită profesii reglementate de activitățile de supraveghere în masă; subliniază în special că orice incertitudini legate de confidențialitatea informațiilor comunicate în cadrul relației dintre avocat și client ar putea avea un impact negativ asupra dreptului cetățenilor la consiliere juridică, asupra accesului la justiție și asupra dreptului la un proces echitabil;

12. consideră programele de supraveghere ca fiind încă un pas către constituirea unui stat pe deplin protejat, care schimbă paradigma cunoscută a dreptului penal în societăți democratice, conform căreia orice atingere adusă drepturilor fundamentale ale suspecților trebuie să fie autorizată de către un judecător sau procuror pe baza unei suspiciuni rezonabile și în condiții reglementate prin lege, și care promovează în locul acesteia activități de aplicare a legii combinate cu activități de spionaj, cu garanții juridice neclare și insuficiente, care adesea nu respectă principiul echilibrului și controlului democratic și drepturile fundamentale, în special prezumția de nevinovăție; în acest sens, reamintește hotărârea Curții Constituționale Federale din Germania[1] privind interzicerea utilizării unor filtre preventive („*präventive Rasterfahndung*”), cu excepția cazurilor în care există dovezi ale unui pericol concret la adresa altor drepturi majore protejate prin lege, și faptul

[1] 1 BvR 518/02 din 4 aprilie 2006.

că o amenințare generală sau tensiuni internaționale nu sunt suficiente pentru a justifica astfel de măsuri;

13. este convins de faptul că legile și tribunalele secrete reprezintă o încălcare a statului de drept; subliniază că orice hotărâre a unei instanțe sau a unui tribunal și orice decizie a unei autorități administrative a unui stat din afara UE, care autorizează, în mod direct sau indirect, transferul de date cu caracter personal, nu poate fi în niciun caz recunoscută sau aplicată, cu excepția situației în care există un tratat de asistență juridică reciprocă sau un acord internațional în vigoare între țara terță solicitantă și Uniune sau un stat membru și sau o autorizarea prealabilă din partea autorității de supraveghere competente; reamintește că nicio hotărâre pronunțată de o instanță sau un tribunal secret și nicio decizie a unei autorități administrative a unui stat din afara UE care autorizează în mod secret, direct sau indirect, activități de supraveghere, nu este recunoscută sau aplicată;

14. subliniază faptul că preocupările menționate mai sus sunt exacerbate de progresele rapide ale tehnologiei și ale societății, întrucât internetul și dispozitivele mobile sunt peste tot în viața modernă de zi cu zi („informatica omniprezentă”) și că modelul de afaceri al majorității furnizorilor de internet se bazează pe prelucrarea de date cu caracter personal; consideră că amploarea acestei probleme nu are precedent; constată că acest fenomen poate să atragă după sine exploatarea abuzivă a infrastructurii de colectare și prelucrare în masă a datelor în cazul schimbării regimului politic;

15. constată că nu există nicio garanție, nici pentru instituțiile publice ale UE, nici pentru cetățenii săi, în baza căreia securitatea informatică sau viața lor privată pot fi protejate de atacurile unor intruși foarte bine echipați (nu există securitate informatică 100 %); remarcă faptul că, pentru a asigura securitatea informatică maximă, europenii trebuie să fie dispuși să aloce suficiente resurse, atât umane, cât și financiare, pentru a menține independența și autonomia Europei în domeniul IT;

16. respinge cu fermitate concepția conform căreia toate chestiunile legate de programele de supraveghere în masă reprezintă strict o problemă de securitate națională și țin deci de competența exclusivă a statelor membre; reiterează că statele membre trebuie să respecte pe deplin dreptul UE și Convenția europeană a drepturilor omului atunci când acționează în vederea asigurării securității naționale; reamintește o hotărâre recentă a Curții de Justiție conform căreia „deși adoptarea măsurilor apte să asigure siguranța lor internă și externă este de competența statelor membre, simplul fapt că o decizie privește siguranța statului nu poate determina inaplicabilitatea dreptului Uniunii”[1]; în plus, reamintește faptul că sunt în joc protecția vieții private a tuturor cetățenilor UE, precum și securitatea și fiabilitatea tuturor rețelelor de comunicații din UE; prin urmare, este convins că discuțiile și acțiunile de la nivelul UE sunt nu numai legitime, ci reprezintă și o chestiune legată de autonomia UE;

17. salută instituțiile și experții care au contribuit la această anchetă; regretă faptul că autorități din mai multe state membre au refuzat cooperarea în cadrul anchetei efectuate de Parlamentul European în numele cetățenilor; salută faptul că mai mulți membri ai Congresului și ai parlamentelor naționale au fost cooperanți;

18. este conștient de faptul că, într-un timp atât de scurt, a fost posibilă realizarea doar a unei anchete preliminare privind toate chestiunile puse în discuție din iulie 2013; este conștient

[1] Hotărârea în cauza C-300/11, ZZ/Secretary of State for the Home Department, 4 iunie 2013.

atât de amploarea dezvăluirilor de care este vorba, cât și de faptul că ele evoluează constant; adoptă prin urmare o abordare prospectivă care constă într-un set de propuneri specifice și un mecanism de monitorizare în cadrul următoarei legislaturi parlamentare, care să garanteze că respectivele constatări rămân o prioritate pe agenda politică a UE;

19. intenționează să solicite Comisiei să-și asume, după alegerile europene din mai 2014, angajamente politice ferme privind punerea în aplicare a propunerilor și recomandărilor acestei anchete;

Recomandări

20. invită autoritățile SUA și statele membre ale UE care nu au făcut încă acest lucru să interzică activitățile secrete de supraveghere în masă;

21. invită statele membre ale UE, îndeosebi cele care participă la așa-numitele programe „9 ochi" și „14 ochi"[1], să își evalueze în detaliu și să își revizuiască, dacă este necesar, legislația națională și practicile interne care vizează activitățile serviciilor de informații pentru a se asigura că acestea fac obiectul supravegherii parlamentare și judiciare și controlului public, că respectă principiile privind legalitatea, necesitatea și proporționalitatea, respectarea garanțiilor procedurale, notificarea utilizatorului și transparența, inclusiv în raport cu manualul bunelor practici al ONU și cu recomandările Comisiei de la Veneția, asigurându-se că sunt în conformitate cu standardele Convenției europene a drepturilor omului și că respectă obligațiile în materie de drepturi fundamentale ale statelor membre, îndeosebi în ceea ce privește protecția datelor, viața privată și prezumția de nevinovăție;

22. invită toate statele membre ale UE, în special, având în vedere Rezoluția sa din 4 iulie 2013 și audierile privind anchetele, Regatul Unit, Franța, Germania, Suedia, Țările de Jos și Polonia, să se asigure că actualele sau viitoarele lor cadre legislative și mecanisme de supraveghere care reglementează activitățile agențiilor de informații respectă standardele convenției europene a drepturilor omului și legislația Uniunii Europene privind protecția datelor cu caracter personal; invită statele membre în cauză să clarifice acuzațiile privind activitățile de supraveghere în masă, inclusiv supravegherea în masă a telecomunicațiilor transfrontaliere, supravegherea fără ținte precise a comunicațiilor prin cablu, posibilele acorduri încheiate între serviciile de informații și societățile de telecomunicații în ceea ce privește accesul și schimbul de date cu caracter personal și accesul la cablurile transatlantice, prezența personalului și echipamentelor serviciilor americane de informații pe teritoriul UE fără controlul operațiunilor de supraveghere și compatibilitatea acestora cu legislația UE; invită parlamentele naționale ale țărilor în cauză să își intensifice cooperarea cu organismele de supraveghere a serviciilor de informații la nivel european;

23. invită Regatul Unit, în special având în vedere relatările numeroase din mass-media referitoare la supravegherea în masă de către serviciile de informații GCHQ, să își revizuiască actualul cadru juridic bazat pe o „interacțiune complexă" între trei părți separate de legislație – *Human Rights Act* (legea privind drepturile omului) din 1998, *Intelligence Services Act* (Legea privind serviciile de informații) din 1994 și *Regulation of*

[1] La „programul 9 ochi" participă SUA, Regatul Unit, Canada, Australia, Noua Zeelandă, Danemarca, Franța, Norvegia și Țările de Jos; la „programul 14 ochi" participă țările menționate și Germania, Belgia, Italia, Spania și Suedia.

