COMISIA
EUROPEANĂ

Bruxelles, 6.11.2015
COM(2015) 566 final

COMUNICARE A 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)

COMUNICARE A 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)

1. INTRODUCERE: ANULAREA DECIZIEI PRIVIND SFERA DE SIGURANȚĂ

Prin hotărârea pronunțată de Curtea de Justiție a Uniunii Europene (denumită în continuare „Curtea de Justiție" sau „Curtea") la 6 octombrie 2015 în cauza C-362/14 (Schrems)[1] se reafirmă importanța dreptului fundamental la protecția datelor cu caracter personal, astfel cum este consacrat în Carta drepturilor fundamentale a UE, inclusiv atunci când aceste date sunt transferate în afara UE.

Transferul de date cu caracter personal este un element esențial al relațiilor transatlantice. UE și Statele Unite reprezintă, una pentru cealaltă, cel mai important partener comercial, iar transferurile de date fac în tot mai mare măsură parte integrantă din schimburile lor comerciale.

Pentru a facilita aceste fluxuri de date, asigurând în același timp un nivel ridicat de protecție a datelor cu caracter personal, Comisia a recunoscut caracterul adecvat al cadrului reprezentat de sfera de siguranță, prin adoptarea Deciziei 2000/520/CE a Comisiei din 20 iulie 2000 (denumită în continuare „decizia privind sfera de siguranță"). Prin această decizie, Comisia a recunoscut, în temeiul articolului 25 alineatul (6) din Directiva 95/46/CE[2], faptul că principiile sferei de siguranță privind protecția vieții private și întrebările frecvente aferente publicate de Departamentul Comerțului al SUA. asigură un nivel de protecție adecvat în scopul transferurilor de date cu caracter personal din UE[3]. Drept urmare, a devenit posibil transferul liber al datelor cu caracter personal din state membre ale UE către societăți din Statele Unite ale Americii care s-au angajat să respecte principiile respective, în pofida faptului că în Statele Unite ale Americii nu există o lege privind protecția datelor în general. Funcționarea mecanismului sferei de siguranță se baza pe angajamentele și autocertificarea societăților care aderau la acesta. Deși angajamentul de a respecta principiile sferei de siguranță privind protecția vieții private și „întrebările de bază" este voluntar, normele în cauză sunt, în conformitate cu legislația SUA, obligatorii pentru entitățile care s-au angajat să

[1] Hotărârea din 6 octombrie 2015 în cauza C-362/14 Maximilian Schrems/Data Protection Commissioner, EU:C:2015:650 (denumită în continuare și „hotărârea" sau „hotărârea pronunțată în cauza Schrems").

[2] 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 din 23.11.95, p. 31 (denumită în continuare „Directiva 95/46/CE" sau „directiva").

[3] În sensul prezentei comunicări, termenul „UE" include și SEE. Prin urmare, referirile la „state membre" trebuie interpretate ca incluzând statele membre ale SEE.

le respecte, iar Comisia Federală pentru Comerț a SUA are competența de a asigura respectarea lor[4].

Prin hotărârea din 6 octombrie 2015, Curtea a invalidat decizia privind sfera de siguranță. În acest context, prezenta comunicare își propune să ofere o imagine de ansamblu a instrumentelor alternative pentru efectuarea de transferuri de date transatlantice conforme cu dispozițiile Directivei 95/46/CE în absența unei decizii privind caracterul adecvat. Sunt, de asemenea, descrise pe scurt consecințele hotărârii asupra altor decizii ale Comisiei privind caracterul adecvat. În hotărârea sa, Curtea precizează că o decizie privind caracterul adecvat adoptată în temeiul articolului 25 alineatul (6) din Directiva 95/46/CE nu poate fi luată decât în cazul în care Comisia constată că nivelul de protecție a datelor cu caracter personal din țara terță în cauză este nu neapărat identic, dar „în esență echivalent" cu cel garantat în cadrul UE în temeiul directivei interpretate în lumina Cartei drepturilor fundamentale. În ceea ce privește decizia privind sfera de siguranță, Curtea a susținut că aceasta nu conține suficiente elemente prin care Comisia să constate limitarea accesului autorităților publice din SUA la datele transferate în temeiul deciziei, nici privind existența unei protecții juridice eficiente împotriva unor astfel de ingerințe. Mai concret, Curtea precizează că o reglementare care le permite autorităților publice accesul în mod generalizat la conținutul comunicărilor electronice aduce atingere substanței dreptului fundamental la respectarea vieții private. În plus, Curtea a confirmat că, chiar dacă există o decizie privind caracterul adecvat adoptată în temeiul articolului 25 alineatul (6) din Directiva 95/46/CE, autoritățile pentru protecția datelor din statele membre au în continuare competența și obligația de a examina, în condiții de independență deplină, dacă transferul datelor către o țară terță respectă cerințele impuse de directiva menționată, interpretate în lumina articolelor 7, 8 și 47 din Carta drepturilor fundamentale. Pe de altă parte, Curtea a afirmat, de asemenea, că sarcina de a invalida un act al UE, cum ar fi o decizie a Comisiei privind caracterul adecvat, îi revine exclusiv Curții de Justiție.

