



Bruxelles, 29.2.2016
COM(2016) 117 final

COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU

Fluxuri de date transatlantice: restabilirea încrederii prin garanții puternice

1. INTRODUCERE: ROLUL SCHIMBURILOR DE DATE CU CARACTER PERSONAL ÎN CADRUL RELAȚIILOR UE-SUA

Un parteneriat transatlantic solid între Uniunea Europeană și Statele Unite ale Americii este mai vital ca oricând. Avem aceleași valori, urmărim obiective politice și economice comune și cooperăm strâns în lupta împotriva amenințărilor comune la adresa securității noastre. Forța durabilă a relației noastre este evidențiată de amploarea schimburilor noastre comerciale și de cooperarea strânsă în ceea ce privește chestiunile globale.

Transferul și schimbul de date cu caracter personal reprezintă o componentă esențială care stă la baza legăturilor strânse dintre Uniunea Europeană (UE) și Statele Unite ale Americii (SUA) în domeniul comercial, precum și în sectorul aplicării legii. Aceste schimburi de date necesită un nivel înalt de protecție a datelor și garanții corespunzătoare.

În iunie 2013, o serie de rapoarte privind programele de colectare de informații la scară largă ale SUA au ridicat întrebări serioase, atât la nivelul UE, cât și la nivelul statelor membre, cu privire la impactul asupra drepturilor fundamentale ale cetățenilor europeni al prelucrării pe scară largă a datelor cu caracter personal atât de către autoritățile publice, cât și de întreprinderile private din Statele Unite.

Ca răspuns la acestea, la 27 noiembrie 2013, Comisia a publicat o Comunicare privind restabilirea încrederii în fluxurile de date dintre UE și SUA¹, în care prezenta un plan de acțiune menit să restabilească încrederea în transferurile de date în beneficiul economiei digitale, al protecției drepturilor europenilor și al relației transatlantice în sens mai larg. Comunicarea a stabilit următoarele acțiuni-cheie pentru atingerea acestui obiectiv:

- (i) adoptarea pachetului de reforme privind protecția datelor propus de Comisie în 2012²;
- (ii) consolidarea sferei de siguranță, pe baza celor 13 recomandări prevăzute în Comunicarea privind sfera de siguranță³ și
- (iii) consolidarea garanțiilor în materie de protecție a datelor în ceea ce privește cooperarea în domeniul aplicării legii, în special prin încheierea negocierilor legate de Acordul-cadru

¹ Comunicare a Comisiei către Parlamentul European și Consiliu, Restabilirea încrederii în fluxurile de date dintre UE și SUA, COM(2013) 846 final, 27.11.2013 (denumită în continuare „Comunicarea din 2013” sau „Comunicarea”), disponibilă adresa: http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf.

² Propunerea de Directivă a Parlamentului European și a Consiliului privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și la libera circulație a acestor date, COM(2012) 10 final, 25.1.2012 și Propunerea de Regulament al Parlamentului European și al Consiliului privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal și libera circulație a acestor date (Regulament general privind protecția datelor), COM(2012) 11 final, 25.1.2012, disponibile la adresa: http://ec.europa.eu/justice/data-protection/reform/index_en.htm

³ Comunicare a Comisiei către Parlamentul European și Consiliu privind funcționarea sferei de siguranță din punctul de vedere al cetățenilor UE și al întreprinderilor stabilite în UE, COM(2013) 847 final, 27.11.2013, p. 18-19 (denumită în continuare „Comunicarea privind sfera de siguranță”), disponibilă la adresa: http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf.

UE-SUA privind protecția datelor. Acest acord-cadru cuprindea, de asemenea, obiectivul de a obține angajamente din partea SUA privind drepturile individuale garantate din punct de vedere juridic, inclusiv căi de atac judiciare, în special prin adoptarea unei legi privind căile de atac judiciare care să extindă la cetățenii UE anumite drepturi consacrate în Legea SUA din 1974 privind protecția vieții private, drepturi de care la acea dată beneficiau doar cetățenii și rezidenții permanenți din SUA.

Aceste obiective au fost reafirmate în orientările politice⁴ ale Comisiei Juncker: *„Protecția datelor este un drept fundamental de importanță deosebită în era digitală. Pe lângă finalizarea rapidă a activității legislative privind un set comun de norme în materie de protecție a datelor în Uniunea Europeană, trebuie, de asemenea, să promovăm acest drept în relațiile noastre externe. Având în vedere dezvoltările recente privind supravegherea în masă, partenerii noștri apropiați, precum Statele Unite, trebuie să ne convingă că actualele mecanisme de siguranță sunt cu adevărat sigure, în cazul în care doresc ca acestea să fie menținute. De asemenea, Statele Unite trebuie să garanteze că toți cetățenii UE au dreptul de a introduce o acțiune în instanțele din SUA privind asigurarea respectării drepturilor lor în materie de protecție a datelor, indiferent dacă au sau nu reședința pe teritoriul acestei țări. Acest lucru va fi esențial pentru restabilirea încrederii în relațiile transatlantice.”*

De atunci, Comisia a acționat în direcția atingerii acestor obiective. Comisia a accelerat procesul de negociere privind acordul-cadru, care a fost parafat de către părți la 8 septembrie 2015. Discuțiile interinstituționale având drept subiect pachetul de reforme privind protecția datelor au fost intensificate, astfel încât s-a ajuns la un acord politic între Consiliu și Parlamentul European la 15 decembrie 2015. În ceea ce privește transferurile transatlantice de date în sfera comercială, în ianuarie 2014 Comisia a inițiat dialogul cu SUA pentru a consolida sfera de siguranță. Invalidarea deciziei privind sfera de siguranță de către Curtea de Justiție în Hotărârea Schrems din 6 octombrie 2015⁵ a confirmat necesitatea unui nou cadru și a furnizat orientări suplimentare cu privire la condițiile pe care acesta ar trebui să le îndeplinească. În urma acestei hotărâri, la 6 noiembrie 2015, Comisia a emis orientări pentru întreprinderi, în care prezenta instrumentele alternative care permit continuarea transferului de date cu caracter personal către Statele Unite⁶. La 2 februarie 2016 s-a ajuns la un acord politic privind un nou cadru pentru fluxurile de date transatlantice, Scutul de confidențialitate UE-SUA (*EU-U.S Privacy Shield*)⁷, care să înlocuiască acordurile anterioare.

Aceste realizări vor fi benefice relației transatlantice și ar trebui să redea cetățenilor europeni încrederea în economia digitală și să consolideze, în același timp, drepturile fundamentale ale

⁴ Un nou început pentru Europa: Agenda mea pentru locuri de muncă, creștere, echitate și schimbări democratice. Orientări politice pentru viitoarea Comisie Europeană.

