|  |  |
| --- | --- |
| Parlamentul European  2014-2019 |  |

**TEXTE ADOPTATE**

P8\_TA(2018)0315

Caracterul adecvat al protecției oferite de Scutul de confidențialitate UE-SUA

PE621.713

Rezoluția Parlamentului European din 5 iulie 2018 referitoare la caracterul adecvat al protecției oferite de Scutul de confidențialitate UE-SUA (2018/2645(RSP))

*Parlamentul European*,

– având în vedere Tratatul privind Uniunea Europeană (TUE), Tratatul privind funcționarea Uniunii Europene (TFUE) și articolele 6, 7, 8, 11, 16, 47 și 52 din Carta drepturilor fundamentale a Uniunii Europene (Carta UE),

– având în vedere Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor)[[1]](#footnote-1) (RGPD) și Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului[[2]](#footnote-2),

– având în vedere hotărârea Curții de Justiție a Uniunii Europene din 6 octombrie 2015, pronunțată în cauza C-362/14 *Maximillian Schrems/Comisarul pentru protecția datelor*[[3]](#footnote-3),

– având în vedere Hotărârea Curții Europene de Justiție din 21 decembrie 2016 pronunțată în cauzele C-203/15 *Tele2 Sverige AB/Post- och telestyrelsen și* C-698/15 *Secretary of State for the Home Department/Tom Watson și alții,* [[4]](#footnote-4),

– având în vedere Decizia de punere în aplicare a Comisiei (UE) 2016/1250 din 12 iulie 2016 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind caracterul adecvat al protecției oferite de Scutul de confidențialitate UE-SUA[[5]](#footnote-5),

– având în vedere avizul 4/2016 al Autorității Europene pentru Protecția Datelor (AEPD) din 30 mai 2016 referitor la proiectul de decizie privind caracterul adecvat al Scutului de confidențialitate UE-SUA[[6]](#footnote-6),

– având în vedere avizul 01/2016 al Grupului de lucru pentru protecția datelor „Articolul 29” (Grupul de lucru „Articolul 29”), din 13 aprilie 2016, referitor la proiectul de decizie privind caracterul adecvat al Scutului de confidențialitate UE-SUA[[7]](#footnote-7) și declarația Grupului de lucru „Articolul 29” din 26 iulie 2016[[8]](#footnote-8),

– având în vedere Raportul Comisiei din 18 octombrie 2017 către Parlamentul European și Consiliu privind prima evaluare anuală privind funcționarea Scutului de confidențialitate (COM(2017)0611) și documentul de lucru al serviciilor Comisiei care însoțește documentul (SWD(2017)0344),

– având în vedere documentul din 28 noiembrie 2017 al Grupului de lucru „Articolul 29”, intitulat „Scutul de confidențialitate UE-SUA - Prima revizuire comună anuală ”[[9]](#footnote-9),

– având în vedere scrisoarea de răspuns a grupului de lucru „Articolul 29” din 11 aprilie 2018 privind reautorizarea secțiunii 702 din Legea privind supravegherea activităților străine de spionaj (FISA) din Statele Unite,

– având în vedere Rezoluția sa din 6 aprilie 2017 referitoare la caracterul adecvat al protecției oferite de Scutul de confidențialitate UE-SUA[[10]](#footnote-10),

– având în vedere articolul 123 alineatul (2) din Regulamentul său de procedură,

A. întrucât Curtea de Justiție a Uniunii Europene (CJUE), în hotărârea sa din 6 octombrie 2015, pronunțată în cauza C-362/14, *Maximillian Schrems v. Comisarul pentru protecția datelor*, a invalidat decizia privind Sfera de siguranță și a clarificat faptul că un nivel adecvat de protecție într-o țară terță trebuie considerat ca fiind „în esență echivalent” cu cel garantat în cadrul Uniunii, în temeiul Directivei 95/46/CE, interpretată în spiritul Cartei UE, subliniind necesitatea de a încheia negocierile privind un nou acord, astfel încât să se asigure securitatea juridică cu privire la modul în care ar trebui transferate datele cu caracter personal din UE către SUA;

B. întrucât, atunci când analizează nivelul de protecție asigurat de o țară terță, Comisia are obligația să evalueze fondul normelor aplicabile în țara în cauză, care emană din legislația sa internă sau din angajamentele sale internaționale, precum și practica stabilită pentru a asigura respectarea normelor în cauză, deoarece trebuie să se țină seama, în conformitate cu articolul 25 alineatul (2) din Directiva 95/46/CE, de toate împrejurările în care are loc transferul unor date cu caracter personal către o țară terță; întrucât evaluarea trebuie să vizeze nu numai legislația și practicile legate de protecția datelor cu caracter personal în scopuri comerciale și private, ci trebuie să includă și toate aspectele cadrului aplicabil țării sau sectorului în cauză, în special, dar nu numai, aplicarea legii, securitatea națională și respectarea drepturilor fundamentale;