Hotărârea Curții se bazează pe Comunicarea Comisiei din 2013 privind funcționarea sferei de securitate din perspectiva cetățenilor UE și a întreprinderilor stabilite în UE[5], în care Comisia a identificat o serie de deficiențe și a prezentat 13 recomandări. Pe baza acestor recomandări, Comisia a participat, începând cu luna ianuarie 2014, la discuții cu autoritățile din SUA, având drept scop instituirea unui nou acord, mai solid, pentru schimburile transatlantice de date.

În urma hotărârii Curții, Comisia rămâne angajată în direcția găsirii unui nou cadru, mai solid, pentru transferul transatlantic de date cu caracter personal. În acest sens, Comisia a reluat

[4] Pentru o prezentare mai aprofundată a mecanismului sferei de siguranță, a se vedea Comunicarea Comisiei către Parlamentul European și Consiliu privind funcționarea sferei de securitate din perspectiva cetățenilor UE și a întreprinderilor stabilite în UE, COM(2013) 847 final.

[5] Comunicarea Comisiei către Parlamentul European și Consiliu privind funcționarea sferei de securitate din perspectiva cetățenilor UE și a întreprinderilor stabilite în UE, COM(2013) 847 final, 27.11.2013. A se vedea, de asemenea, Comunicarea Comisiei către Parlamentul European și Consiliu „Restabilirea încrederii în fluxurile de date dintre UE și SUA", COM(2013) 846 final, 27.11.2013, precum și memorandumul conex „Restabilirea încrederii în fluxurile de date dintre UE și SUA – întrebări frecvente", MEMO/13/1059, 27.11.2013.

imediat și a accelerat discuțiile cu guvernul SUA, vizând să se asigure că un nou acord privind transferurile transatlantice de date cu caracter personal respectă pe deplin standardele stabilite de Curte. Prin urmare, orice astfel de acord trebuie să prevadă suficiente limitări, garanții și mecanisme de control judiciar încât să asigure protecția permanentă a datelor cu caracter personal ale cetățenilor UE, inclusiv în ceea ce privește eventualul acces al autorităților publice responsabile cu asigurarea respectării legilor și securitatea națională. În această perioadă de tranziție, la nivelul agenților economici s-au exprimat îngrijorări privind posibilitatea continuării transferurilor de date[6]. Prin urmare, este nevoie să se clarifice condițiile în care astfel de transferuri pot continua. Această situație a determinat Grupul de lucru instituit prin articolul 29 – organismul consultativ independent din care fac parte reprezentanții autorităților pentru protecția datelor din statele membre și Autoritatea Europeană pentru Protecția Datelor – să publice, pe 16 octombrie, o declarație[7] privind primele concluzii care pot fi trase în urma hotărârii. Printre altele, această declarație conține următoarele îndrumări privind transferurile de date:

- transferurile de date nu se mai pot întemeia pe decizia Comisiei privind sfera de siguranță, care a fost invalidată;

- între timp, clauzele contractuale standard (denumite în continuare și „CCS") și regulile corporatiste obligatorii (denumite în continuare și „RCO") pot fi utilizate ca bază pentru transferurile de date, deși Grupul de lucru instituit prin articolul 29 a afirmat că va continua să analizeze impactul hotărârii asupra acestor instrumente alternative.

Declarația a făcut, de asemenea, apel la statele membre și la instituțiile UE să se angajeze în discuții cu autoritățile din SUA în vederea găsirii unor soluții juridice și tehnice pentru transferurile de date. În opinia Grupului de lucru instituit prin articolul 29, negocierile pentru un nou acord privind sfera de siguranță ar putea contribui la identificarea acestor soluții.