Investigatory Powers Act (Regulamentul privind competențele puterilor cu atribuții de investigare) din 2000;

24. ia act de revizuirea Legii olandeze din 2002 privind informațiile și securitatea (raportul Comisiei Dessens din 2 decembrie 2013); sprijină recomandările comisiei de reexaminare care vizează consolidarea transparenței, activității de control și de supraveghere a serviciilor olandeze de informații; invită Țările de Jos să se abțină de la extinderea competențelor serviciilor de informații, astfel încât supravegherea neindividualizată și la scară mare să se poată realiza și asupra comunicațiilor prin cablu ale cetățenilor nevinovați, îndeosebi având în vedere că cele mai mari puncte de Internet Exchange din lume sunt instalate la Amsterdam (AMS-IX); face apel la prudență la definirea mandatului și a capacităților noii Unități cibernetice comune SIGINT, precum și în ceea ce privește prezența și operațiunile personalului serviciilor de informații al SUA pe teritoriul olandez;

25. invită statele membre, inclusiv atunci când acestea sunt reprezentate de propriile servicii de informații, să nu accepte de la țări terțe date care au fost colectate în mod ilegal și să nu permită pe teritoriul lor activități de supraveghere desfășurate de guvernele sau serviciile țărilor terțe care sunt ilegale în temeiul dreptului național sau care nu respectă garanțiile juridice prevăzute de instrumentele internaționale sau ale UE, inclusiv protecția drepturilor omului în temeiul TUE, a Convenției CEDO și a Cartei drepturilor fundamentale a UE;

26. solicită să se pună capăt interceptărilor în masă și procesării de imagini de pe camere web de către orice serviciu secret; solicită statelor membre să investigheze detaliat dacă, în ce fel și în ce măsură serviciile lor secrete au fost implicate în colectarea și procesarea de imagini de pe camere web și să șteargă toate imaginile stocate care au fost colectate prin astfel de programe de supraveghere în masă;

27. invită statele membre să își îndeplinească imediat obligația pozitivă prevăzută de Convenția europeană a drepturilor omului în ceea ce privește protejarea cetățenilor săi de supravegherea efectuată de țări terțe sau de propriile servicii de informații ale acestora și care contravine cerințelor convenției, inclusiv în cazul în care este vizată garantarea securității naționale, și să garanteze că statul de drept nu este afectat de aplicarea extrateritorială a legislației unei țări terțe;

28. îl invită pe Secretarul General al Consiliului Europei să demareze procedura bazată pe articolul 52 conform căreia „orice Înaltă Parte Contractantă va furniza, la solicitarea Secretarului General al Consiliului Europei, explicațiile cerute asupra modului în care dreptul său intern asigură aplicarea efectivă a tuturor dispozițiilor acestei convenții”;

29. invită statele membre să ia imediat măsurile adecvate, inclusiv acțiuni în instanță, împotriva încălcării suveranității lor și prin urmare a încălcării dreptului public internațional, comise prin intermediul programelor de supraveghere în masă; de asemenea, invită statele membre să utilizeze toate instrumentele internaționale disponibile pentru apărarea drepturilor fundamentale ale cetățenilor UE, în special prin declanșarea procedurii reclamațiilor între state în baza articolului 41 din Pactul internațional cu privire la drepturile civile și politice (PIDCP);

30. solicită statelor membre să instituie mecanisme eficace prin care cei care sunt responsabili de programe de supraveghere (în masă) ce contravin statului de drept și drepturilor

fundamentale ale cetățenilor să fie trași la răspundere pentru acest abuz de putere;

31. invită SUA să își revizuiască fără întârziere legislația, astfel încât să fie conformă cu dreptul internațional, să recunoască viața privată și celelalte drepturi ale cetățenilor UE, să ofere căi de atac judiciare cetățenilor UE, să plaseze drepturile cetățenilor UE pe picior de egalitate cu drepturile cetățenilor SUA și să semneze protocolul opțional care recunoaște reclamațiile individuale în temeiul PIDCP;

32. salută în această privință observațiile formulate și Directiva prezidențială emisă de președintele american Obama la 17 ianuarie 2014 ca un pas spre a limita autorizarea utilizării supravegherii și a prelucrării datelor în scopuri legate de securitatea națională și spre a asigura un tratament egal al informațiilor cu caracter personal ale tuturor persoanelor, indiferent de naționalitate sau cetățenie, din partea comunității americane a serviciilor secrete; așteaptă însă, în contextul relațiilor UE-SUA, măsuri specifice noi, care, mai mult decât orice, să consolideze încrederea în transferurile transatlantice de date și să ofere garanții obligatorii pentru drepturi aplicabile în materie de viață privată ale cetățenilor UE, după cum descrie în detaliu prezentul raport;

33. își exprimă profunda îngrijorare în legătură cu lucrările Comisiei pentru Convenția privind criminalitatea informatică din cadrul Consiliului European în ceea ce privește interpretarea articolului 32 din Convenția privind criminalitatea informatică din 23 noiembrie 2001 (Convenția de la Budapesta) privind accesul transfrontalier la date informatice stocate cu consimțământ sau dacă acestea sunt disponibile publicului și se opune oricărei încheieri a unui protocol adițional sau a unor orientări menite să extindă domeniul de aplicare al prezentei prevederi dincolo de regimul actual instituit prin convenția în cauză, care reprezintă deja o excepție majoră de la principiul teritorialității, deoarece ar putea avea drept urmare accesul liber la distanță al autorităților de aplicare a legii la servere și computere localizate în alte jurisdicții, fără ca acestea să recurgă la acordurile de asistență juridică reciprocă și la alte instrumente de cooperare judiciară introduse pentru a garanta drepturile fundamentale ale cetățenilor, inclusiv protecția datelor și respectarea procedurilor, în special Convenția nr. 108 a Consiliului Europei;

34. invită Comisia să efectueze, înainte de iulie 2014, o evaluare a aplicabilității Regulamentului (CE) nr. 2271/96 în cazurile de conflict de legi privind transferurile de date cu caracter personal;

35. invită Agenția pentru Drepturi Fundamentale a Uniunii Europene să efectueze cercetări detaliate referitoare la protecția drepturilor fundamentale în contextul supravegherii, în special referitoare la situația juridică actuală a cetățenilor UE în ceea ce privește căile de atac de care dispun în legătură cu practicile în cauză;

Transferurile internaționale de date

Cadrul juridic al SUA privind protecția datelor și „sfera de siguranță” a SUA

36. ia act de faptul că întreprinderile pe care dezvăluirile mass-mediei le-au indicat ca fiind implicate în supravegherea în masă a cetățenilor UE de către NSA a SUA sunt companii care și-au autodeclarat adeziunea la „sfera de siguranță”, acesta fiind instrumentul juridic utilizat pentru transferul datelor cu caracter personal din UE către SUA (printre ele numărându-se Google, Microsoft, Yahoo!, Facebook, Apple, LinkedIn); își exprimă îngrijorarea în legătură cu faptul că aceste organizații nu criptează informațiile și

comunicațiile care circulă între centrele lor de date, făcând astfel posibilă interceptarea informațiilor de către serviciile de informații; salută declarațiile ulterioare ale unora dintre companii americane potrivit cărora vor accelera planurile de criptare a fluxurilor de date la nivelul propriilor centre de date globale;

37. consideră că accesul la scară largă a serviciilor de informații ale SUA la datele cu caracter personal din UE prelucrate în cadrul „sferei de siguranță” nu respectă criteriile pentru derogare în temeiul „securității naționale”;

38. este de părere că, întrucât, în contextul actual, principiile „sferei de siguranță” nu oferă o protecție adecvată a cetățenilor UE, aceste transferuri ar trebui efectuate prin intermediul altor instrumente, cum ar fi clauzele contractuale sau regulile corporatiste obligatorii (BCR), cu condiția ca aceste instrumente să stabilească garanții și protecții specifice, care să nu fie împiedicate de alte cadre juridice;

39. consideră că Comisia nu a luat măsurile necesare în vederea remedierii deficiențelor cunoscute ale actualului proces de implementare a „sferei de siguranță”;

40. invită Comisia să prezinte măsuri care să prevadă suspendarea imediată a Deciziei 2000/520/CE a Comisiei, care confirmă caracterul adecvat al protecției oferite de principiile „sferei de siguranță” și al întrebărilor de bază aferente, publicate de Departamentul Comerțului al SUA; prin urmare, invită autoritățile SUA să prezinte o propunere referitoare la un nou cadru privind transferul de date cu caracter personal din UE în SUA care să respecte legislația Uniunii privind protecția datelor și să prevadă un nivel adecvat de protecție;

41. invită autoritățile competente ale statelor membre, în special autoritățile de protecție a datelor, să utilizeze atribuțiile de care dispun și să suspende fără întârziere fluxurile de date către toate organizațiile care și-au autodeclarat adeziunea la principiile „sferei de siguranță” și să solicite ca fluxurile în cauză să fie realizate exclusiv în cadrul altor instrumente, cu condiția ca acestea să prezinte garanțiile și asigurările adecvate cu privire la viața privată, drepturile fundamentale și libertățile persoanelor;

42. invită Comisia să prezinte până în decembrie 2014 o evaluare cuprinzătoare a cadrului SUA privind viața privată care să reglementeze activitățile comerciale, de aplicare a legii și ale serviciilor de informații, precum și recomandări concrete, având în vedere lipsa unei legislații generale în materie de protecție a datelor în Statele Unite; încurajează Comisia să colaboreze cu administrația SUA pentru a stabili un cadru legal care să prevadă un nivel înalt de protecție a indivizilor în cazul transferului datelor lor cu caracter personal în SUA și să asigure compatibilitatea cadrelor european și american privind viața privată;

Transferuri către alte țări terțe în temeiul deciziei privind caracterul adecvat

43. reamintește că Directiva 95/46/CE prevede că transferul de date cu caracter personal către o țară terță poate fi efectuat doar în cazul în care, fără a aduce atingere conformității cu dispozițiile naționale adoptate în temeiul altor dispoziții ale directivei, țara terță în cauză asigură un nivel adecvat de protecție, scopul acestei dispoziții vizând asigurarea continuității protecției garantate de legislația UE în materie de protecție a datelor în cazurile în care datele cu caracter personal sunt transferate în afara UE;

44. reamintește că Directiva 95/46/CE prevede că este necesară evaluarea caracterului

adecvat al nivelului de protecție asigurat de o țară terță ținând cont de toate circumstanțele specifice unei operațiuni de transfer de date sau unui set de astfel de operațiuni; de asemenea, reamintește că directiva menționată mai sus conferă totodată Comisiei competențe de punere în aplicare conform cărora Comisia poate afirma dacă o țară terță asigură un nivel adecvat de protecție în temeiul criteriilor prevăzute de Directiva 95/46/CE; reamintește că Directiva 95/46/CE conferă Comisiei competența de a comunica dacă o țară terță nu asigură un nivel adecvat de protecție;