C. întrucât transferurile de date cu caracter personal între organizațiile comerciale din UE și SUA sunt un element important al relațiilor transatlantice, având în vedere digitalizarea tot mai mare a economiei mondiale; întrucât aceste transferuri ar trebui efectuate cu respectarea deplină a dreptului la protecția datelor cu caracter personal și a dreptului la viața privată; întrucât unul dintre obiectivele fundamentale ale UE este protecția drepturilor fundamentale, astfel cum este consacrată în Carta UE;

D. întrucât compania Facebook, semnatară a Scutului de confidențialitate, a confirmat că datele a 2,7 milioane de cetățeni ai UE au fost utilizate în mod necorespunzător de către firma de consultanță politică Cambridge Analytica;

E. întrucât, în avizul său nr. 4/2016, AEPD a ridicat o serie de probleme cu privire la proiectul de Scut de confidențialitate; întrucât AEPD salută în același aviz eforturile depuse de toate părțile implicate de a găsi o soluție pentru transferurile de date cu caracter personal din UE către SUA în scopuri comerciale pe baza unui sistem de autocertificare;

F. întrucât, în avizul său 01/2016 referitor la proiectul de decizie de punere în aplicare privind caracterul adecvat al Scutului de confidențialitate UE-SUA, Grupul de lucru „Articolul 29” a salutat îmbunătățirile aduse de Scutul de confidențialitate față de decizia privind Sfera de siguranță, exprimând însă dubii majore atât cu privire la aspectele comerciale, cât și la accesul autorităților publice la datele transferate în cadrul Scutului de confidențialitate;

G. întrucât, la 12 iulie 2016, în urma unor discuții suplimentare cu administrația SUA, Comisia a adoptat Decizia de punere în aplicare (UE) 2016/1250, care declară adecvat nivelul de protecție a datelor cu caracter personal transferate din Uniune către organizații din Statele Unite în cadrul Scutului de confidențialitate UE-SUA;

H. întrucât Scutul de confidențialitate UE-SUA este însoțit de mai multe asigurări și angajamente unilaterale ale administrației SUA, care explică, printre altele, principiile de protecție a datelor, funcționarea supravegherii, a impunerii respectării normelor și a căilor de atac, precum și elementele de protecție și garanție în virtutea cărora agențiile de securitate pot accesa și prelucra datele cu caracter personal;

I. întrucât, în declarația sa din 26 iulie 2016, Grupul de lucru „Articolul 29” a salutat îmbunătățirile aduse de mecanismul Scutului de confidențialitate UE-SUA, în comparație cu cel al Sferei de siguranță, și a felicitat Comisia și autoritățile SUA pentru faptul că au luat în considerare preocupările sale; întrucât, cu toate acestea, Grupul de lucru „Articolul 29” menționează că rămân încă o serie de probleme, atât în ceea ce privește aspectele comerciale, cât și în ceea ce privește accesul autorităților publice din SUA la datele transferate din UE, cum ar fi lipsa unor norme specifice privind deciziile automatizate și absența unui drept general de a ridica obiecții, necesitatea unor garanții mai stricte privind independența și competențele mediatorului sau lipsa unor garanții concrete că nu se vor efectua colectări masive și fără distincție ale datelor personale (colectări în masă);

J. întrucât, în rezoluția sa din 6 aprilie 2017, Parlamentul recunoaște faptul că Scutul de confidențialitate UE-SUA conține îmbunătățiri semnificative în ceea ce privește claritatea standardelor, în comparație cu fosta Sferă de siguranță UE-SUA, dar consideră, în același timp, că rămân încă niște lacune importante în ceea ce privește anumite aspecte comerciale, securitatea națională și asigurarea respectării legii; întrucât solicită Comisiei să efectueze, în cursul primei revizuiri anuale comune, o examinare completă și aprofundată a tuturor lacunelor și deficiențelor și să arate modul în care acestea au fost abordate, astfel încât să se asigure conformitatea cu Carta UE și cu legislația Uniunii, precum și să analizeze atent dacă mecanismele și garanțiile indicate în asigurările și clarificările administrației SUA sunt eficace și fezabile;