⁵ Hotărârea din 6 octombrie 2015 în cauza C-362/14 Maximilian Schrems/Data Protection Commissioner, EU:C:2015:650.

⁶ A se vedea Comunicarea Comisiei către Parlamentul European și Consiliu privind transferul datelor cu caracter personal dinspre UE către Statele Unite ale Americii în temeiul Directivei 95/46/CE în urma hotărârii pronunțate de Curtea de Justiție în cauza C-362/14 (Schrems), COM(2015) 566 final, 6.11.2015. A se vedea, de asemenea, declarația Grupului de lucru „articolul 29” privind consecințele hotărârii Schrems din 3 februarie 2016, disponibilă la adresa: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgment_en.pdf

⁷ A se vedea http://europa.eu/rapid/press-release_IP-16-216_ro.htm

acestora. De asemenea, ele vor oferi UE și statelor sale membre un cadru juridic pentru protecția datelor mai puternic, ceea ce va duce la o mai bună integrare a pieței interne, în special a pieței unice digitale, și îi va permite UE să își intensifice eforturile în vederea promovării și dezvoltării standardelor internaționale în materie de protecție a vieții private și a datelor cu caracter personal.

În paralel au fost lansate o serie de inițiative importante care au dus la schimbări semnificative ale ordinii juridice din SUA. La 17 ianuarie 2014, președintele Obama a anunțat⁸ că vor fi adoptate reforme privind activitățile de colectare de informații prin interceptarea de semnale, iar acestea au fost formulate ulterior în Directiva prezidențială 28 (PPD-28)⁹. Este important de notat că aceste reforme prevedeau extinderea anumitor măsuri de protecție a vieții private și la alți cetățeni decât cetățenii americani, precum și o reorientare a procesului de colectare a datelor dinspre colectarea masivă de date înspre o abordare care acordă prioritate colectării și accesului axate pe ținte specifice. Comisia a salutat aceste noi orientări, care constituie un pas important în direcția cea bună¹⁰. Acest proces de reformă a fost, de asemenea, important în ceea ce privește furnizarea de informații pentru discuțiile cu SUA referitoare la Scutul de confidențialitate UE-SUA. De atunci au fost introduse alte modificări. De exemplu, în iunie 2015, Statele Unite au adoptat Legea SUA privind libertatea¹¹, care a modificat anumite programe de supraveghere din Statele Unite, a consolidat controlul judiciar și a sporit transparența publică cu privire la utilizarea respectivelor programe. În sfârșit, la 10 februarie 2016, Congresul SUA a adoptat Legea privind căile de atac judiciare (*Judicial Redress Act*), care a fost promulgată de Președintele Obama la 24 februarie 2016¹².

Prezenta comunicare analizează în acest context specific progresele realizate în îndeplinirea obiectivelor formulate în comunicarea din 2013. Ea va sublinia, de asemenea, domeniile în care mai sunt necesare eforturi pentru a consolida și a restabili pe deplin încrederea în fluxurile transatlantice de date.

2. REFORMA UE ÎN MATERIE DE PROTECȚIE A DATELOR

2.1 Contextul

Cu scopul de a profita de oportunitățile unei lumi digitale din ce în ce mai interconectate și de a răspunde provocărilor acesteia, Comisia Europeană și-a prezentat pachetul de reformă privind protecția datelor („reformă”) în ianuarie 2012. Prin consolidarea normelor interne ale UE și prin sporirea controlului pe care cetățenii îl au asupra propriilor date cu caracter personal, reforma vizează stimularea încrederii în economia digitală, indiferent dacă datele cu caracter personal sunt prelucrate în interiorul unui singur stat membru, în UE sau în țări terțe, cum ar fi Statele Unite.

⁸ <https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence>

⁹ <https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>

¹⁰ [http://europa.eu/rapid/press-release MEMO-14-30_en.htm](http://europa.eu/rapid/press-release_MEMO-14-30_en.htm)

¹¹ Legea SUA din 2015 privind libertatea, Pub. L., No. 114-23, § 401, 129 Stat. 268.

¹² H.R.1428 - Legea din 2015 privind căile de atac judiciare. Aceasta va intra în vigoare la 90 de zile după adoptare.

Pachetul de reformă cuprinde două instrumente juridice, un regulament general privind protecția datelor¹³ (denumit în continuare „Regulamentul”), care stabilește un cadru comun al UE pentru protecția datelor, și o directivă privind protecția datelor în domeniul cooperării polițienești și judiciare (denumită în continuare „Directiva privind poliția”)¹⁴. Propunând un regulament care va fi direct aplicabil în statele membre, obiectivul Comisiei a fost de a stabili un standard comun de protecție a datelor pentru toți cetățenii, eliminând astfel diferențele dintre nivelurile de protecție din statele membre. De asemenea, Directiva privind poliția va stabili pentru prima dată un set comun de norme la nivelul UE, ținând cont în același timp de specificitățile tradițiilor judiciare și de aplicare a legii din statele membre.

La 15 decembrie 2015, Parlamentul European și Consiliul au ajuns la un acord politic cu privire la pachetul de reformă, finalizând astfel una dintre acțiunile-cheie prevăzute în Comunicarea din 2013.

2.2 Ce s-a schimbat?

Regulamentul actualizează, modernizează și, în unele cazuri, consolidează principiile de protecție a datelor stabilite în Directiva privind protecția datelor din 1995¹⁵, în vederea garantării dreptului la viața privată. Acesta se concentrează pe consolidarea drepturilor cetățenilor, aprofundarea pieței interne a UE, asigurarea unei aplicări mai stricte a normelor, raționalizarea transferurilor internaționale de date cu caracter personal și stabilirea unor standarde globale de protecție a datelor. Normele sunt concepute în așa fel încât să se asigure protecția datelor cu caracter personal ale cetățenilor UE, indiferent de locul unde acestea sunt transmise, prelucrate sau stocate, chiar și în afara UE, cum este cazul cel mai adesea în lumea digitală. Trebuie în special subliniate o serie de elemente din cadrul reformei.

În primul rând, **acoperirea teritorială**: Regulamentul prevede în mod clar faptul că se aplică și întreprinderilor stabilite într-o țară terță în cazul în care acestea oferă bunuri și servicii în UE sau monitorizează comportamentul cetățenilor UE. Întreprinderile stabilite în afara UE vor trebui să aplice aceleași reguli ca și întreprinderile stabilite în UE. În acest mod se asigură o protecție extinsă a drepturilor cetățenilor UE și se creează, de asemenea, condiții de concurență echitabile între întreprinderile din UE și cele străine, evitându-se astfel dezechilibre de ordin concurențial între întreprinderile din UE și întreprinderile străine care își desfășoară activitatea în UE sau vizează consumatorii europeni.