45. reamintește că, în cazul din urmă, statele membre trebuie să ia măsurile necesare pentru a împiedica transferurile de date de același tip către țara terță în cauză și că Comisia trebuie să deschidă negocieri în vederea remedierii situației;

46. invită Comisia și statele membre să stabilească fără întârziere dacă nivelurile adecvate de protecție asigurate de Legea privind protecția vieții private din Noua Zeelandă și de Legea privind protecția informațiilor cu caracter personal și a documentelor electronice din Canada, așa cum se stipulează în Deciziile Comisiei 2013/65/UE și 2002/2/CE, au fost afectate de implicarea serviciilor lor naționale de informații în activitățile de supraveghere în masă a cetățenilor UE și, după caz, să ia măsuri adecvate de suspendare sau de contracarare a deciziilor privind caracterul adecvat; de asemenea, invită Comisia să evalueze situația pentru alte țări a cărora adecvare a fost evaluată; se așteaptă ca Comisia să prezinte Parlamentului European constatările sale referitoare la țările menționate mai sus până cel târziu în decembrie 2014;

Transferuri în temeiul clauzelor contractuale și al altor instrumente

47. reamintește că autoritățile naționale de protecție a datelor au arătat că nu au fost prevăzute nici clauze contractuale tip, nici BCR în cazurile de acces la datele cu caracter personal în scopuri de supraveghere în masă și că un astfel de acces nu respectă clauzele de derogare de la clauzele contractuale sau de la BCR care se referă la derogări excepționale justificate de interesul legitim într-o societate democratică și numai atunci când acest lucru este necesar și proporțional;

48. invită statele membre să interzică sau să suspende fluxurile de date către țări terțe bazate pe clauze contractuale tip, pe clauze contractuale sau pe BCR autorizate de autoritățile naționale competente în cazurile în care este posibil ca legislația în care se încadrează destinatarul datelor să îi impună cerințe care sunt cu mult peste restricțiile strict necesare, adecvate și proporționale într-o societate democratică și care riscă să aibă efecte negative asupra garanțiilor oferite de legislația aplicabilă în materie de protecție a datelor și de clauzele contractuale tip, sau pentru că continuarea transferului ar crea un risc de prejudicii grave pentru persoanele ale căror date sunt transferate;

49. invită Grupul de lucru privind articolul 29 să elaboreze orientări și recomandări privind garanțiile și protecțiile care trebuie prevăzute de instrumentele contractuale pentru transferurile internaționale de date cu caracter personal din UE în vederea asigurării protecției vieții private, a drepturilor fundamentale și a libertăților persoanelor, ținând cont îndeosebi de legislațiile din țările terțe privind activitățile de intelligence și securitatea națională, precum și implicarea companiilor care primesc date într-o țară terță în urma unor activități de supraveghere în masă ale serviciilor de informații ale țării terțe;

50. invită Comisia să examineze fără întârziere clauzele contractuale tip pe care le-a stabilit pentru a determina dacă acestea asigură protecția necesară în ceea ce privește accesul la

datele cu caracter personal transferate în temeiul clauzelor în scopuri de intelligence și, dacă se dovedește a fi nevoie, să le revizuiască;

Transferuri în temeiul Acordului de asistență juridică reciprocă

51. invită Comisia să efectueze înainte de finele anului 2014 o evaluare aprofundată a actualului Acord de asistență juridică reciprocă, în temeiul articolului 17 din acest acord, cu scopul de a verifica aplicarea sa efectivă și de a vedea, în special, dacă SUA s-a folosit în mod real de acest acord pentru a obține informații sau probe din UE și dacă acordul a fost ocolit pentru a obține informații direct din UE, și de a evalua impactul acordului asupra drepturilor fundamentale ale persoanelor; o astfel de evaluare nu ar trebui să se refere exclusiv la declarațiile oficiale ale SUA ca elemente suficiente pentru analiză, ci să se bazeze și pe evaluări specifice ale UE; această examinare aprofundată ar trebui să abordeze și consecințele aplicării structurii constituționale a UE asupra acestui instrument în vederea conformității cu dreptul Uniunii, luând în considerare în special Protocolul nr. 36 și articolul 10 al acestuia, precum și Declarația nr. 50 referitoare la acest protocol; solicită în aceeași măsură Consiliului și Comisiei să evalueze acordurile bilaterale dintre statele membre și Statele Unite cu scopul de a supraveghea congruența dintre aceste acorduri și cele pe care UE le menține sau decide să le mențină cu Statele Unite;

Asistența reciprocă a UE în materie penală

52. solicită Consiliului și Comisiei să informeze Parlamentul în legătură cu utilizarea efectivă de către statele membre a Convenției privind asistența reciprocă în materie penală între statele membre, în special titlul III referitor la interceptarea telecomunicațiilor; invită Comisia să înainteze o propunere, în conformitate cu Declarația nr. 50, referitoare la Protocolul nr. 36, potrivit solicitării, înainte de finele anului 2014 în vederea adaptării acestuia la cadrul prevăzut de Tratatul de la Lisabona;

Transferuri realizate în cadrul acordurilor TFTP și PNR

53. este de părere că informațiile furnizate de Comisia Europeană și de Trezoreria SUA nu clarifică dacă serviciile de informații ale SUA au acces la mesajele financiare ale SWIFT din UE prin interceptarea rețelelor SWIFT sau a sistemelor de operare ale băncilor sau a rețelelor de comunicații, singure sau în cooperare cu serviciile naționale de informații din UE sau fără a face apel la canalele bilaterale existente de asistență juridică reciprocă și de cooperare judiciară;

54. reiterează rezoluția sa din 23 octombrie 2013 și cere Comisiei suspendarea Acordului TFTP;

55. invită Comisia să răspundă îngrijorărilor datorate faptului că trei dintre cele mai importante sisteme computerizate de rezervare folosite de companiile aeriene în toată lumea sunt situate în SUA și că datele din PNR sunt salvate în sisteme de tip *cloud* care funcționează pe teritoriul SUA și se supun dreptului american, care nu este adecvat pentru protecția datelor;

Acordul-cadru privind protecția datelor în domeniul cooperării polițienești și judiciare („acordul cadru”)

56. consideră că o soluție satisfăcătoare în cadrul „acordului cadru” constituie o premisă

pentru restaurarea completă a încrederii între partenerii transatlantici;

57. cere reluarea imediată a negocierilor cu SUA cu privire la „acordul cadru”, care ar trebui să prevadă ca drepturile cetățenilor UE să fie pe picior de egalitate cu drepturile cetățenilor SUA; subliniază de asemenea că acordul în cauză ar trebui să prevadă căi de atac administrative și judiciare efective și aplicabile pentru toți cetățenii UE din SUA, fără nicio discriminare;

58. solicită Comisiei și Consiliului să nu inițieze cu SUA noi acorduri sectoriale sau contracte referitoare la transferul de date cu caracter personal în scopuri de aplicare a legii, atât timp cât „acordul cadru” nu a intrat în vigoare;

59. îndeamnă Comisia să raporteze în detaliu despre diferitele puncte ale mandatului de negociere și despre ultimele schimbări ale situației până în aprilie 2014;

Reforma privind protecția datelor

60. invită Președinția Consiliului și statele membre să își intensifice activitatea referitoare la pachetul de măsuri privind protecția datelor în vederea adoptării acestora în 2014, astfel încât cetățenii UE să se poată bucura de un nivel înalt de protecție în viitorul foarte apropiat; subliniază că Consiliul trebuie să își asume un angajament ferm și să își declare sprijinul deplin pentru a da dovadă de credibilitate și hotărâre față de țările terțe;

61. subliniază faptul că atât Regulamentul, cât și Directiva privind protecția datelor sunt necesare pentru protejarea drepturilor fundamentale ale persoanelor și, prin urmare, ambele trebuie abordate ca un pachet de adoptat în același timp, în vederea asigurării că toate activitățile de prelucrare a datelor din UE oferă un nivel ridicat de protecție în orice împrejurare; subliniază faptul că va adopta măsuri suplimentare de cooperare în domeniul aplicării legii doar după ce Consiliul începe negocierile cu Parlamentul și cu Comisia cu privire la pachetul de măsuri privind protecția datelor;

62. reamintește faptul că noțiunile de „respectare a vieții private începând cu momentul conceperii” și de „respectare implicită a vieții private” consolidează protecția datelor și ar trebui să fie utilizate ca orientări pentru toate produsele, serviciile și sistemele furnizate pe internet;

63. consideră că asigurarea unui grad mai ridicat de transparență și a unor standarde de siguranță mai înalte pentru mediul online și telecomunicații reprezintă un factor necesar pentru îmbunătățirea regimului privind protecția datelor; prin urmare, solicită Comisiei să prezinte o propunere legislativă referitoare la termenii și condițiile generale standardizate pentru mediul online și serviciile de telecomunicații și să acorde un mandat unui organism de supraveghere care să monitorizeze respectarea termenilor și condițiilor respective;

Cloud computing

64. ia act de faptul că încrederea în *cloud* computing și în furnizorii acestei tehnologii din SUA a fost afectată în mod negativ de practicile menționate mai sus; subliniază, prin urmare, că dezvoltarea serviciilor de tip *cloud* și a soluțiilor informatice la nivel european reprezintă un element esențial pentru creștere și ocuparea forței de muncă, pentru încrederea în aceste servicii și în furnizorii lor, precum și pentru asigurarea unui nivel ridicat al protecției datelor cu caracter personal;