K. întrucât, deși Raportul Comisiei către Parlament și Consiliu referitor la prima evaluare anuală privind funcționarea Scutului de confidențialitate și documentul de lucru al serviciilor Comisiei care însoțește acest document recunosc că autoritățile americane au instituit structurile și procedurile necesare pentru a asigura funcționarea corectă a Scutului de confidențialitate și concluzionează că Statele Unite continuă să asigure un nivel adecvat de protecție a datelor cu caracter personal transferate în temeiul Scutului de confidențialitate, au adresat însă zece recomandări autorităților SUA pentru a soluționa unele preocupări legate nu numai de sarcinile și activitățile Departamentul Comerțului din SUA, ca administrație responsabilă cu monitorizarea certificării organizațiilor care aderă la Scutul de confidențialitate și a asigurării respectării principiilor, ci și de securitatea națională, cum ar fi reautorizarea secțiunii 702 din FISA, sau de numirea unui mediator permanent și de faptul că membrii Comitetului de supraveghere a vieții private și a libertăților civile (PCLOB) nu sunt încă în funcție;

L. întrucât în avizul Grupului de lucru „Articolul 29” din 28 noiembrie 2017 intitulat „Scutul de confidențialitate UE-SUA - Prima revizuire comună anuală” se recunosc, în urma primei revizuiri comune anuale, progresele înregistrate în ceea ce privește Scutul de confidențialitate în comparație cu decizia, invalidată, privind Sfera de siguranță; întrucât Grupul de lucru „Articolul 29” recunoaște eforturile depuse de către autoritățile din SUA și de către Comisie pentru a pune în aplicare Scutul de confidențialitate;

M. întrucât Grupul de lucru „Articolul 29” a identificat un număr important de probleme nerezolvate îngrijorătoare, atât în ceea ce privește aspectele comerciale, cât și cele legate de accesul autorităților publice din SUA la datele transferate către SUA în temeiul Scutului de confidențialitate (fie în scopuri de asigurare a respectării legii, fie în scopuri de securitate națională), care trebuie să fie abordate atât de Comisie, cât și de autoritățile din SUA; întrucât a solicitat crearea imediată a unui plan de acțiune pentru a demonstra că toate aceste preocupări vor fi abordate, cel târziu la cea de a doua revizuire comună;

N. întrucât, în cazul în care nu se abordează preocupările exprimate de Grupul de lucru „Articolul 29” în termenele stabilite, membrii acestuia vor lua măsuri adecvate, inclusiv vor adresa decizia privind caracterul adecvat al Scutului de confidențialitate instanțelor naționale pentru ca acestea să facă o trimitere preliminară la CJUE;

O. întrucât CJUE a fost sesizată cu o acțiune în anulare (cauza T-738/16, *La Quadrature du Net și alții v Comisia*) și o sesizare din partea Înaltei Curți a Irlandei în cauza între comisarul pentru protecția datelor din Irlanda și Facebook Ireland Limited și Maximilian Schrems (cauza *Schrems II*); întrucât în sesizare se constată că are loc, în continuare, o supraveghere în masă și se analizează dacă există o cale de atac eficace în legislația SUA pentru cetățenii UE ale căror date cu caracter personal sunt transferate către Statele Unite;

P. întrucât, la 11 ianuarie 2018, Congresul SUA a reautorizat și modificat secțiunea 702 din FISA pentru șase ani fără a răspunde preocupărilor exprimate în raportul de analiză comună al Comisiei și în avizul Grupului de lucru „Articolul 29”;

Q. întrucât, în cadrul legislației bugetare generale promulgate la 23 martie 2018, Congresul SUA a promulgat *Clarifying Overseas Use of Data (CLOUD) Act*, care facilitează accesul în scopul asigurării respectării legii la conținutul comunicațiilor și la alte date conexe, permițând autorităților de aplicare a legii din SUA să impună producerea datelor transmise în cadrul comunicațiilor, chiar dacă acestea sunt stocate în afara Statelor Unite, și dând anumitor țări străine dreptul să încheie acorduri executive cu SUA pentru a permite prestatorilor de servicii din SUA să răspundă la anumite ordine străine care solicită accesul la datele transmise în cadrul comunicațiilor;

R. întrucât Facebook Inc., Cambridge Analytica și SCL Elections Ltd sunt societăți certificate în cadrul Scutului de confidențialitate și, ca atare, au beneficiat de decizia privind caracterul adecvat ca temei juridic pentru transferul datelor cu caracter personal din Uniunea Europeană către Statele Unite ale Americii și prelucrarea ulterioară a acestora;

S. întrucât, în conformitate cu articolul 45 alineatul (5) din Regulamentul general privind protecția datelor, în cazul în care informațiile disponibile indică faptul că o țară terță nu asigură un nivel de protecție adecvat, Comisia trebuie să abroge, să modifice sau să suspende decizia sa privind caracterul adecvat,