În al doilea rând, o **aplicare mai strictă** a normelor de protecție a datelor: Regulamentul prevede un regim de sancțiuni eficace prin armonizarea competențelor autorităților naționale de supraveghere în materie de protecție a datelor (denumite în continuare APD). Acestea vor avea competența de a impune amenzi de până la 20 de milioane de euro sau de până la 4 % din cifra de afaceri anuală totală a unei întreprinderi realizată la nivel mondial. Această competență de a impune sancțiuni disuasive pentru nerespectarea normelor privind protecția datelor, coroborată cu acoperirea teritorială menționată mai sus, va garanta că întreprinderile

¹³ COM(2012) 11 final, 25.1.2012: a se vedea nota de subsol 2.

¹⁴ COM(2012) 10 final, 25.1.2012: a se vedea nota de subsol 2.

¹⁵ Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, JO L 281, 23.11.95, p. 31 („Directiva privind protecția datelor”).

care își desfășoară activitatea în UE vor avea tot interesul de a se conforma legislației UE. Noile norme introduc, de asemenea, un regim de răspundere mai clar și mai strict pentru operatori și persoanele împuternicite de către aceștia.

În al treilea rând, **norme armonizate pentru cooperarea în domeniul aplicării legii:** Directiva privind poliția va aplica, în ceea ce privește chestiunile legate de aplicarea dreptului penal, principiile și normele generale în materie de protecție a datelor referitoare la prelucrarea datelor cu caracter personal de către poliție și autoritățile judiciare din statele membre. Acest aspect include norme armonizate pentru transferurile internaționale de date cu caracter personal în contextul cooperării în domeniul aplicării dreptului penal¹⁶. Noua directivă va spori nivelul de protecție a cetățenilor și va garanta în același timp că datele victimelor, ale martorilor și ale suspectilor de infracțiuni sunt protejate în mod adecvat în contextul unei anchete penale sau al unei măsuri de aplicare a legii. Supravegherea este asigurată de către autorități naționale independente în materie de protecție a datelor și cetățenii trebuie să beneficieze de căi de atac judiciare eficiente. În același timp, printr-o mai mare armonizare a legilor se va putea ajunge la o cooperare mai eficientă, la nivelul poliției și al autorităților judiciare, atât între statele membre, cât și între statele membre și partenerii internaționali, în vederea combaterii criminalității și a terorismului într-un mod mai eficient. Aceasta este o parte esențială a Agendei europene privind securitatea¹⁷.

În al patrulea rând, **norme solide pentru transferuri internaționale mai sigure:** atât Regulamentul, cât și Directiva privind poliția prevăd norme transparente, detaliate și cuprinzătoare privind transferurile de date cu caracter personal către țări terțe. Acestea acoperă toate formele de transferuri internaționale, fie că sunt efectuate în scopuri comerciale sau în scopuri de aplicare a legii, între părțile din sectorul privat sau autoritățile publice ori între entitățile private și autoritățile publice. În timp ce structura normelor privind transferurile internaționale rămâne în esență aceeași ca în actuala directivă privind protecția datelor (și anume: deciziile privind caracterul adecvat al protecției, clauzele contractuale standard și regulile corporatiste obligatorii, precum și anumite derogări de la interdicția generală de a transfera date cu caracter personal în afara UE), reforma clarifică și simplifică normele respective în mai multe moduri, reducând în același timp birocratia. Aceasta introduce, de asemenea, câteva noi instrumente pentru transferurile internaționale.

În plus, Regulamentul consolidează **competențele autorităților în materie de protecție a datelor din UE**, inclusiv în ceea ce privește transferurile internaționale. În comparație cu actuala directivă privind protecția datelor, dispozițiile privind independența, atribuțiile și competențele APD din UE sunt precizate mai detaliat și sunt consolidate în mod substanțial. Aceste atribuții includ în mod expres competența de a suspenda fluxurile de date către un destinatar dintr-o țară terță sau către o organizație internațională. Directiva privind poliția

¹⁶ Spre deosebire de aplicarea normelor în temeiul Deciziei-cadru 2008/977/JAI a Consiliului din 27 noiembrie 2008 privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală, care acoperă numai schimburile transfrontaliere de date între autoritățile competente ale statelor membre, aplicarea acestor norme în temeiul Directivei privind poliția nu va mai depinde de schimbul prealabil de date între autoritățile de aplicare a dreptului penal ale statelor membre.

¹⁷ A se vedea Comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social și Comitetul Regiunilor, intitulată „Agenda europeană privind securitatea”, COM(2015) 185 final, 28.4.2015.

conține dispoziții similare în ceea ce privește transferurile internaționale și competențele APD în sectorul aplicării legii.

Mai precis, în ceea ce privește normele referitoare la **deciziile** Comisiei privind **caracterul adecvat**, Regulamentul prevede un catalog precis și detaliat de elemente pe care Comisia trebuie să le ia în considerare atunci când evaluează nivelul de protecție a datelor oferit de cadrul legislativ al unei țări terțe. Acest proces constă într-o evaluare cuprinzătoare care trebuie realizată de Comisie și care ar trebui să acopere – un element care este, de asemenea, în concordanță cu Hotărârea Schrems – normele care reglementează accesul autorităților publice ale unei țări terțe la datele cu caracter personal. O altă caracteristică esențială a acestei evaluări este că cetățenii dispun de drepturi efective și garantate din punct de vedere juridic în materie de protecție a datelor și pot obține căi de atac administrative și judiciare efective.

În plus, Regulamentul prevede în mod expres obligația Comisiei de a **revizui periodic**, cel puțin o dată la patru ani, toate deciziile sale privind caracterul adecvat, pentru a ține pasul cu toate evoluțiile relevante dintr-o țară terță care ar putea avea consecințe directe sau chiar un impact negativ asupra nivelului de protecție din cadrul legislativ al acesteia. Această monitorizare continuă a adecvării va fi un proces mai dinamic, deoarece va presupune, de asemenea, un dialog cu autoritățile din țara terță în cauză.

În ceea ce privește transferurile către țări terțe în care nu există nicio decizie privind caracterul adecvat, Regulamentul stipulează condițiile care reglementează utilizarea de **instrumente alternative de transfer**, cum ar fi clauzele contractuale standard sau regulile corporatiste obligatorii. Acesta adaugă, de asemenea, alte instrumente de transfer, cum ar fi coduri de conduită aprobate și mecanisme de certificare aprobate. În fine, Regulamentul clarifică și situația în care pot fi utilizate **derogări**.