65. solicită tuturor organismelor publice din Uniune să nu utilizeze servicii de tip *cloud* în situația în care s-ar putea aplica alte legislații decât legislația UE;

66. își exprimă din nou preocupările profunde cu privire la divulgarea directă obligatorie către autoritățile din țările terțe a datelor și a informațiilor cu caracter personal din UE, prelucrate în temeiul unor acorduri privind serviciile de *cloud*, de către furnizorii de servicii de *cloud*, sub rezerva legislației din țara terță sau prin utilizarea unor servere de stocare localizate în țări terțe, și în legătură cu accesul direct de la distanță la datele și informațiile cu caracter personal prelucrate de autoritățile de aplicare a legii și de serviciile de informații din țările terțe;

67. deplânge faptul că acest tip de acces este obținut de obicei prin aplicarea directă de către autoritățile din țările terțe a propriilor norme juridice, fără a se utiliza instrumentele internaționale destinate cooperării judiciare, cum ar fi acordurile de asistență judiciară reciprocă sau alte forme de cooperare judiciară:

68. invită Comisia și statele membre să accelereze lucrările parteneriatului european pentru *cloud* și să implice, în același timp, pe deplin societatea civilă și comunitatea tehnică, cum ar fi Internet Engineering Task Force (IETF), precum și să integreze aspectele legate de protecția datelor;

69. îndeamnă Comisia ca, în cazul în care negociază acorduri internaționale care implică prelucrarea datelor cu caracter personal, să acorde o atenție deosebită riscurilor și provocărilor pe care *cloud* computingul le reprezintă pentru drepturile fundamentale, în special, dar nu numai, pentru dreptul la viață privată și la protecția datelor cu caracter personal, astfel cum se prevede la articolele 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene; îndeamnă, de asemenea, Comisia să ia act de normele interne ale partenerilor de negociere care reglementează accesul autorităților de aplicare a legii și al serviciilor de informații la datele cu caracter personal prelucrate prin servicii de *cloud* computing, în special solicitând acordarea accesului numai cu condiția ca acestea să respecte pe deplin garanțiile procedurale și să existe un temei juridic lipsit de ambiguități, precum și cerința de a specifica condițiile exacte de acordare a accesului, scopul obținerii accesului, măsurile de securitate instituite cu privire la transmiterea datelor și drepturile cetățenilor, precum și normele în materie de supraveghere și un mecanism eficient de soluționare a litigiilor;

70. reamintește că toate întreprinderile care furnizează servicii în UE trebuie să respecte, fără excepție, dreptul UE și sunt răspunzătoare pentru orice încălcări ale acestuia și subliniază faptul că este important să existe sancțiuni administrative eficace, proporționale și disuasive care să poată fi aplicate furnizorilor de servicii de *cloud* computing care nu respectă standardele UE în materie de protecție a datelor;

71. invită Comisia și autoritățile competente ale statelor membre să evalueze măsura în care normele UE în materie de confidențialitate și de protecție a datelor au fost încălcate prin colaborarea persoanelor juridice din UE cu serviciile secrete sau prin acceptarea ordinelor judecătorești ale autorităților țărilor terțe prin care se solicită date cu caracter personal ale cetățenilor UE, ceea ce contravine legislației UE privind protecția datelor;

72. invită întreprinderile care furnizează servicii noi utilizând „volume mari de date” („Big Data”) și aplicații noi, cum ar fi „internetul obiectelor”, să aplice deja măsuri de protecție a datelor din etapa de dezvoltare, în scopul de a menține un nivel ridicat de încredere în

rândul cetățenilor;

Acordul referitor la parteneriatul transatlantic pentru comerț și investiții (TTIP)

73. ia act de faptul că UE și SUA continuă negocierile în vederea unui parteneriat transatlantic pentru comerț și investiții, care are o importanță strategică majoră pentru crearea de creștere economică;

74. subliniază cu fermitate că, având în vedere importanța economiei digitale pentru relațiile UE-SUA și pentru obiectivul reconstruirii încrederii dintre cele două părți, aprobarea de către Parlamentul European a acordului final TTIP ar putea fi periclitată atât timp cât nu se încetează definitiv activitățile secrete de supraveghere în masă, precum și interceptarea comunicațiilor în cadrul instituțiilor UE și al reprezentanțelor diplomatice și în absența unei soluții adecvate în ceea ce privește dreptul cetățenilor UE la confidențialitatea datelor, inclusiv la căi de atac administrative și judiciare; subliniază faptul că este posibil ca Parlamentul European să aprobe acordul final TTIP doar cu condiția ca acordul să respecte în totalitate, printre altele, drepturile fundamentale recunoscute de carta UE, și ca protecția vieții private a persoanelor în raport cu prelucrarea și diseminarea datelor cu caracter personal să fie reglementată în continuare de articolul XIV din Acordul General privind Comerțul cu Servicii (GATS); subliniază faptul că legislația UE privind protecția datelor nu poate fi considerată „o discriminare arbitrară sau nejustificabilă” în conformitate cu articolul XIV din GATS;

Supravegherea democratică a serviciilor de informații

75. subliniază că, în ciuda faptului că supravegherea activităților serviciilor de informații ar trebui să se bazeze deopotrivă pe legitimitate democratică (cadru juridic solid, autorizare ex ante și verificare ex post) și pe capacitate și expertiză tehnică adecvate, acestea lipsesc în mod dramatic majorității actualelor organisme de supraveghere din UE și SUA, în special în ceea ce privește capacitățile tehnice;

76. invită (așa cum a făcut-o și în cazul Echelon) toate parlamentele naționale care nu au făcut-o încă să instituie supravegherea rezonabilă a activităților de intelligence de către parlamentari sau de organisme de experți cu atribuții juridice de investigare; invită parlamentele naționale să asigure că astfel de comisii/organisme de supraveghere dispun de suficiente resurse, expertiză tehnică și mijloace juridice, inclusiv de dreptul de a efectua inspecții la fața locului, pentru a putea să controleze în mod efectiv serviciile de informații;

77. solicită înființarea a unui grup alcătuit din deputați și experți care să examineze, în mod transparent și în colaborare cu parlamentele naționale, recomandările pentru a consolida supravegherea democratică, inclusiv controlul parlamentar, al serviciilor de informații și pentru a intensifica colaborarea în domeniul supravegherii în UE, îndeosebi în ceea ce privește dimensiunea sa transfrontalieră; consideră că grupul ar trebui să examineze, în special, posibilitatea adoptării unor standarde europene sau orientări minime cu privire la supravegherea (ex ante sau ex post) a serviciilor de informații pe baza bunelor practici existente și a recomandărilor adresate de organismele internaționale (ONU, Consiliul Europei), inclusiv a faptului că organismele lor de supraveghere sunt considerate terți în temeiul „regulii terțului” sau al principiului controlului emitentului privind controlul și răspunderea pentru informațiile din străinătate, criteriile privind îmbunătățirea transparenței, bazate pe principiul general al accesului la informații și pe așa-numitele

„principii Tshwane”[1], precum și principiile privind limitele în ceea ce privește durata și domeniului de aplicare al oricărei supravegheri, care garantează că acestea sunt proporționale și se limitează la scopul lor;

78. invită acest grup să elaboreze un raport în vederea pregătirii conferinței care urmează să fie organizate de Parlament cu organismele naționale de supraveghere, fie parlamentare, fie independente, și să ofere sprijin pentru organizarea acesteia până la începutul anului 2015;

79. invită statele membre să utilizeze bunele practici cu scopul de a ameliora accesul organismelor lor de supraveghere la informații referitoare la activitățile de spionaj (inclusiv la informații clasificate și informații din alte servicii) și de a conferi competența de efectuare a inspecțiilor pe teren, competențe solide de investigare, resurse adecvate și expertiză specializată, independență absolută față de guvernele respective și de a prevede obligația de raportare către parlamentele respective;

80. invită statele membre la dezvoltarea cooperării între organismele de supraveghere, în special în cadrul Rețelei europene a autorităților naționale de supraveghere a serviciilor de informații (ENNIR);

81. îndeamnă ÎR/VP să raporteze periodic cu privire la activitățile Centrului de analiză a informațiilor al UE (IntCen), care face parte din Serviciul European de Acțiune Externă, organismelor responsabile din cadrul Parlamentului, inclusiv cu privire la respectarea deplină a drepturilor fundamentale și a normelor aplicabile ale UE în materie de confidențialitate a datelor, permițând o mai bună supraveghere de către Parlament a dimensiunii externe a politicilor UE; îndeamnă Comisia și ÎR/VP să prezinte o propunere de temei juridic pentru activitățile IntCen, în cazul în care se prevăd eventuale operațiuni sau viitoare competențe în cadrul propriului sistem de informații și de colectare a datelor care pot avea un impact asupra strategiei de securitate internă a Uniunii;

82. solicită Comisiei să prezinte până în decembrie 2014 o propunere referitoare la procedura privind certificatul de securitate al personalului UE, întrucât actualul sistem, care se bazează pe certificatul de securitate acordat de statul membru al resortisantului, prevede diferite cerințe și durate ale procedurilor în cadrul sistemelor naționale, generând tratamente diferite pentru deputații în Parlamentul European și echipa acestora în funcție de naționalitate;