1. subliniază deficiențele persistente ale Scutului de confidențialitate în ceea ce privește respectarea drepturilor fundamentale ale persoanelor vizate; subliniază riscul tot mai mare ca CJUE să invalideze Decizia de punere în aplicare a Comisiei (UE) 2016/1250 privind Scutul de confidențialitate;

2. ia act de existența unor îmbunătățiri în comparație cu acordul privind Sfera de siguranță, printre care introducerea unor definiții-cheie, obligații mai stricte legate de păstrarea datelor și transferurile ulterioare către țări terțe, crearea unui mediator pentru a garanta accesul la căi de atac individuale și o supraveghere independentă, un sistem de control și echilibru care să asigure drepturile persoanelor vizate (PCLOB), evaluări de conformitate interne și externe, o documentare și monitorizare mai periodică și mai riguroasă, disponibilitatea mai multor căi de atac, precum și rolul proeminent al autorităților naționale de protecție a datelor în ceea ce privește examinarea plângerilor;

3. reamintește că Grupul de lucru „Articolul 29” a stabilit termenul de 25 mai 2018 pentru soluționarea chestiunile restante, în caz contrar, acesta putând decide să aducă chestiunea Scutului de confidențialitate în fața instanțelor naționale pentru ca acestea să facă o trimitere preliminară la CJUE[[11]](#footnote-11);

***Aspecte instituționale/Numiri***

4. regretă faptul că a durat atât de mult timp pentru a-i desemna pe cei doi membri suplimentari în contextul numirii președintelui PCLOB și îndeamnă Senatul să analizeze profilurile acestora pentru a ratifica desemnarea lor, astfel încât să se restabilească cvorumul agenției independente și să i se permită acesteia să își îndeplinească misiunile de prevenire a terorismului și de protecție a vieții private și a libertăților civile;

5. își exprimă îngrijorarea legată de faptul că lipsa unui președinte și a unui cvorum a limitat capacitatea PCLOB de a acționa și de a-și îndeplini obligațiile; subliniază că, în perioada în care cvorumul nu este atins, PCLOB nu poate iniția noi proiecte de consiliere sau de supraveghere și nu poate angaja personal; reamintește faptul că PCLOB nu a publicat încă raportul său îndelung așteptat privind desfășurarea supravegherii în temeiul Ordinului executiv 12333 și nu a furnizat informații privind funcționarea concretă a acestui ordin executiv și privind necesitatea și proporționalitatea sa în ceea ce privește interferențele la nivelul protecției datelor în acest context; ia act de faptul că acest raport este deosebit de necesar, având în vedere că modul în care Ordinul executiv 12333 este utilizat este incert și imprevizibil; regretă faptul că PCLOB nu a publicat un nou raport privind secțiunea 702 din FISA înainte de a fi fost reautorizată în ianuarie 2018; consideră că absența cvorumului subminează în mod grav garanțiile și asigurările de conformitate și de supraveghere emise de autoritățile din SUA; îndeamnă, așadar, autoritățile din SUA să numească fără întârziere noii membri ai Comitetului și să-i confirme în funcție;

6. având în vedere faptul că Directiva prezidențială nr. 28 (PPD 28) este unul dintre elementele centrale pe care se bazează Scutul de confidențialitate, solicită publicarea raportului PCLOB privind PPD 28, care face, în continuare, obiectul privilegiului prezidențial și, prin urmare, nu a fost încă publicat;

7. își reiterează poziția potrivit căreia mecanismul Ombudsmanului instituit de Departamentul de Stat al SUA nu este suficient de independent și nu este investit cu competențe efective suficiente pentru a-și îndeplini atribuțiile și a oferi căi de atac eficace pentru cetățenii UE; subliniază faptul că trebuie precizate competențele exacte ale mecanismului Ombudsmanului, în special în ceea ce privește competențele sale față de comunitatea serviciilor de informații și eficacitatea reală a căilor de atac împotriva deciziilor sale; regretă faptul că Ombudsmanul poate doar solicita anumite măsuri și informații din partea organismelor guvernamentale ale SUA și nu poate ordona autorităților să înceteze și să pună capăt supravegherii ilegale sau să distrugă definitiv informațiile; subliniază că, deși există un Ombudsman interimar, până în prezent administrația SUA nu a numit încă un nou Ombudsman permanent, ceea ce nu favorizează încrederea reciprocă; consideră că, în absența numirii unui Ombudsman independent, cu experiență și care să dispună de competențe suficiente, garanțiile SUA potrivit cărora cetățenii UE beneficiază de căi de atac eficiente sunt nule și neavenite;