2.3 Calea de urmat

Reforma în materie de protecție a datelor este un pas esențial pentru consolidarea drepturilor fundamentale ale cetățenilor în era digitală și facilitarea activităților întreprinderilor prin simplificarea normelor pentru întreprinderi pe piața unică digitală. Încrederea consumatorilor în operatorii din UE și din țările terțe va alimenta și va stimula astfel economia digitală la nivel european și mondial. Reforma va avea un impact pozitiv asupra relațiilor noastre comerciale cu SUA, partenerul nostru comercial cel mai important, va spori claritatea și va crea un mediu stabil în care întreprinderile din UE și cele străine să își poată desfășura activitatea. La rândul lor, întreprinderile din SUA vor beneficia de securitatea juridică inerentă colaborării cu o zonă integrată din punct de vedere economic, care aplică un set uniform de norme privind protecția datelor.

Existența unor norme comune în domeniul aplicării legii va asigura o mai bună protecție a datelor cetățenilor și accesul acestora la căi de atac judiciare eficace. Facilitarea cooperării transfrontaliere dintre autoritățile polițienești și judiciare din statele membre va spori eficiența aplicării dreptului penal și va crea astfel condițiile necesare pentru a preveni mai eficace criminalitatea în UE. În același timp, aceasta va permite o mai bună cooperare cu omologii lor din țările terțe.

Se preconizează că adoptarea formală a pachetului de reformă de către Parlamentul European și Consiliu va avea loc în primul semestru al anului 2016. Regulamentul se va aplica după doi ani de la adoptare, în timp ce Directiva privind poliția prevede o perioadă de punere în aplicare de doi ani. Toate părțile interesate, atât din interiorul, cât și din afara UE, ar trebui să utilizeze perioada de tranziție de doi ani pentru a se pregăti în vederea aplicării noilor reglementări. Comisia are rolul său în acest proces. În cursul acestei perioade de tranziție, Comisia va colabora îndeaproape cu statele membre, APD și alte părți interesate pentru a asigura o aplicare uniformă a normelor și a promova pregătirea contextului pentru asigurarea conformității.

3. SCUTUL DE CONFIDENȚIALITATE UE-SUA: UN NOU CADRU TRANSATLANTIC PENTRU FLUXURILE DE DATE CU CARACTER PERSONAL

3.1 Contextul

Pentru a facilita fluxurile de date cu caracter personal între UE și SUA în scopul schimburilor comerciale și a asigura în același timp protecția datelor respective, Comisia considera în 2000 cadrul sferei de siguranță drept un cadru ce asigură un nivel adecvat de protecție¹⁸. Ca urmare, în ciuda absenței unei legi generale privind protecția datelor în SUA, datele cu caracter personal puteau fi transferate în mod liber dinspre statele membre ale UE către întreprinderile din SUA care aderaseră la principiile privind protecția vieții private aflate la baza cadrului.

În comunicarea din 2013 privind sfera de siguranță¹⁹, Comisia a evidențiat o serie de deficiențe în ceea ce privește funcționarea mecanismului de-a lungul timpului, în special lipsa de transparență din partea întreprinderilor cu privire la aderarea acestora la sistem, precum și lipsa unui control eficace al aplicării legii de către autoritățile din SUA în ceea ce privește respectarea de către întreprinderile respective a principiilor sistemului privind protecția vieții private. În plus, dezvăluirile anterioare din cursul aceluiași an privind programele de supraveghere au ridicat semne de întrebare în ceea ce privește amploarea și domeniul de aplicare al anumitor programe americane de informații și nivelul de acces al autorităților publice din SUA la datele cu caracter personal ale cetățenilor europeni care erau transferate în cadrul sferei de siguranță. Ținând seama de aceste elemente, precum și de altele²⁰, Comisia a concluzionat că mecanismul sferei de siguranță trebuia revizuit. În acest context, Comisia a formulat 13 recomandări²¹ menite să consolideze și să actualizeze garanțiile de protecție a datelor incluse în acest cadru. Recomandările se concentrău asupra următoarelor aspecte: (i)

¹⁸ Decizia 2000/520/CE a Comisiei din 20 iulie 2000. În respectiva decizie, pe baza articolului 25 alineatul (6) din Directiva privind protecția datelor, Comisia considera că principiile privind protecția vieții private ale sferei de siguranță și întrebările frecvente aferente formulate de Departamentul de Comerț al SUA ofereau o protecție adecvată pentru transferurile de date cu caracter personal dinspre UE. Funcționarea mecanismului sferei de siguranță se baza pe angajamentele și autocertificarea societăților care aderau la acesta. Normele erau obligatorii pentru aceste entități în temeiul legislației SUA, iar Comisia Federală pentru Comerț a SUA avea competența de a asigura respectarea lor.

¹⁹ A se vedea nota de subsol 3.

²⁰ Aceste aspecte includeau și creșterea exponențială a fluxurilor de date și importanța critică a acestora pentru economia transatlantică, precum și creșterea rapidă a numărului de întreprinderi din SUA care aderă la mecanismul sferei de siguranță. A se vedea Comunicarea privind sfera de siguranță, p. 37.

²¹ Comunicarea privind sfera de siguranță, p. 18-19.

consolidarea principiilor esențiale privind respectarea vieții private și sporirea transparenței politicilor în materie de respectare a vieții private ale întreprinderilor autocertificate din SUA care au încorporat aceste principii; (ii) obținerea unui nivel mai bun și mai eficace de supraveghere, monitorizare și control de către autoritățile din SUA a modului în care întreprinderile se conformează principiilor; (iii) disponibilitatea unor mecanisme de soluționare a litigiilor pentru plângerile individuale care să fie abordabile din punct de vedere financiar și (iv) necesitatea de a asigura faptul că utilizarea derogării privind securitatea națională și aplicarea legii prevăzută în decizia din 2000 privind sfera de siguranță se limitează la ceea ce este strict necesar și proporțional.

Pe baza acestor 13 recomandări, Comisia a inițiat discuții cu autoritățile din SUA în ianuarie 2014. Invalidarea ulterioară, la 6 octombrie 2015, a deciziei privind sfera de siguranță de către Curtea de Justiție a confirmat necesitatea unui cadru nou și mai puternic pentru fluxurile de date comerciale transatlantice. În timp ce hotărârea Curții se bazează pe recomandările Comisiei din 2013, aceasta subliniază și mai mult nevoia de a institui limitări, garanții și mecanisme de control juridic pentru a asigura protecția continuă a datelor cu caracter personal ale cetățenilor din UE, inclusiv în cazul în care datele sunt accesate și utilizate de autoritățile publice pentru securitatea națională, interesul public sau aplicarea legii.

La 2 februarie 2016, după doi ani de discuții intense, UE și SUA au ajuns la un acord politic privind un nou cadru, Scutul de confidențialitate UE-SUA. Acest nou acord cuprinde noi garanții importante și va asigura un nivel ridicat de protecție a drepturilor fundamentale ale cetățenilor UE. Acordul va oferi întreprinderilor de pe ambele maluri ale Atlanticului care doresc să facă afaceri împreună securitatea juridică necesară și va da un nou elan parteneriatului transatlantic.