83. reamintește că dispozițiile acordului interinstituțional dintre Parlamentul European și Consiliu privind transmiterea și prelucrarea de către Parlamentul European a informațiilor clasificate deținute de Consiliu în alte chestiuni decât cele vizate de domeniul politicii externe și de securitate comune ar trebui utilizate în vederea ameliorării supravegherii la nivelul UE;

Agențiile UE

84. solicită organismului comun de supraveghere al Europol, alături de autoritățile naționale de protecție a datelor, să realizeze o inspecție comună înainte de finele anului 2014 pentru a verifica dacă informațiile și datele cu caracter personal partajate cu Europol au fost

[1] The Global Principles on National Security and the Right to Information (Principiile globale privind securitatea națională și dreptul la informație), iunie 2013.

obținute în mod legal de către autoritățile naționale, în special dacă informațiile sau datele au fost inițial obținute prin intermediul serviciilor de informații din UE sau dintr-o țară terță, și dacă se aplică măsuri adecvate pentru prevenirea utilizării și diseminării unor astfel de informații sau date; consideră că Europol nu ar trebui să prelucreze informații sau date obținute prin încălcarea drepturilor fundamentale care sunt protejate în temeiul Cartei drepturilor fundamentale;

85. invită Europol să utilizeze pe deplin mandatul său și să solicite autorităților competente din statele membre să inițieze investigații penale privind atacuri și breșe informatice grave cu un eventual impact transfrontalier; consideră că mandatul UE ar trebui îmbunătățit pentru a-i permite să demareze propriile anchete în urma unor atacuri rău intenționate asupra rețelei și a sistemului informatic a două sau mai multe state membre sau organisme ale Uniunii[1]; invită Comisia să revizuiască activitățile Centrului european de combatere a criminalității informatice (EC3) și să prezinte, dacă este necesar, o propunere referitoare la un cadru cuprinzător pentru consolidarea competențelor sale;

Libertatea de exprimare

86. își exprimă profunda îngrijorare în legătură cu amenințările din ce în ce mai numeroase la adresa libertății presei și impactul dur asupra jurnaliștilor a intimidării de către autoritățile publice, în special în ceea ce privește protejarea confidențialității surselor jurnalistice; reiterează solicitările exprimate în Rezoluția sa din 21 mai 2013 referitoare la „Carta UE: norme standard pentru libertatea mass-mediei în UE”;

87. ia act de deținerea lui David Miranda și de confiscarea materialului aflat în posesia sa de către autoritățile Regatului Unit în temeiul secțiunii 7 din Legea privind terorismul din 2000 (precum și cererea către ziarul *The Guardian* de a distruge sau de a preda materialul) și își exprim preocupările privind faptul că aceasta constituie o interferență potențial gravă cu dreptul la libertatea de exprimare și libertatea presei astfel cum este recunoscut de articolul 10 din CEDO și articolul 11 din Carta UE și că acesta ar putea fi un exemplu de utilizare abuzivă a legislației privind combaterea terorismului;

88. atrage atenția cu privire la situația grea a denunțătorilor și a celor care îi sprijină, inclusiv jurnaliștii, ca urmare a dezvăluirilor lor; invită Comisia să examineze măsura în care o viitoare propunere legislativă de instituire a unui program european de protecție eficace și cuprinzătoare a denunțărilor, astfel cum s-a solicitat în rezoluția Parlamentului din 23 octombrie 2013, ar trebui să includă alte domenii de competență ale Uniunii, acordând o atenție deosebită complexității denunțării în domeniul activității de intelligence; solicită statelor membre ale UE să examineze în profunzime posibilitatea acordării de protecție internațională denunțătorilor împotriva urmăririlor în justiție;

89. invită statele membre să se asigure că legislația lor, îndeosebi în domeniul securității naționale, oferă o alternativă sigură la absența divulgării sau raportării delictelor, cum ar fi cazurile de corupție, infracțiunile penale, încălcările obligațiilor juridice, erori judiciare sau abuzul de putere, care respectă dispozițiile diferitelor instrumente internaționale (ale ONU și Consiliului Europei) de combatere a corupției, principiile prevăzute în rezoluția

[1] Poziția Parlamentului European din 25 februarie 2014 referitoare la propunerea de regulament al Parlamentului European și al Consiliului privind Agenția Uniunii Europene pentru cooperare și formare în materie de aplicare a legii (Europol) (Texte adoptate, P7_TA(2014)0121).

APCE din 1729 (2010), principiile Tshwane etc;

Securitatea informatică în UE

90. subliniază că incidentele recente au arătat în mod clar vulnerabilitatea acută a UE și în special a instituțiilor UE, a guvernelor și a parlamentelor naționale, a marilor companii europene, a infrastructurilor și a rețelelor informatice europene, în fața atacurilor sofisticate care folosesc programe informatice complexe și *malware*; remarcă faptul că aceste atacuri necesită resurse financiare și umane de o asemenea amploare încât cel mai probabil ele pornesc de la entități publice care acționează în numele guvernelor străine; în acest context, consideră cazul pirateriei sau intruziunii în compania de telecomunicații Belgacom ca fiind un exemplu îngrijorător al unui atac asupra capacității informatice a UE; subliniază că îmbunătățirea capacității și securității IT a UE reduce, de asemenea, vulnerabilitatea UE în fața unor atacuri informatice grave comise de organizații criminale majore sau de grupări teroriste;

91. este de părere că dezvăluirile privind supravegherea în masă care au declanșat această criză pot fi folosite ca o oportunitate pentru ca Europa să ia inițiativa de a construi, ca măsură strategică prioritară, o capacitate informatică cheie autonomă și puternică; subliniază faptul că, pentru a câștiga încrederea, o astfel de capacitate informatică europeană ar trebui să se bazeze, în măsura în care acest lucru este posibil, pe standarde deschise și pe software și, dacă este posibil, hardware cu sursă deschisă, care să asigure transparența și examinarea întregului lanț de aprovizionare, de la etapa proiectării procesorului la stratul de aplicații; subliniază faptul că, pentru a recâștiga competitivitatea în sectorul strategic al serviciilor informatice, este necesar să se adopte un nou acord digital și să se depună eforturi comune și la scară largă de către instituțiile UE, statele membre, instituțiile de cercetare, industrie și societatea civilă; invită Comisia și statele membre să utilizeze achizițiile publice ca o pârghie de a sprijini această capacitate de resurse din UE, făcând din standardele privind securitatea și viața privată o cerință cheie în achizițiile publice de bunuri și servicii informatice; prin urmare, îndeamnă Comisia să revizuiască practicile actuale privind achizițiile publice în ceea ce privește achizițiile publice bazate pe date pentru a putea limita achizițiile publice doar la întreprinderile certificate și, eventual, doar la întreprinderile din UE în cazul în care sunt vizate interese de securitate sau interese esențiale;

92. condamnă cu fermitate faptul că serviciile de informații străine au încercat să reducă standardele de securitate informatică și să instaleze aplicații „*backdoor*” într-un mare număr de sisteme informatice; solicită Comisiei să prezinte un proiect legislativ pentru a interzice utilizarea instrumentelor „*backdoor*” de către autoritățile de aplicare a legii; în consecință, recomandă utilizarea programelor informatice cu sursă deschisă în toate mediile în care securitate informatică reprezintă o preocupare;

93. solicită tuturor statelor membre, Comisiei, Consiliului și Consiliului European să sprijine pe deplin, inclusiv prin finanțarea în domeniul cercetării și dezvoltării, dezvoltarea de capacități inovatoare și tehnologice la nivel european în termeni de instrumente informatice, companii și furnizori de servicii IT (hardware, software, servicii și rețele), inclusiv în scopul asigurării securității cibernetice, precum și de capacități de codare și criptare; invită toate instituțiile responsabile din UE și din statele membre să investească în tehnologiile locale și independente ale UE, precum și să dezvolte masiv și să mărească capabilitățile de detectare;

94. solicită Comisiei, organismelor de standardizare și Agenției europene pentru securitatea rețelelor și a informațiilor (ENISA) să elaboreze, până în decembrie 2014, standarde minime de securitate și confidențialitate și orientări generale pentru sistemele informatice, rețele și servicii, inclusiv serviciile de tip cloud, pentru a proteja mai bine datele cu caracter personal ale cetățenilor UE, precum și integritatea tuturor sistemelor informatice; consideră că asemenea standarde ar trebui să devină criterii de referință pentru noi standarde mondiale și ar trebui să fie stabilite printr-un proces deschis și democratic, care să nu fie condus de o singură țară, entitate sau întreprindere multinațională; este de părere că îngrijorărilor legitime privind aplicarea legii și activitățile de spionaj de care trebuie să se țină cont pentru a sprijini lupta împotriva terorismului nu trebuie să conducă la o subminare generală a fiabilității sistemelor informatice; își exprimă sprijinul pentru recentele decizii luate de Internet Engineering Task Force (IETF) de a include guvernele în modelul de amenințare la adresa securității pe internet;

95. subliniază faptul că autoritățile de reglementare a telecomunicațiilor din UE și de la nivel național și, în anumite cazuri și companiile de telecomunicații, au neglijat în mod evident securitatea informatică a utilizatorilor și clienților lor; invită Comisia să utilizeze din plin atribuțiile de care dispune în temeiul Directivei-cadru asupra confidențialității și comunicațiilor electronice pentru a consolida protecția confidențialității comunicațiilor prin adoptarea de măsuri care să asigure că echipamentul terminal este compatibil cu dreptul utilizatorilor de a controla și de a proteja datele lor cu caracter personal, și care să asigure un nivel ridicat de securitate a rețelelor și serviciilor de telecomunicații, inclusiv prin impunerea unei criptări end-to-end de ultimă generație a comunicațiilor;