8. ia act de recenta confirmare de către Senat a unui nou președinte și a patru comisari ai Comisiei Federale pentru Comerț (CFC); regretă că până la confirmarea menționată au fost vacante patru din cele cinci mandate din cadrul CFC, având în vedere faptul că CFC este agenția competentă însărcinată cu asigurarea respectării principiilor Scutului de confidențialitate de către organizațiile din SUA;

9. subliniază faptul că dezvăluirile recente privind practicile Facebook și Cambridge Analytica evidențiază necesitatea unor acțiuni proactive de supraveghere și de asigurare a aplicării normelor, care să nu se bazeze doar pe reclamații, ci să prevadă verificări sistematice a conformității practice a politicilor de confidențialitate cu principiile Scutului de confidențialitate pe tot parcursul ciclului de certificare; invită autoritățile UE competente în materie de protecție a datelor să ia măsurile necesare și să suspende transferurile în cazurile de neconformitate;

***Aspecte comerciale***

10. consideră că, în scopul de a asigura transparența și a evita declarațiile de certificare false, Departamentul Comerțului al Statelor Unite nu ar trebui să tolereze societățile americane care fac declarații publice despre certificarea lor în cadrul Scutului de confidențialitate înainte ca acesta să fi finalizat procesul de certificare și să le fi inclus pe lista Scutului de confidențialitate; este preocupat de faptul că Departamentul Comerțului nu a folosit posibilitatea prevăzută în Scutul de confidențialitate de a solicita copii ale clauzelor contractuale utilizate de societățile certificate în cadrul contractelor încheiate cu terți pentru a asigura conformitatea; consideră, prin urmare, că nu există un control eficace al respectării efective a dispozițiilor Scutului de confidențialitate de către societățile certificate; invită Departamentul Comerțului să efectueze în mod proactiv și periodic evaluări de conformitate *ex officio* pentru a monitoriza respectarea efectivă de către societăți a normelor și cerințelor Scutului de confidențialitate;

11. consideră că diversele căi de atac disponibile pentru cetățenii UE s-ar putea dovedi a fi prea complexe, greu de utilizat și, prin urmare, mai puțin eficace; constată că, astfel cum au subliniat societățile care furnizează mecanisme independente de recurs, majoritatea plângerilor sunt prezentate direct întreprinderilor de către persoane care caută informații generale privind Scutul de confidențialitate și prelucrarea datelor lor; recomandă, prin urmare, autorităților SUA să ofere cetățenilor, pe site-ul de internet al Scutului de confidențialitate, informații mai concrete cu privire la drepturile lor și căile de atac disponibile, într-un mod accesibil și ușor de înțeles;

12. având în vedere dezvăluirile recente privind utilizarea abuzivă a datelor cu caracter personal de către întreprinderi certificate în cadrul Scutului de confidențialitate, cum ar fi Facebook și Cambridge Analytica, invită autoritățile SUA însărcinate cu asigurarea respectării Scutului de confidențialitate să adopte fără întârziere măsuri cu privire la astfel de dezvăluiri, în deplină conformitate cu garanțiile și angajamentele oferite de a susține actualul Scut de confidențialitate și, dacă este cazul, să retragă aceste întreprinderi de pe lista Scutului de confidențialitate; de asemenea, solicită autorităților UE competente în materie de protecție a datelor să cerceteze astfel de dezvăluiri și, dacă este cazul, să suspende sau să interzică transferurile de date în temeiul Scutului de confidențialitate; consideră că dezvăluirile demonstrează clar că mecanismul Scutului de confidențialitate nu oferă o protecție adecvată a dreptului la protecția datelor;

13. este deosebit de îngrijorat de schimbarea în ceea ce privește serviciul Facebook pentru utilizatorii din țările terțe din afara Statelor Unite și a Canadei, care până în prezent au beneficiat de drepturi în temeiul legislației UE referitoare la protecția datelor și care sunt obligați acum să accepte ca operator de date Facebook SUA în loc de Facebook Irlanda; consideră că acest lucru reprezintă un transfer de date cu caracter personal a aproximativ 1,5 miliarde de utilizatori către o țară terță; are îndoieli serioase cu privire la faptul că o astfel de limitare la scară largă fără precedent a drepturilor fundamentale ale utilizatorilor unei platforme care este un monopol *de facto* corespunde obiectivului Scutului de confidențialitate; solicită autorităților pentru protecția datelor din UE să cerceteze această chestiune;