În urma încheierii negocierilor cu SUA, Comisia va prezenta noul acord Grupului de lucru „Articolul 29” (care va include și APD din UE), în vederea obținerii unui aviz privind nivelul de protecție oferit. În plus, decizia privind caracterul adecvat va trece prin procedura de comitologie înainte de adoptare. Autoritatea Europeană pentru Protecția Datelor va fi, de asemenea, consultată.

3.2 Ce s-a schimbat?

Scutul de confidențialitate UE-SUA oferă un răspuns solid și eficace atât la cele 13 recomandări ale Comisiei, cât și la Hotărârea Schrems. Acesta cuprinde o serie de îmbunătățiri importante, în comparație cu cadrul precedent, cu privire la angajamentele care trebuie asumate de întreprinderile din SUA și conține, de asemenea, angajamente noi și importante și explicații detaliate cu privire la reglementările și practicile relevante din SUA ale autorităților americane. Spre deosebire de actul premergător, Scutul de confidențialitate se referă nu numai la angajamentele din sectorul comercial, ci și - în mod semnificativ și pentru prima oară în relațiile UE-SUA - la cele din domeniul accesului autorităților publice la datele cu caracter personal, inclusiv în scopuri legate de securitatea națională. Acesta este un element crucial și necesar, având în vedere jurisprudența Curții, pentru a restabili încrederea în relațiile transatlantice în urma dezvoltărilor privind programele de supraveghere.

Cele mai importante realizări ale acestui nou acord pot fi grupate în patru categorii principale:

În primul rând, **obligatii stricte pentru întreprinderi și un control solid al respectării acestor obligații**: noul sistem va fi mai transparent și va cuprinde mecanisme eficace de supraveghere pentru a garanta că întreprinderile respectă normele pe care au obligația legală de a le respecta. Societățile americane care doresc să importe date cu caracter personal din Europa în temeiul Scutului de confidențialitate vor trebui să accepte obligații stricte cu privire la modul de prelucrare a datelor cu caracter personal și de garantare a drepturilor individuale. Este vorba inclusiv de condiții mai stricte și de dispoziții mai riguroase privind răspunderea pentru întreprinderile care aderă la Scutul de confidențialitate și care transferă date din UE, de exemplu pentru activități de subprelucrare, către părți terțe din afara cadrului, fie în SUA, fie în alte țări terțe („transferuri ulterioare”). În ceea ce privește supravegherea, Departamentul de Comerț al SUA s-a angajat să monitorizeze cu regularitate și rigurozitate modul în care întreprinderile își respectă angajamentele și să excludă întreprinderile care pretind să beneficieze de sistem fără a îndeplini condițiile necesare pentru aderare. Angajamentele întreprinderilor sunt obligatorii și garantate din punct de vedere juridic în temeiul legislației SUA de către Comisia Federală pentru Comerț, iar întreprinderile care nu se conformează acestora se vor confrunta cu sancțiuni severe.

În al doilea rând, **limite și garanții clare în ceea ce privește accesul guvernului SUA**: pentru prima dată, guvernul SUA, prin intermediul Departamentului de Justiție și al Biroului Directorului Serviciului Național de Informații, organismul de supraveghere a întregii comunități a serviciilor de informații din SUA, a oferit UE declarații scrise și asigurări că accesul autorităților publice în scopul aplicării legii, al asigurării securității naționale și în alte scopuri de interes public va fi supus unor limitări, garanții și mecanisme de supraveghere clare. SUA va institui, de asemenea, un nou mecanism de atac pentru persoanele vizate din UE în domeniul securității naționale, prin intermediul unui Ombudsman care va fi independent de autoritățile naționale de securitate. Ombudsmanul va fi însărcinat cu urmărirea plângerilor și cererilor efectuate de cetățeni din UE în ceea ce privește accesul în scopul securității naționale și va trebui să confirme că legile relevante au fost respectate sau că neconformitatea a fost remediată. Această măsură reprezintă un progres semnificativ și se va aplica nu numai pentru transferurile efectuate în temeiul Scutului de confidențialitate, ci pentru *toate* transferurile de date cu caracter personal efectuate către SUA în scopuri comerciale, indiferent de baza utilizată pentru a transfera aceste date.

În al treilea rând, **protecția efectivă a drepturilor la viața privată a cetățenilor UE, cu mai multe căi de atac posibile**: orice cetățean european care consideră că datele sale au fost utilizate în mod necorespunzător în temeiul noului acord va beneficia de mai multe posibilități accesibile și abordabile din punct de vedere financiar de a obține măsuri reparatorii individuale, printre posibilități numărându-se inclusiv organismele alternative gratuite de soluționare a litigiilor. Societățile se angajează să răspundă plângerilor într-un termen stabilit. În plus, orice întreprindere care manipulează date în materie de resurse umane din Europa trebuie să se angajeze să respecte deciziile APD de resort din UE, în timp ce alte întreprinderi își pot asuma un astfel de angajament dacă doresc. De asemenea, cetățenii își pot prezenta plângerea autorității „locale” de protecție a datelor, care va dispune de o procedură formală

prin care să adreseze plângerile Departamentului de Comerț și Comisiei Federale pentru Comerț, pentru a facilita investigarea și soluționarea plângerii respective într-un interval de timp rezonabil. Dacă însă o plângere nu este soluționată prin niciuna dintre aceste posibilități, cetățenii vor putea să recurgă, în ultimă instanță, la Comitetul Scutului de confidențialitate, un mecanism de soluționare a litigiilor având competența de a lua decizii obligatorii și garantate din punct de vedere juridic pentru a sancționa întreprinderile din SUA care au aderat la Scutul de confidențialitate. În plus, APD din UE vor putea oferi asistență cetățenilor în pregătirea plângerii. După cum s-a menționat mai sus, în cazul plângerilor privind eventualul acces al autorităților naționale în materie de servicii de informații, va fi instituit un nou Ombudsman, ceea ce va oferi o cale suplimentară de atac.

În al patrulea și ultimul rând, un **mechanism comun de revizuire anuală**: acesta va permite Comisiei să monitorizeze în mod regulat funcționarea tuturor aspectelor legate de Scutul de confidențialitate, inclusiv limitele și garanțiile legate de accesul în scopul securității naționale. Comisia și Departamentul de Comerț al SUA vor realiza revizuirea, cu implicarea autorităților de protecție a datelor din UE și a autorităților naționale de securitate ale SUA, precum și a Ombudsmanului. În acest mod, Statele Unite vor trebui să își respecte angajamentele asumate. Dar Comisia nu se va opri aici, ci va utiliza, de asemenea, toate celelalte surse de informații disponibile, inclusiv rapoartele voluntare de transparență ale întreprinderilor privind nivelul cererilor de acces ale guvernului²². Revizuirea anuală depășește sfera dispozițiilor cuprinse în noul Regulament, care impune ca aceste revizuiuri să aibă loc cel puțin o dată la patru ani, ceea ce arată voința atât a UE, cât și a SUA de a asigura în mod riguros conformitatea deplină.