96. sprijină strategia informatică a UE, însă consideră că aceasta nu acoperă toate amenințările posibile și că ar trebui lărgită pentru a include comportamentele ostile ale statelor; subliniază necesitatea unei securități informatice mai solide și a rezilienței sistemelor informatice;

97. invită Comisia să prezinte până cel târziu în ianuarie 2015, un plan de acțiune pentru consolidarea independenței informatice a UE, inclusiv o abordare mai coerentă a capacităților tehnologice în dezvoltare din domeniul IT la nivelul UE (inclusiv sisteme informatice, echipamente, servicii, cloud computing, programe de criptare și anonimizare) și a protecției infrastructurilor informatice critice (inclusiv în termeni de proprietate și vulnerabilitate);

98. invită Comisia, în cadrul viitorului program de lucru al programului Orizont 2020, să aloce mai multe resurse pentru stimularea la nivel european a cercetării, dezvoltării, inovării și formării din domeniul tehnologiilor IT, în special tehnologiile și infrastructurile de consolidare a confidențialității, criptologia, securitatea informatică, cele mai bune soluții de securitate posibile, inclusiv soluții de securitate open-spurce și alte servicii ale societății informaționale, promovând piața internă a produselor software și hardware europene, precum și mijloace de comunicare și infrastructuri de comunicații criptate, inclusiv prin dezvoltarea unei strategii industriale europene pentru industria informatică; consideră că întreprinderile mici și mijlocii dețin un rol special în domeniul cercetării; subliniază faptul că UE nu ar trebui să aloce fonduri proiectelor care au drept unic scop dezvoltarea de instrumente de acces ilegal la sisteme informatice;

99. solicită Comisiei să traseze actualele responsabilități și să revizuiască până cel târziu în decembrie 2014 nevoia unui mandat mai amplu, o mai bună coordonare și/sau resurse

suplimentare și capacități tehnice în ceea ce privește ENISA, Centrul european de combatere a criminalității informatice al Europol și alte centre de expertiză specializată ale Uniunii, centrul de răspuns la incidente de securitate cibernetică (CERT-UE) și Autoritatea Europeană pentru Protecția Datelor (AEPD), astfel încât acestea să poată juca un rol-cheie în asigurarea securității sistemelor de comunicații europene și să fie mai eficiente în prevenirea și investigarea unor breșe informatice grave în UE și să realizeze (sau să ajute statele membre și organismele UE să realizeze) investigații tehnice pe teren în cazul breșelor informatice importante; solicită Comisiei, în special, să aibă în vedere consolidarea rolul ENISA în apărarea sistemelor interne din cadrul instituțiilor UE și înființarea în cadrul structurii ENISA a unei echipe de intervenție în caz de urgență informatică (CERT) pentru UE și statele sale membre;

100. solicită Comisiei să evalueze eventuala necesitate a unei Academii IT a UE care să reunească cei mai buni experți europeni și internaționali independenți din toate domeniile conexe, care să aibă sarcina de a oferi tuturor instituțiilor și organismelor relevante ale UE consiliere științifică privind tehnologiile din domeniul IT, inclusiv strategiile privind securitatea;

101. invită serviciile competente ale Secretariatului Parlamentului European, sub responsabilitatea Președintelui Parlamentului, să efectueze, până cel târziu în iunie 2015, împreună cu un raport intermediar până cel târziu în decembrie 2014, o analiză și o evaluare amănunțite a fiabilității securității informatice a Parlamentului European, care să pună accent pe: mijloace bugetare, resurse umane, capacități tehnice, organizare internă și toate elementele relevante, pentru a obține un nivel ridicat de securitate al sistemelor informatice ale Parlamentului; consideră că o astfel de evaluare trebuie să furnizeze cel puțin o analiză a informațiilor și recomandări referitoare la:

– nevoia unor audituri de securitate regulate, riguroase și independente și de teste de penetrare, cu experți aleși din afara PE asigurând astfel transparența și garantând credibilitatea lor față de țări terțe sau orice alte tipuri de interese legitime;

– includerea în cererile de oferte privind noile sisteme IT a unor bune practici specifice legate de securitatea/confidențialitatea IT, inclusiv posibilitatea unei cerințe referitoare la programe informatice cu sursă deschisă ca o condiție de achiziție sau cerința ca întreprinderile europene de încredere să participe la cererile de oferte atunci când sunt implicate domenii sensibile, legate de securitate;

– lista întreprinderilor care au contract cu Parlamentul European în domeniile IT și al telecomunicațiilor, având în vedere orice informații dezvăluite cu privire la cooperarea acestora cu serviciile de informații (precum dezvăluirile despre contractele NSA cu companii precum RSA, ale cărei produse sunt folosite de Parlamentul European pentru a presupusa protecție a accesului la distanță la datele lor a deputaților în Parlamentul European și a personalului său), inclusiv posibilitatea ca aceleași servicii să fie furnizate de către alte întreprinderi, de preferat europene;

– fiabilitatea și soliditatea programelor informatice, îndeosebi a sistemelor comerciale concepute la comandă, utilizate de instituțiile UE în sistemele lor informatice cu privire la penetrările și intruziunile autorităților de aplicare a legii sau ale serviciilor de informații din UE sau țări terțe, ținând seama de standardele internaționale relevante, de principiile legate de bunele practici în materie de gestionare a

riscurilor de securitate și aderarea la standardele UE de securitate a rețelelor de informații în ceea ce privește breșele de securitate;

– utilizarea mai multor sisteme open-source;

– pași și măsuri de luat pentru a aborda folosirea sporită a instrumentelor mobile (smartphone, tablete, profesionale sau personale) și efectele acestora asupra securității informatice a sistemului;

– securitatea comunicațiilor între diferite locuri de desfășurare a activității Parlamentului și a sistemelor informatice utilizate în cadrul Parlamentului ;

– folosirea și locația serverelor și a centrelor informatice pentru sistemele IT ale Parlamentului și implicațiile asupra securității și integrității respectivelor sisteme;

– punerea efectivă în aplicare a normelor existente privind breșele de securitate și notificarea promptă a autorităților competente de către furnizorii IT în legătură cu rețele de telecomunicații disponibile pentru marele public;

– utilizarea tehnologiilor de tip *cloud computing* și a serviciilor de stocare de către Parlament, inclusiv natura datelor stocate în *cloud*, modul în care sunt protejate conținutul și accesul la *cloud* și locul unde este situat *cloudul*, clarificând cadrul juridic aplicabil privind protecția datelor și informațiile, precum și evaluând posibilitățile utilizării exclusive a serverelor de *cloud* situate pe teritoriul UE;

– un plan care să permită folosirea sporită a unor tehnologii criptografice, în special criptarea de tip autentificare *end-to-end* pentru toate serviciile IT și de comunicații, ca de exemplu *cloud computing*, e-mail, mesageria instant și telefonia;

– folosirea semnăturilor electronice în e-mail;

– un plan pentru utilizarea unui standard de criptare din oficiu, precum GNU Privacy Guard, pentru e-mailuri care ar permite în același timp utilizarea semnăturilor digitale;

– posibilitatea de a institui un serviciu sigur de mesagerie instant în cadrul Parlamentului, care să permită o comunicare sigură, păstrând pe servere doar conținutul criptat;

102. invită toate instituțiile și agențiile UE, în special Consiliul European, Consiliul, Serviciul European de Acțiune Externă (inclusiv delegațiile UE), Comisia, Curtea de Justiție și Banca Centrală Europeană, să realizeze o evaluare similară în cooperare cu ENISA, Europol și centrele CERT, până cel târziu în iunie 2015, împreună cu un raport intermediar până în decembrie 2014; invită statele membre să efectueze evaluări similare;

103. subliniază faptul că, în ceea ce privește acțiunea externă a UE, ar trebui efectuate evaluări ale nevoilor bugetare aferente și ar trebui adoptate fără întârziere primele măsuri cu privire la Serviciul European de Acțiune Externă (SEAE), precum și că trebuie alocate fondurile adecvate în proiectul de buget pentru 2015;

104. este de părere că sistemele IT la scară mare utilizate în spațiul de libertate, securitate și justiție, cum ar fi Sistemul de Informații Schengen II, Sistemul de informații privind

vizele, Eurodac şi eventuale sisteme viitoare, precum UE-ESTA, ar trebui să fie dezvoltate şi gestionate astfel încât să asigure că datele nu sunt compromise ca urmare a cererilor autorităţilor din ţările terţe; solicită agenţiei eu-LISA să informeze Parlamentul cu privire la fiabilitatea sistemelor în vigoare până la finele anului 2014;

105. solicită Comisiei şi SEAE să ia măsuri la nivel internaţional, în special în colaborare cu ONU şi, în cooperare cu parteneri interesaţi, să pună în aplicare o strategie UE pentru o guvernanţă democratică a internetului în vederea prevenirii unei influenţe abuzive asupra activităţilor ICANN şi IANA din partea unor entităţi, companii sau state individuale prin asigurarea unei reprezentări adecvate a tuturor părţilor interesate în cadrul acestor organisme, evitând, totodată, facilitarea controlului sau a cenzurii de stat ori balcanizarea şi fragmentarea internetului;