14. își exprimă îngrijorarea cu privire la faptul că, dacă această problemă nu este soluționată, utilizarea abuzivă a datelor cu caracter personal de către diferite entități care urmăresc să manipuleze opinia politică sau comportamentul de vot poate amenința procesul democratic și ideea de bază că alegătorii sunt capabili să ia decizii pentru sine în cunoștință de cauză și bazate pe fapte;

15. salută și sprijină invitațiile adresate legislatorului american de a se orienta spre o lege omnibus privind protecția vieții private și a datelor;

16. își reiterează preocupările cu privire la absența unor norme și garanții specifice în Scutul de confidențialitate pentru deciziile bazate pe prelucrarea și crearea automată de profiluri, care produc efecte juridice sau afectează în mod semnificativ persoanele; ia act de intenția Comisiei de a comanda un studiu cu scopul de a colecta dovezi concrete și de a evalua în continuare pertinența procesului decizional automatizat pentru transferurile de date în cadrul Scutului de confidențialitate; invită Comisia să prevadă norme specifice privind procesul decizional automatizat pentru a oferi garanții suficiente, dacă studiul recomandă acest lucru; ia act, în această privință, de informațiile furnizate de revizuirea comună potrivit cărora nu poate avea loc un proces decizional automatizat pe baza datelor cu caracter personal care au fost transferate în cadrul Scutului de confidențialitate; regretă că, potrivit Grupului de lucru „Articolul 29”, reacțiile din partea societăților au rămas foarte generale, rămânând neclar dacă aceste afirmații corespund cu realitatea din toate întreprinderile care aderă la Scutul de confidențialitate; subliniază, de asemenea, aplicabilitatea Regulamentului general privind protecția datelor în condițiile prevăzute la articolul 3 alineatul (2) din RGPD;

17. subliniază că ar trebui aduse îmbunătățiri în ceea ce privește interpretarea și procesarea datelor legate de resursele umane din cauza interpretării diferite a noțiunii de „resurse umane” de către guvernul SUA, pe de o parte, și Comisia și Grupul de lucru „Articolul 29”, pe de altă parte; este pe deplin de acord cu invitația adresată de Grupul de lucru „Articolul 29” Comisiei de a desfășura negocieri cu autoritățile SUA pentru a modifica mecanismul Scutului de confidențialitate cu privire la această chestiune;

18. își reiterează îngrijorarea cu privire la faptul că principiile Scutului de confidențialitate nu urmează modelul UE de prelucrare bazată pe consimțământ, ci permit clauza „opt-out” sau dreptul la opoziție numai în situații foarte specifice; îndeamnă, prin urmare, în lumina revizuirii comune, ca Departamentul Comerțului să colaboreze cu autoritățile europene pentru protecția datelor pentru a oferi orientări mai precise în ceea ce privește principiile esențiale ale Scutului de confidențialitate, cum ar fi principiul opțiunii, principiul notificării, transferurile ulterioare, relația operator-persoană împuternicită de către operator și accesul, care sunt mult mai în concordanță cu drepturile persoanelor vizate în conformitate cu Regulamentul (UE) 2016/679;

19. își reiterează îngrijorarea cu privire la respingerea de către Congres, în martie 2017, a normei prezentate de Comisia federală pentru comunicații referitoare la „Protecția vieții private a clienților serviciilor de bandă largă și ai altor servicii de telecomunicații”, care, în practică, elimină normele referitoare la protecția vieții private în contextul serviciilor de bandă largă, ce ar fi obligat furnizorii de servicii de internet să obțină consimțământul explicit al consumatorilor înainte de vânzarea sau schimbul de date de navigare pe internet și alte informații confidențiale cu agențiile de publicitate și alte întreprinderi; consideră că acest lucru reprezintă o altă amenințare la adresa protecției vieții private în Statele Unite;

***Aspecte legate de asigurarea respectării legii și securitatea națională***

20. consideră că termenul „securitate națională” din mecanismul Scutului de confidențialitate nu este circumscris în mod specific pentru a garanta că încălcările în materie de protecție a datelor pot fi efectiv examinate în instanțe pentru a asigura respectarea unui control strict a ceea ce este necesar și proporțional; solicită, prin urmare, o definiție clară a conceptului de „securitate națională”;

21. ia act de faptul că numărul de obiective în temeiul secțiunii 702 din Legea privind supravegherea activităților străine de spionaj (FISA) a crescut din cauza evoluțiilor tehnologice și ale modelelor de comunicare, precum și a amenințărilor aflate în continuă schimbare;