Această revizuire nu va fi un exercițiu de formă, fără consecințe. În situațiile în care întreprinderile sau autoritățile publice din SUA nu își respectă angajamentele, Comisia va iniția procedura de suspendare a Scutului de confidențialitate. Astfel cum Curtea de Justiție a subliniat în Hotărârea Schrems, o decizie privind caracterul adecvat nu trebuie să rămână literă moartă; dimpotrivă, întreprinderile și autoritățile din SUA trebuie să întrețină cadrul și să îl susțină continuu prin respectarea angajamentelor asumate. În caz contrar, beneficiul specific în ceea ce privește transferurile de date obținut în urma luării deciziei privind caracterul adecvat nu se mai justifică și va fi retras.

3.3 Calea de urmat

Angajamentele convenite de SUA în temeiul Scutului de confidențialitate vor constitui baza unei noi decizii a Comisiei privind caracterul adecvat și se vor reflecta în această decizie. Întreprinderile sunt încurajate să înceapă deja pregătirile astfel încât să fie în măsură să participe la noul cadru cât mai repede posibil după instituirea sa, în urma adoptării deciziei Comisiei. La rândul său, guvernul SUA își va publica declarațiile în Registrul Federal al SUA, atestând astfel în mod public că își respectă angajamentele.

Scutul de confidențialitate UE-SUA necesită intervenția unui număr important de actori:

²² Unele firme importante de internet din SUA întocmesc deja astfel de rapoarte pentru a recâștiga încrederea clienților lor. Legea SUA din 2015 privind libertatea permite publicarea de rapoarte voluntare privind cererile de acces, cel puțin în anumite limite, pentru a proteja interesele în materie de securitate națională.

- întreprinderile americane participante, care trebuie să îndeplinească obligațiile ce le revin în temeiul cadrului, fiind pe deplin conștiente că acesta va fi strict respectat și că vor fi sancționate în cazul în care nu i se conformează. Pentru a consolida încrederea consumatorilor, întreprinderile sunt, de asemenea, încurajate să opteze pentru APD din UE în vederea soluționării plângerilor efectuate în temeiul Scutului de confidențialitate, întrucât este probabil ca cetățenii europeni să se orienteze cu predilecție către aceste autorități. În mod similar, măsura în care întreprinderile sunt pregătite să utilizeze posibilitatea prevăzută în legislația SUA de a publica rapoarte de transparență privind cererile de acces, în scopul asigurării securității naționale și aplicării legii, la datele primite de la nivelul UE va contribui la menținerea încrederii în faptul că un astfel de acces este limitat la ceea ce este necesar și proporțional²³;
- diferitele autorități din SUA însărcinate cu supravegherea și asigurarea aplicării cadrului și cu respectarea, în același timp, a limitelor și garanțiilor în ceea ce privește accesarea datelor în scopul aplicării legii și al asigurării securității naționale, precum și cele însărcinate cu formularea unui răspuns prompt și semnificativ la plângerile adresate de cetățeni ai UE cu privire la o eventuală utilizare necorespunzătoare a datelor lor cu caracter personal;
- APD din UE, care au un rol important în ceea ce privește garantarea faptului că cetățenii își pot exercita drepturile în mod efectiv în cadrul Scutului de confidențialitate, inclusiv prin dirijarea plângerilor acestora către autoritățile de resort din SUA, cooperarea cu autoritățile respective, declanșarea mecanismului de avertizare a Ombudsmanului, sprijinirea reclamanților în ceea ce privește prezentarea plângerii acestora către Comitetul Scutului de confidențialitate, precum și monitorizarea transferurilor de date în materie de resurse umane și
- Comisia, care este responsabilă în ceea ce privește luarea deciziei privind caracterul adecvat și revizuirea acesteia în mod regulat: aceste revizuii periodice marchează o diferență semnificativă față de procedura anterioară, care era statică, prin aceea că transformă decizia privind caracterul adecvat luată în temeiul Scutului de confidențialitate într-un cadru dinamic, monitorizat îndeaproape.

Revizuirea comună anuală și raportul subsecvent al Comisiei, precum și posibilitatea suspendării acordului în cazul nerespectării acestuia, vor avea astfel un rol central în asigurarea durabilității Scutului de confidențialitate. Obiectivul nostru transatlantic comun ar trebui să fie acela de a dezvolta împreună o cultură puternică a respectării vieții private și a protecției drepturilor individuale care să refacă și să mențină încrederea.

²³ Aceste rapoarte ar trebui să fie întocmite în conformitate cu dispozițiile Legii SUA din 2015 privind libertatea. A se vedea nota de subsol 22.

4. ACORDUL CADRU: CONSOLIDAREA GARANȚIILOR ÎN MATERIE DE PROTECȚIE A DATELOR ÎN VEDEREA COOPERĂRII ÎN DOMENIUL APLICĂRII LEGII

4.1 Contextul

Un aspect important al relației transatlantice este capacitatea UE, a statelor membre și a SUA de a răspunde eficient la amenințările și provocările comune în materie de securitate, într-un mod coordonat și bazat pe cooperare. Acest răspuns colectiv depinde în mod semnificativ de capacitatea noastră de a face schimb de date cu caracter personal în cadrul cooperării polițienești și judiciare în materie penală. Pentru a realiza acest obiectiv, de-a lungul timpului s-au încheiat numeroase acorduri bilaterale între statele membre și SUA, precum și între UE și SUA²⁴. În același timp, este la fel de important ca aceste acorduri în materie de aplicare a legii să furnizeze garanții eficace privind protecția datelor. Obiectivul dublu de a colabora cu succes cu partenerii noștri din SUA în combaterea infracțiunilor grave și a terorismului și de a spori în același timp nivelul de protecție a cetățenilor europeni, în conformitate cu drepturile lor fundamentale și cu normele UE de protecție a datelor, în cazul în care se efectuează transferuri în aceste scopuri, a declanșat un proces de negocieri lansat în martie 2011, cu privire la un acord internațional în materie de protecție a datelor în domeniul aplicării legii, și anume Acordul-cadru UE-SUA privind protecția datelor²⁵.

UE și SUA au finalizat negocierile în vara anului 2015. Cele două părți au parafat acordul-cadru la 8 septembrie 2015 la Luxemburg²⁶, acesta urmând să fie ratificat pe ambele maluri ale Atlanticului. Semnarea acordului-cadru a fost totuși condiționată de adoptarea Legii privind căile de atac judiciare de către Congresul SUA, astfel încât să se prevadă pentru prima dată egalitatea de tratament dintre cetățenii UE și cetățenii SUA, care fac obiectul Legii SUA din 1974 privind protecția vieții private²⁷. Proiectul de lege a fost aprobat de Congres la 10 februarie 2016, iar legea a fost promulgată la 24 februarie 2016.