106. solicită UE să îşi asume rolul de lider în remodelarea arhitecturii şi guvernanţei internetului, în vederea abordării riscurilor referitoare la fluxurile de date şi la stocarea acestora, urmărind minimizarea datelor, o transparenţă sporită şi mai puţine depozite centralizate de date brute, precum şi redirecţionarea traficului de internet sau criptarea deplină end-to-end a întregului trafic de internet, astfel încât să se evite riscurile asociate în prezent cu rutarea traficului pe teritoriul ţărilor care nu respectă standardele de bază privind drepturile fundamentale, protecţia datelor şi viaţa privată;

107. solicită promovarea:

- motoarelor de căutare şi a reţelelor sociale din UE, ca pas important în direcţia independenţei informatice a UE;

- furnizorilor europeni de servicii informatice;

- criptării comunicaţiilor, în general, inclusiv a comunicaţiilor prin e-mail şi prin SMS;

- elementelor europene esenţiale din punct de vedere informatic, de exemplu, a soluţiilor pentru sistemele de operare bazate pe modelul client-server, a utilizării standardelor cu sursă deschisă, a dezvoltării de elemente europene pentru conectarea la reţea, cum ar fi routerele;

108. invită Comisia să prezinte o propunere legislativă pentru un sistem UE de rutare, incluzând procesarea registrului detaliat al comunicaţiilor (CDR) la nivelul UE, sistem care va fi o substructură a internetului existent şi nu va depăşi graniţele UE; observă faptul că toate datele privind rutarea şi CDR ar trebui prelucrate în conformitate cu cadrele legislative ale UE;

109. invită statele membre ca, în cooperare cu ENISA, Centrul european de combatere a infracţiunilor informatice al Europol, centrele CERT şi autorităţile naţionale de protecţie a datelor, precum şi unităţile de combatere a infracţiunilor informatice, să dezvolte o cultură a securităţii şi să lanseze o campanie de educare şi de sensibilizare care să le dea cetăţenilor posibilitatea să facă alegeri mai informate referitoare la datele personale pe care decid să le publice pe internet şi la protejarea într-o mai mare măsură a acestora, inclusiv prin criptare şi tehnologii de tip *cloud computing* sigure, utilizând la maximum platforma cu informaţii de interes public prevăzută de Directiva privind serviciile universale;

110. solicită Comisiei ca, până în decembrie 2014, să prezinte propuneri legislative de încurajare a producătorilor de programe și echipamente informatice să introducă în cadrul produselor lor mai multe elemente de securitate și de luare în considerare a vieții private începând cu momentul conceperii, precum și caracteristici implicite, inclusiv prin aplicarea unor factori de descurajare a colectării în masă, abuzive și disproporționate a datelor cu caracter personal și prin introducerea responsabilității juridice a producătorilor cu privire la puncte slabe cunoscute, dar neremediate, produse defecte sau nesigure sau instalarea unor uși secrete (*backdoors*) care permit accesul neautorizat la date și prelucrarea neautorizată a acestora; în acest sens, invită Comisia să evalueze posibilitatea instituirii unui sistem de certificare sau de validare a echipamentelor informatice, inclusiv a unor proceduri de testare la nivelul UE pentru a asigura integritatea și securitatea produselor;

Reconstruirea încrederii

111. consideră că, dincolo de necesitatea unei schimbări legislative, ancheta a arătat că SUA are nevoie să restaureze încrederea partenerilor săi din UE, întrucât activitățile serviciilor sale de informații sunt în primul rând în joc;

112. subliniază că această criza de încredere se referă la:

- spiritul de cooperare din cadrul UE, întrucât unele activități ale serviciilor de informații pot periclita atingerea obiectivelor Uniunii;

- cetățeni, care și-au dat seama că nu numai țările terțe sau companiile multinaționale, ci și propriul lor guvern pot să îi spioneze;

- respectarea drepturilor fundamentale, a democrației și a statului de drept, precum și credibilitatea unor garanții și a supravegherii democratice, judiciare și parlamentare într-o societate digitală;

Între UE și SUA

113. reamintește importantul parteneriat istoric și strategic dintre statele membre ale UE și SUA, bazat pe o credință comună în democrație, statul de drept și drepturile fundamentale;

114. consideră că supravegherea în masă a cetățenilor și spionarea liderilor politici de către SUA au produs daune majore la nivelul relațiilor dintre UE și SUA și au avut un impact negativ asupra încrederii în organizațiile SUA care acționează în UE; această situație este agravată și mai mult de lipsa unor căi de atac judiciare și administrative prevăzute de legislația SUA pentru cetățenii UE, îndeosebi în cazul activităților de supraveghere derulate în scopul colectării de date;

115. recunoaște faptul că, în contextul provocărilor mondiale cu care se confruntă UE și SUA, parteneriatul transatlantic trebuie să fie consolidat în continuare și că este esențială continuarea cooperării transatlantice în domeniul combaterii terorismului pe o nouă bază de încredere fundamentată pe respectul comun efectiv al statului de drept și respingerea tuturor practicilor arbitrare de supraveghere în masă; insistă, prin urmare, asupra faptului că trebuie luate măsuri clare de către SUA pentru restabilirea încrederii și accentuarea valorilor comune fundamentale pe care se bazează parteneriatul;

116. este pregătit să se angajeze într-un dialog cu omologii săi din SUA astfel încât, în cadrul dezbaterii americane în curs de desfășurare de la nivel public și din cadrul Congresului cu privire la reformarea supravegherii și la revizuirea controlului serviciilor de informații, să se garanteze dreptul la viață privată și alte drepturi ale cetățenilor și rezidenților UE sau ale altor persoane protejate de legislația UE, precum și drepturi egale la informare și protecția confidențialității în fața tribunalelor americane, inclusiv accesul la justiție, prin, de exemplu, revizuirea Legii privind protecția vieții private (*Privacy Act)* și a Legii privind confidențialitatea comunicațiilor electronice (*Electronic Communications Privacy Act*) și ratificarea primului Protocol opțional la Pactul internațional cu privire la drepturile civile și politice (PIDCP), astfel încât să se evite perpetuarea actualei discriminări;

117. insistă asupra demarării reformelor necesare și a instituirii unor garanții reale pentru cetățenii europeni cu scopul de a asigura că folosirea supravegherii și a prelucrării de date în scopuri de spionaj străin este proporțională, se limitează la condiții clar specificate și se bazează pe o suspiciune rezonabilă sau o cauză probabilă a unei activități teroriste; subliniază că acest obiectiv trebuie să facă obiectul unui control judiciar transparent;

118. consideră că este nevoie de semnale politice clare de la partenerii noștri americani pentru a demonstra că SUA face diferența între aliați și adversari;

119. îndeamnă Comisia Europeană și administrația SUA să abordeze, în contextul negocierilor în curs de desfășurare referitoare la acordul-cadru UE-SUA privind transferul de date în scopuri de aplicare a legii, drepturile la informare și la căi de atac judiciare ale cetățenilor UE și să încheie aceste negocieri, în conformitate cu angajamentul luat în cadrul reuniunii ministeriale în materie de justiție și afaceri interne dintre UE și SUA din 18 noiembrie 2013, înainte de vara anului 2014;

120. încurajează SUA să adere la Convenția Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (Convenția 108), având în vedere că a aderat la Convenția privind cibercriminalitatea din 2001, consolidând astfel baza juridică comună dintre aliații transatlantici;

121. solicită instituțiilor UE să exploreze posibilitatea de a stabili cu SUA un cod de conduită care să garanteze că SUA nu desfășoară activități de informare împotriva instituțiilor și infrastructurilor UE;

În cadrul Uniunii Europene

122. consideră, de asemenea, că implicarea și activitățile statelor membre ale UE au condus la o pierdere a încrederii, inclusiv între statele membre și între cetățenii UE și autoritățile statelor lor membre; este de părere că încrederea pierdută nu se va putea restabili decât prin clarificarea deplină a scopurilor activităților de supraveghere și a mijloacelor de supraveghere, prin dezbaterea publică și, în cele din urmă, prin revizuirea legislației, inclusiv prin adoptarea de măsuri menite să pună capăt activităților de supraveghere în masă și să consolideze sistemul de control judiciar și parlamentar; reiterează faptul că, din cauza acestor activități de supraveghere în masă, este dificil să se dezvolte politici de securitate cuprinzătoare ale UE și subliniază faptul că principiul UE de cooperare sinceră solicită statelor membre să se abțină de la desfășurarea de activități de intelligence pe teritoriul altor state membre;

123. ia act de faptul că anumite state membre continuă discuțiile bilaterale cu autoritățile SUA

pe tema acuzațiilor de spionaj și că unele state membre au încheiat (Regatul Unit) sau prevăd încheierea (Germania, Franța) așa-numitelor „acorduri anti-spionaj”; subliniază că aceste state membre trebuie să respecte pe deplin cadrul legislativ și interesele UE în ansamblul său; consideră că, dată fiind nevoia unei abordări europene pentru această problemă, acordurile bilaterale menționate sunt contraproductive și irelevante; solicită Consiliului să informeze Parlamentul cu privire la progresele statelor membre în legătură cu un acord reciproc anti-spionaj la nivelul UE;

124. consideră că astfel de acorduri nu ar trebui să încalce tratatele Uniunii, în special principiul cooperării sincere [în temeiul articolului 4 alineatul (3) din TUE] și nici să submineze politicile UE în general și, în special, cele referitoare la piața internă, concurență loială și dezvoltarea economică, industrială și socială; decide să reexamineze orice astfel de acorduri pentru a analiza compatibilitatea lor cu dreptul european și își rezervă dreptul de a invoca procedurile tratatului în cazul în care astfel de acorduri se dovedesc a fi contrare coeziunii Uniunii sau principiilor fundamentale care stau la baza ei;