22. regretă faptul că SUA nu a profitat de oportunitatea oferită de recenta reautorizare a secțiunii 702 din FISA pentru a include garanțiile prevăzute în PPD 28; solicită dovezi și angajamente obligatorii din punct de vedere juridic care să garanteze că colectarea de date în temeiul secțiunii 702 din FISA nu se face fără discernere și că accesul nu este realizat în mod generalizat (colectare în masă), ceea ce este în opoziție cu Carta UE; ia act de explicația Comisiei din documentul de lucru al serviciilor sale potrivit căreia supravegherea în temeiul secțiunii 702 din FISA se bazează întotdeauna pe selectori și, prin urmare, nu permite colectarea în masă; se alătură, așadar, solicitării Grupului de lucru „Articolul 29”care dorește o versiune actualizată a raportului PCLOB referitor la definiția noțiunii de „obiective”, la „sarcina selectorilor” și la procesul concret de aplicare a selectorilor în contextul programului UPSTREAM pentru a preciza și analiza dacă, în acest context, are loc un acces în masă la datele cu caracter personal; regretă că persoanele fizice din UE sunt excluse de la protecția suplimentară oferită de reautorizarea secțiunii 702 din FISA; regretă că reautorizarea secțiunii 702 conține mai multe modificări care sunt numai procedurale și nu abordează aspectele cele mai problematice, astfel cum a observat și Grupul de lucru „Articolul 29”; invită Comisia să trateze cu seriozitate viitoarea analiză a Grupului de lucru „Articolul 29” referitoare la secțiunea 702 din FISA și să acționeze în consecință;

23. afirmă că reautorizarea secțiunii 702 din legea FISA pentru încă șase ani pune sub semnul întrebării legalitatea Scutului de confidențialitate;

24. își reiterează îngrijorarea cu privire la Ordinul executiv 12333, care permite Agenției Naționale de Securitate (NSA) să transmită un volum mare de date cu caracter personal, colectate fără mandat, hotărâre judecătorească sau autorizație a Congresului, altor 16 agenții, inclusiv FBI, Agenția Națională Antidrog și Departamentul pentru Securitate Internă; regretă absența oricărui control jurisdicțional al activităților de supraveghere desfășurate în temeiul Ordinului executiv 12333;

25. subliniază obstacolele persistente în ceea ce privește căile de atac pentru cetățenii din afara SUA, care fac obiectul unei măsuri de supraveghere pe baza secțiunii 702 din FISA sau a Ordinului executiv 12333, din cauza cerințelor procedurale privind calitatea de a exercita acțiunea („standing”), astfel cum sunt interpretate în prezent de instanțele din SUA, pentru a permite cetățenilor din afara SUA să introducă acțiuni în justiție în fața instanțelor din SUA împotriva deciziilor care îi afectează;

26. își exprimă îngrijorarea cu privire la consecințele Ordinului executiv 13768 referitor la „Îmbunătățirea siguranței publice pe teritoriul Statelor Unite” asupra căilor de atac judiciare și administrative disponibile pentru persoanele fizice în SUA, deoarece măsurile de protecție din Legea privind protecția informațiilor cu caracter personal nu se mai aplică pentru cetățenii din afara SUA; ia act de poziția Comisiei potrivit căreia evaluarea adecvării nu se bazează pe măsurile de protecție prevăzute de Legea privind protecția informațiilor cu caracter personal și că, prin urmare, acest Ordin executiv nu afectează Scutul de confidențialitate; consideră că Ordinul executiv 13768 indică totuși intenția guvernului SUA de a anula garanțiile privind protecția datelor acordate anterior pentru cetățenii UE și de a nu ține cont de angajamentele asumate față de UE în cursul președinției Obama;

27. își exprimă profunda îngrijorare cu privire la adoptarea recentă a Legii de clarificare a utilizării legale a datelor în străinătate (Clarifying Lawful Overseas Use of Data Act - CLOUD Act, H.R. 4943), care extinde competențele autorităților americane și străine de aplicare a legii pentru a viza și accesa datele persoanelor dincolo de frontierele internaționale, fără a recurge la instrumentele tratatelor de asistență juridică reciprocă (MLAT), care prevăd garanții adecvate și respectă competențele judiciare ale țărilor în care sunt situate informațiile; subliniază faptul că Legea CLOUD ar putea avea implicații grave pentru UE, deoarece are un domeniu amplu de aplicare și poate crea un conflict cu legislația UE în materie de protecție a datelor;

28. consideră că o soluție mai echilibrată ar fi fost să se consolideze actualul sistem internațional de MLAT, cu scopul de a încuraja cooperarea internațională și judiciară; reiterează că, astfel cum este consacrat în articolul 48 din Regulamentul general privind protecția datelor, asistența juridică reciprocă și alte acorduri internaționale constituie mecanismele privilegiate pentru a permite accesul la date cu caracter personal în străinătate;