4.2 Ce s-a schimbat?

Acordul-cadru va consacra, pentru prima dată, un set armonizat și cuprinzător de garanții în materie de protecție a datelor, care se va aplica tuturor schimburilor transatlantice între autoritățile de resort din domeniul aplicării dreptului penal. Acesta este un acord fundamental privind drepturile cetățenilor, care stabilește un înalt standard de protecție pe baza căruia trebuie măsurate toate schimburile de date din acordurile existente și viitoare.

²⁴ Este vorba, în special, de Acordul UE-SUA privind Registrul cu numele pasagerilor și Programul UE-SUA de urmărire și de identificare a finanțărilor în scopuri teroriste.

²⁵ Un acord între UE și SUA privind protecția datelor cu caracter personal atunci când acestea sunt transferate și prelucrate în scopul prevenirii, investigării, detectării sau urmăririi infracțiunilor, inclusiv a terorismului, în cadrul cooperării polițienești și al cooperării judiciare în materie penală.

²⁶ http://europa.eu/rapid/press-release_STATEMENT-15-5610_en.htm

²⁷ Legea privind căile de atac judiciare acordă drepturi cetățenilor din „țările acoperite”, care sunt desemnate de guvernul SUA. Această acoperire este condiționată, la rândul său, de următoarele criterii: (a) țara [sau organizația regională] a încheiat un acord cu Statele Unite privind protecția vieții private în cazul informațiilor transmise în scopul prevenirii, investigării, detectării sau urmăririi infracțiunilor; (b) țara [sau organizația regională] permite transferul de date cu caracter personal în scopuri comerciale înspre și dinspre Statele Unite și (c) politicile privind transferul datelor cu caracter personal în scopuri comerciale, precum și acțiunile conexe din țara sau organizația regională nu afectează în mod semnificativ interesele Statelor Unite în materie de securitate națională.

În primul rând, **măsurile de protecție și garanțiile prevăzute de acordul-cadru se vor aplica în mod orizontal la toate schimburile de date survenite în contextul cooperării transatlantice în domeniul aplicării legii în materie penală.** Aceasta include transferuri efectuate pe baza legislațiilor interne, a acordurilor dintre UE și SUA, a acordurilor dintre statele membre și SUA (cum ar fi tratatele de asistență judiciară reciprocă), precum și pe baza unor acorduri specifice referitoare la transferul de date cu caracter personal de către entități private în scopul aplicării legii. Astfel, dispozițiile convenite vor spori imediat, în cazul transferului de date către SUA, nivelul de protecție garantat pentru persoanele vizate din UE. Ele vor spori, de asemenea, securitatea juridică pentru cooperarea transatlantică în materie de aplicare a legii, prin asigurarea faptului că acordurile existente conțin toate măsurile de protecție necesare și că pot, așadar, răspunde la posibilele contestări de ordin juridic.

În al doilea rând, dispozițiile acoperă toate normele de bază ale UE în materie de protecție a datelor în ceea ce privește **standardele privind prelucrarea datelor** (de exemplu, calitatea și integritatea datelor, securitatea datelor, răspunderea și supravegherea), **garanțiile și limitările** (de exemplu, limitările legate de scop și de utilizare, păstrarea datelor, transferurile ulterioare, prelucrarea datelor sensibile), precum și **drepturile individuale** (accesul, rectificarea, căile de atac administrative și judiciare).

În al treilea rând, acordul va asigura că sunt instituite **drepturi la o cale de atac judiciară pentru refuzul accesului, refuzul rectificării și divulgarea ilegală.** Acest aspect reprezintă o îmbunătățire majoră și va contribui în mod semnificativ la restabilirea încrederii în schimburile transatlantice. Această cerere-cheie, pe care UE o formulase de multă vreme și care rămăsese fără răspuns timp de mai mulți ani, a fost deja reflectată în Legea privind căile de atac judiciare introdusă în Congresul SUA în martie 2015 și adoptată la 10 februarie 2016. Această lege va oferi și cetățenilor UE²⁸ trei căi de atac judiciare principale prevăzute de Legea SUA din 1974 privind protecția vieții private, care în prezent sunt rezervate doar cetățenilor și rezidenților permanenți din SUA. Astfel, pentru prima dată, cetățenii UE vor fi în măsură să beneficieze de drepturi cu aplicabilitate generală pentru orice transfer transatlantic de date în domeniul aplicării dreptului penal. Se elimină în acest fel o diferență esențială de tratament între cetățenii UE și cetățenii SUA.

În al patrulea rând, acordul-cadru generalizează și extinde principiul **supravegherii independente** la întregul sector de aplicare a legii, drept cerință de bază în materie de protecție a datelor, care nu este prezentă în multe dintre acordurile bilaterale existente. Această măsură înseamnă acordarea de competențe efective de a investiga și de a soluționa plângerile individuale referitoare la conformitatea cu acordul.

În al cincilea rând, punerea efectivă în aplicare a acordului-cadru va face obiectul **unor revizuii comune periodice.** În cadrul acestor revizuii, se va acorda o atenție deosebită dispozițiilor referitoare la drepturile cetățenilor (accesul, rectificarea, căile de atac administrative și judiciare).

²⁸ În conformitate cu Legea privind căile de atac judiciare, și alte țări terțe sau „organizații de integrare economică regională” pot fi desemnate drept „țări acoperite”, ceea ce înseamnă că cetățenii acestora beneficiază de dreptul la exercitarea unei căi de atac judiciare.

Acordul-cadru în sine nu autorizează transferuri de date și nici nu constituie o decizie privind caracterul adecvat.