125. invită statele membre să depună toate eforturile posibile pentru a asigura o mai bună cooperare în vederea furnizării de garanții împotriva spionajului, în colaborare cu organismele și agențiile relevante ale UE, pentru protejarea cetățenilor și instituțiilor UE, a întreprinderilor europene, a industriei și a infrastructurii și rețelelor informatice ale UE, precum și a cercetării europene; consideră că implicarea activă a părților interesate ale UE constituie o condiție prealabilă pentru un schimb de informații eficace; subliniază că amenințările la adresa securității au un caracter internațional mai pronunțat, sunt mai difuze și mai complexe, motiv pentru care este nevoie de o cooperare sporită la nivel european; consideră că aceste evoluții ar trebui să se reflecte într-o mai mare măsură în tratate și, prin urmare, solicită revizuirea tratatelor în vederea consolidării noțiunii de cooperare sinceră între statele membre și Uniune în ceea ce privește obiectivul de a realiza o zonă de securitate și de a preveni spionajul reciproc între statele membre ale UE;

126. consideră că structurile de comunicații securizate împotriva interceptărilor (e-mail și telecomunicații, inclusiv rețele fixe și telefoane mobile) și sălile de reuniune securizate împotriva interceptărilor în cadrul tuturor instituțiilor și delegațiilor UE relevante sunt absolut necesare; prin urmare, solicită crearea unui sistem de e-mail intern criptat al UE;

127. invită Consiliul și Comisia să își exprime fără întârziere acordul privind propunerea de Regulament al Parlamentului European privind modalitățile detaliate de exercitare a dreptului de anchetă al Parlamentului European și de abrogare a Deciziei 95/167/CE, Euratom, ECSC a Parlamentului European, Consiliului și Comisiei, adoptată de Parlament la 23 mai 2012 și prezentată în temeiul articolului 226 din TFUE; solicită revizuirea tratatului în vederea extinderii acestor competențe de anchetă pentru a include, fără restricții sau excepții, toate domeniile de competență sau activitate ale Uniunii, precum și posibilitatea de audiere sub jurământ;

La nivel internațional

128. solicită Comisiei să prezinte, până cel târziu în ianuarie 2015, o strategie a UE privind guvernanța democratică a internetului;

129. solicită statelor membre să răspundă invitației la cea de a 35-a Conferință internațională a comisarilor pentru protecția datelor și a vieții private „pentru a sprijini adoptarea unui protocol adițional la articolul 17 din Pactul internațional cu privire la drepturile civile și

politice (PIDCP), care ar trebui să se bazeze pe standardele elaborate și adoptate de Conferința internațională și pe dispozițiile din Comentariul general nr. 16 al Comitetului pentru Drepturile Omului anexat la convenție în vederea creării unor standarde aplicabile la nivel mondial în materie de protecție a datelor și a vieții private în conformitate cu statul de drept”; invită statele membre să includă în acest exercițiu o solicitare de înființare a unei agenții internaționale a ONU care să se ocupe, îndeosebi, de monitorizarea apariției de instrumente de supraveghere și de reglementarea și investigarea utilizării acestora; solicită Înaltului Reprezentant/Vicepreședintelui Comisiei și Serviciului European de Acțiune Externă să adopte o poziție proactivă;

130. invită statele membre să dezvolte o strategie coerentă și fermă în cadrul ONU, de sprijinire îndeosebi a rezoluției privind „dreptul la viață privată în era digitală”, inițiate de Brazilia și Germania, astfel cum a fost adoptată de Comisia a III-a a Adunării generale a ONU (Comitetul pentru Drepturile Omului) la 27 noiembrie 2013, precum și să adopte în continuare acțiuni pentru protejarea dreptului fundamental la viață privată și la protejarea datelor la nivel internațional, evitând totodată facilitarea controlului sau a cenzurii de stat ori fragmentarea internetului, printre care o inițiativă privind un tratat internațional de interzicere a activităților de supraveghere în masă, precum și înființarea unei agenții de control al acestuia;

Planul de priorități: Un habeas corpus digital european - protejarea drepturilor fundamentale în era digitală

131. hotărăște să prezinte cetățenilor și instituțiilor UE, precum și statelor membre, recomandările enumerate anterior sub forma unui Plan de priorități pentru viitoarea legislatură; invită Comisia și celelalte instituții, organisme, oficii și agenții ale UE menționate în prezenta rezoluție, în conformitate cu articolul 265 din TFUE, să dea curs recomandărilor și solicitărilor din prezenta rezoluție;

132. hotărăște să lanseze „Un *habeas corpus* digital european - protejarea drepturilor fundamentale în era digitală” care include următoarele opt acțiuni și a cărui punere în aplicare va asigura:

– Acțiunea 1: adoptarea pachetului de măsuri privind protecția datelor în 2014;

– Acțiunea 2: încheierea acordului-cadru între UE și SUA care să garanteze dreptul fundamental al cetățenilor la viață privată și la protecția datelor și să asigure căi de atac adecvate pentru cetățenii UE, inclusiv în cazuri de transfer de date din UE în SUA în scopuri de aplicare a legii;

– Acțiunea 3: suspendarea „sferei de siguranță” până la finalizarea unei analize complete și remedierea actualelor lacune, asigurându-se că transferurile de date cu caracter personal în scopuri comerciale din Uniune în SUA pot fi efectuate doar în conformitate cu cele mai ridicate standarde ale UE;

– Acțiunea 4: suspendarea acordului TFTP (Programul de urmărire a finanțărilor în scopuri teroriste) până la (i) finalizarea negocierilor privind acordul-cadru; (ii) finalizarea unei investigații detaliate bazate pe o analiză a UE și abordarea adecvată a tuturor preocupărilor menționate de Parlament în Rezoluția sa din 23 octombrie 2013;

– Acțiunea 5: evaluarea oricărui acord, mecanism sau schimb cu țări terțe care implică date cu caracter personal, cu scopul de a se asigura că dreptul la viață privată și la protecția datelor cu caracter personal nu este încălcat ca urmare a activităților de supraveghere, precum și luarea măsurilor de monitorizare necesare;

– Acțiunea 6: protejarea statului de drept și a drepturilor fundamentale ale cetățenilor UE (inclusiv împotriva amenințărilor la adresa libertății presei), a dreptului publicului de a primi informații imparțiale și a confidențialității profesionale (inclusiv în relația avocat-client), precum și asigurarea unei protecții sporite a denunțătorilor;

– Acțiunea 7: elaborarea unei strategii europene privind independența informatică sporită (un „Nou acord digital – New Deal”, inclusiv alocarea resurselor adecvate la nivel național și la nivelul UE) pentru dezvoltarea industriei informatice și pentru a permite întreprinderilor europene să exploateze avantajul concurențial al vieții private;

– Acțiunea 8: evoluția UE ca jucător de referință cu privire la guvernanța democratică și neutră a internetului;

133. invită instituțiile UE și statele membre să promoveze *habeas corpusul* digital european care protejează drepturile fundamentale în era digitală; își ia angajamentul de a acționa ca susținător al drepturilor cetățenilor UE, conform următorului calendar de monitorizare a punerii în aplicare:

– aprilie - martie 2015: un grup de monitorizare bazat pe o echipă de anchetă a comisiei LIBE responsabil de monitorizarea oricăror noi dezvăluiri referitoare la mandatul anchetei și controlul punerii în aplicare a acestei rezoluții;

– începând din iulie 2014: un mecanism de supraveghere durabil pentru transferurile de date și căile de atac din cadrul comisiei competente;

– primăvara anului 2014: o solicitare formală adresată Consiliului European de a include „*Habeas corpusul* digital european - protejarea drepturilor fundamentale în era digitală” în orientările care urmează să fie adoptate în temeiul articolului 68 din TFUE;

– toamna anului 2014: un angajament că „*Habeas corpusul* digital european - protejarea drepturilor fundamentale în era digitală” alături de recomandările aferente vor servi ca un criteriu-cheie pentru aprobarea următoarei Comisii;

– 2014: o conferință care să reunească experți europeni de nivel înalt în diferite domenii care concură la securitatea informatică (inclusiv matematică, criptografie și tehnologiile de consolidare a confidențialității) pentru a ajuta la stimularea unei strategii informatice a UE pentru următoarea legislatură;

– 2014-2015: reunirea regulată unui grup pe tema încredere/date/drepturile cetățenilor între Parlamentul European și Congresul SUA, precum și cu alte parlamente implicate ale țărilor terțe, inclusiv Brazilia;

– 2014-2015: o conferință cu organismele de supraveghere a serviciilor de informații

ale parlamentelor naționale europene;

o

o o

134. încredințează Președintelui sarcina de a transmite prezenta rezoluție Consiliului European, Consiliului, Comisiei, parlamentelor și guvernelor statelor membre, autorităților naționale de protecție a datelor, AEPD, eu-LISA, ENISA, Agenției pentru Drepturi Fundamentale a Uniunii Europene, Grupului de lucru „articolul 29”, Consiliului Europei, Congresului Statelor Unite ale Americii, administrației SUA, președintelui, guvernului și parlamentului Republice Federative a Braziliei și Secretarului General al Organizației Națiunilor Unite;

135. încredințează Comisiei pentru libertăți civile, justiție și afaceri interne sarcina de a sesiza Parlamentul în plen cu privire la această chestiune la un an de la adoptarea prezentei rezoluții; consideră că este esențial să se evalueze măsura în care recomandările adoptate de Parlament au fost urmate și să se analizeze toate cazurile în care nu s-a dat curs acestor recomandări.