29. regretă faptul că autoritățile SUA nu au reușit să își îndeplinească în mod proactiv angajamentul de a furniza Comisiei informații complete și în timp util cu privire la evoluțiile care ar putea fi relevante pentru Scutul de confidențialitate, inclusiv nerespectarea obligației de a notifica Comisiei modificările intervenite în cadrul juridic din SUA, de exemplu, în ceea ce privește Ordinul executiv 13768 al președintelui Trump referitor la „Îmbunătățirea siguranței publice pe teritoriul Statelor Unite” sau abrogarea normelor privind protecția vieții private pentru furnizorii de servicii de internet;

30. reamintește că, astfel cum se menționează în rezoluția sa din 6 aprilie 2017, nici principiile Scutului de confidențialitate, nici scrisorile în care administrația SUA nu oferă precizări și garanții care să demonstreze existența unor drepturi la căi de atac judiciare eficiente pentru persoanele fizice din UE, în contextul utilizării datelor lor cu caracter personal de către autoritățile SUA în scopul aplicării legii și al interesului public, ceea ce a fost subliniat de CJUE în hotărârea sa din 6 octombrie 2015 ca fiind elementul esențial al dreptului fundamental consacrat în articolul 47 din Carta drepturilor fundamentale a UE;

***Concluzii***

31. solicită Comisiei să ia toate măsurile necesare pentru a se asigura că Scutul de confidențialitate va respecta pe deplin Regulamentul (UE) 2016/679, care se aplică începând de la 25 mai 2018, precum și Carta drepturilor fundamentale a UE, astfel încât criteriul de adecvare să nu ducă la lacune sau la avantaje competitive pentru societățile americane;

32. regretă faptul că Comisia și autoritățile americane competente nu au reluat discuțiile privind acordul referitor la Scutul de confidențialitate și nu au instituit niciun plan de acțiune pentru a soluționa cât mai curând posibil problema deficiențelor identificate, astfel cum a solicitat Grupul de lucru „Articolul 29” în raportul său din decembrie referitor la evaluarea comună; invită Comisia și autoritățile SUA competente să facă acest lucru fără întârziere;

33. reamintește că viața privată și protecția datelor reprezintă drepturi fundamentale exercitabile legal consacrate în tratate, în Carta UE și în Convenția europeană a drepturilor omului, precum și în legislație și jurisprudență; subliniază faptul că acestea trebuie să fie aplicate într-un mod care nu împiedică în mod inutil comerțul sau relațiile internaționale, dar nu pot fi comparate cu interesele comerciale sau politice;

34. consideră că actualul Scut de confidențialitate nu furnizează nivelul adecvat de protecție prevăzut de dreptul Uniunii privind protecția datelor și de Carta drepturilor fundamentale a UE, potrivit interpretării CJUE;

35. consideră că, dacă Statele Unite nu respectă pe deplin cerințele până la 1 septembrie 2018, Comisia nu a acționat în conformitate cu articolul 45 alineatul (5) din RGPD; prin urmare, solicită Comisiei să suspende Scutul de confidențialitate până când autoritățile SUA nu respectă termenii acestuia;

36. încredințează Comisiei pentru libertăți civile, justiție și afaceri interne sarcina de a continua să monitorizeze evoluțiile din acest domeniu, inclusiv cu privire la cauzele înaintate CJUE, precum și de a supraveghea acțiunile întreprinse în urma recomandărilor formulate în rezoluție;

o

o o

37. încredințează Președintelui sarcina de a transmite prezenta rezoluție Consiliului, Comisiei, guvernelor și parlamentelor statelor membre și Consiliului Europei.

1. JO L 119, 4.5.2016, p. 1. [↑](#footnote-ref-1)
2. JO L 119, 4.5.2016, p. 89. [↑](#footnote-ref-2)
3. ECLI:EU:C:2015:650. [↑](#footnote-ref-3)
4. ECLI:EU:C:2016:970. [↑](#footnote-ref-4)
5. JO L 207, 1.8.2016, p. 1. [↑](#footnote-ref-5)
6. JO C 257, 15.7.2016, p. 8. [↑](#footnote-ref-6)
7. <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf> [↑](#footnote-ref-7)
8. <http://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf> [↑](#footnote-ref-8)
9. WP 255, disponibil la adresa <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612621> [↑](#footnote-ref-9)
10. Texte adoptate, P8\_TA(2017)0131. [↑](#footnote-ref-10)
11. <https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782> [↑](#footnote-ref-11)