4.3 Calea de urmat

Intrarea în vigoare a Legii privind căile de atac judiciare²⁹ va pregăti contextul pentru semnarea acordului-cadru. Comisia va prezenta în curând Consiliului o propunere de decizie de autorizare a semnării acordului-cadru. După semnare, decizia de încheiere a acordului va trebui să fie adoptată de Consiliu, după obținerea aprobării Parlamentului European. Acordul-cadru va îmbunătăți semnificativ situația actuală, caracterizată de norme de protecție a datelor fragmentate, nearmonizate și adesea deficitare, care coexistă într-un mozaic de instrumentele multilaterale, bilaterale, naționale și sectoriale. Acordul-cadru are o funcție retroactivă, prin aceea că va completa garanțiile în materie de protecție a datelor din acordurile actuale în cazul și în măsura în care acestea nu dispun de nivelul necesar de protecție. În acest sens, acordul-cadru va aduce o valoare adăugată considerabilă, în special deoarece va „completa golurile” din acordurile existente, care conțin standarde de protecție a datelor mai scăzute decât cele prevăzute de acordul-cadru. Acest lucru va permite continuitatea cooperării în domeniul aplicării legii și va asigura în același timp o mai mare securitate juridică în momentul efectuării transferurilor. În ceea ce privește acordurile viitoare, acordul-cadru va reprezenta un prag de siguranță dincolo de care nivelul de protecție nu poate scădea. Aceasta este o garanție foarte importantă pentru viitor și o schimbare majoră față de situația actuală, în care garanțiile, măsurile de protecție și drepturile trebuie să fie negociate de la zero pentru fiecare nou acord. Prin urmare, acordul-cadru este un model care conține garanțiile standard ce nu mai pot fi negociate în vederea atingerii unui nivel inferior de protecție. Acesta este un precedent foarte important nu numai pentru relațiile dintre UE și Statele Unite, ci și, în general, pentru orice viitor acord încheiat la nivel internațional privind protecția datelor sau schimbul de date.

Negociat în paralel cu reforma, acordul-cadru este aliniat la acquis-ul UE în materie de protecție a datelor. Interacțiunea dintre acordul-cadru și Directiva privind poliția este deosebit de relevantă, dată fiind importanța instituirii unui nivel ridicat și comun de protecție a datelor, indiferent dacă datele cu caracter personal sunt prelucrate la nivel național sau dacă fac obiectul schimburilor transfrontaliere în interiorul UE sau cu țări terțe. În acest sens, acordul-cadru va contribui la justificarea cerințelor generale ale reformei în contextul transatlantic.

Încheierea negocierilor privind acordul-cadru care stabilește standarde comune în domeniul complex al legislației și politicilor constituie o realizare semnificativă. Viitorul acord-cadru va restabili și va consolida încrederea, va oferi garanții privind legalitatea transferurilor de date și va facilita cooperarea dintre UE și SUA în acest domeniu.

Ca o măsură ulterioară, este necesar să abordăm împreună provocările comune din domeniul cooperării polițienești și judiciare. O chestiune importantă și încă nesoluționată este problema accesului direct al autorităților de aplicare a legii la datele cu caracter personal deținute de societățile private din străinătate. Un astfel de acces ar trebui, în principiu, să aibă loc în cadrul canalelor oficiale de cooperare, cum ar fi acordurile de asistență judiciară reciprocă sau

²⁹ Legea privind căile de atac judiciare intră în vigoare la 90 de zile după adoptare.

alte acorduri sectoriale. Întreprinderile private riscă în prezent să se confrunte cu lipsa securității juridice, ceea ce ar putea afecta capacitatea acestora de a funcționa în diferite jurisdicții, atunci când li se solicită să ofere accesul la probe electronice, în temeiul legislației unei țări, constând în date cu caracter personal care fac obiectul legislației dintr-o altă țară. În paralel cu următoarea revizuire a Acordului UE-SUA de asistență judiciară reciprocă³⁰, UE ar dori să se organizeze dialoguri suplimentare cu SUA în acest domeniu, inclusiv în ceea ce privește chestiunea elaborării de norme comune și mai eficace privind colectarea de probe electronice.

5. CONCLUZIE

Încheierea cu succes a principalelor acțiuni evidențiate în comunicarea din 2013 demonstrează capacitatea UE de a rezolva probleme într-un mod pragmatic și prin măsuri specifice, fără a-și sacrifica puternicele valori și tradiții în materie de drepturi fundamentale. Aceasta mai demonstrează că UE și SUA sunt în măsură să treacă peste diferențe și ia decizii dificile pentru a menține o relație strategică ce a trecut cu succes testul timpului. În același timp, în momentul în care începem un nou capitol în relațiile noastre bilaterale, trebuie să rămânem vigilenți, dat fiind că ne confruntăm în continuare cu amenințări și provocări comune într-o lume nesigură.

Odată ce Scutul de confidențialitate și acordul-cadru vor fi în vigoare, le revine ambelor părți sarcina de a asigura că aceste două cadre importante de transfer de date funcționează în mod eficace și într-o manieră durabilă. Succesul lor depinde în mare parte de aplicarea efectivă a acestora și de respectarea drepturilor conferite cetățenilor. De asemenea, acesta depinde de evaluarea continuă a modului lor de funcționare; este necesară, în acest sens, o schimbare de paradigmă, pentru a trece de la un proces static la unul mai dinamic.

În acest context, un element important al acestui proces se referă la reforma în curs a programelor americane de informații. În acest sens, Comisia va urmări îndeaproape viitoarele rapoarte elaborate de Comitetul de supraveghere a vieții private și a libertăților civile (*Privacy and Civil Liberties Oversight Board*) și revizuirea, preconizată pentru 2017, a programului FISA (*Foreign Intelligence Surveillance Act*), articolul 702, în ceea ce privește supravegherea activităților străine. Mai precis, vor fi monitorizate îndeaproape noile reforme privind transparența, supravegherea și extinderea măsurilor de protecție pentru persoanele care nu sunt cetățeni ai SUA.

La un nivel mai general, având în vedere importanța fluxurilor transfrontaliere de date pentru comerțul transatlantic, UE va urmări îndeaproape progresele legislative viitoare înregistrate în SUA în domeniul protecției vieții private. Acum că Europa și-a constituit un singur set de norme, coerent și solid, sperăm că SUA va continua, de asemenea, să depună eforturi în direcția unui sistem cuprinzător de protecție a vieții private și a datelor. Este nevoie de o astfel

³⁰ Decizia 2009/820/PESC a Consiliului din 23 octombrie 2009 privind încheierea, în numele Uniunii Europene, a Acordului privind extrădarea între Uniunea Europeană și Statele Unite ale Americii și a Acordului privind asistența judiciară reciprocă între Uniunea Europeană și Statele Unite ale Americii, JO L 291, 7.11. 2009, p. 40-41.

de abordare cuprinzătoare pentru a realiza convergența pe termen lung dintre cele două sisteme. În acest sens, Comisia va organiza un summit anual pe tema protecției vieții private cu ONG-urile interesate și cu alte părți interesate de pe ambele maluri ale Atlanticului.

Parteneriatul UE-SUA poate fi un motor pentru dezvoltarea și promovarea standardelor juridice internaționale de protecție a vieții private și a datelor cu caracter personal. Inițiativele la nivelul ONU, inclusiv activitatea Raportorului special al ONU privind dreptul la viață privată, pot juca, de asemenea, un rol important în această privință. În anii următori, având în vedere creșterea importanței acestor chestiuni la nivel mondial, UE și SUA ar trebui să profite de această ocazie pentru a apăra valorile comune ale drepturilor și libertăților individuale într-o lume digitală globalizată.