Grupul de lucru instituit prin articolul 29 a anunțat că, dacă până la sfârșitul lunii ianuarie 2016 nu va fi identificată nicio soluție adecvată împreună cu autoritățile din SUA și dacă rezultatele evaluării instrumentelor alternative pentru transferul de date impun acest lucru, autoritățile pentru protecția datelor vor lua toate măsurile necesare și adecvate, inclusiv măsuri coordonate de asigurare a respectării legislației.

---

[6] Reprezentanții asociațiilor industriale au exprimat aceste îngrijorări, printre altele, cu ocazia unei reuniuni organizate de dl vicepreședinte Ansip, dna comisar Jourová și dl comisar Oettinger la scurt timp după pronunțarea hotărârii în cauza Schrems, și anume pe 14 octombrie. A se vedea *Daily news* (Știrile zilnice) din 14.10.2015 (MEX/15/5840). A se vedea, de asemenea „Scrisoarea deschisă privind executarea hotărârii CJUE în cauza C-362/14 Maximillian Schrems/Data Protection Commissioner", datată 13 octombrie 2015, adresată Președintelui Comisiei, Jean-Claude Juncker, și semnată de diverse asociații industriale și societăți din UE și SUA: http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=1045&PortalId=0&TabId=353.

[7] Declarația Grupului de lucru instituit prin articolul 29, disponibilă pe web la adresa: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf.

În fine, Grupul de lucru instituit prin articolul 29 a subliniat că autoritățile pentru protecția datelor, instituțiile UE, statele membre și agenții economici sunt răspunzători în comun pentru găsirea unor soluții sustenabile pentru executarea hotărârii Curții. În particular, grupul de lucru a făcut apel la agenții economici să aibă în vedere recurgerea la soluțiile juridice și tehnice necesare pentru a atenua eventualele riscuri la care se expun prin transferarea de date.

Prezenta comunicare nu aduce atingere competențelor și obligației autorităților pentru protecția datelor de a examina legalitatea acestor transferuri în condiții de independență deplină[8]. Comunicarea nu stabilește norme obligatorii și respectă integral competența instanțelor naționale de a interpreta dreptul aplicabil și, dacă este cazul, de a solicita Curții să pronunțe o hotărâre preliminară. Prezenta comunicare nu poate, de asemenea, să reprezinte temeiul niciunui drept legal și al niciunei pretenții de drept legal, individuale sau colective.

2. ALTERNATIVE PENTRU TRANSFERUL DATELOR CU CARACTER PERSONAL CĂTRE SUA

Normele privind transferurile internaționale de date prevăzute în Directiva 95/46/CE sunt bazate pe o distincție clară între transferurile către țări terțe care asigură un nivel de protecție adecvat (articolul 25 din directivă) și transferurile către țări terțe în privința cărora s-a constatat că nu asigură un nivel de protecție adecvat (articolul 26 din directivă).

Hotărârea pronunțată în cauza Schrems menționează condițiile în care Comisia poate constata, în temeiul articolului 25 alineatul (6) din Directiva 95/46/CE, că o țară terță asigură un nivel de protecție adecvat.

În cazul în care se constată că țara terță către care ar urma să fie exportate date cu caracter personal din UE nu asigură acest nivel de protecție adecvat, articolul 26 din Directiva 95/46/CE prevede o serie de condiții alternative în care transferul poate totuși să aibă loc. În particular, transferurile pot fi efectuate dacă entitatea responsabilă de stabilirea scopurilor și a mijloacelor de prelucrare a datelor cu caracter personal („operatorul”):

- oferă garanții suficiente, în sensul articolului 26 alineatul (2) din Directiva 95/46/CE, privind protecția vieții private și a drepturilor și libertăților fundamentale ale persoanelor, precum și privind exercitarea drepturilor respective. Astfel de garanții pot fi oferite în special prin clauze contractuale care au caracter obligatoriu pentru exportatorul și importatorul datelor (a se vedea secțiunile 2.1 și 2.2 de mai jos). În această categorie intră CCS publicate de Comisie și, în ceea ce privește transferurile dintre diversele entități ale unui grup corporativ multinațional, RCO autorizate de autoritățile pentru protecția datelor; sau

- se bazează pe una dintre derogările prevăzute în mod expres la articolul 26 alineatul (1) literele (a)-(f) din Directiva 95/46/CE (a se vedea secțiunea 2.3 de mai jos).

[8] A se vedea articolul 8 alineatul (3) din Carta drepturilor fundamentale și articolul 16 alineatul (2) din TFUE. Această independență a fost subliniată și de Curte în cadrul hotărârii pronunțate în cauza Schrems.

În comparație cu deciziile privind caracterul adecvat luate ca urmare a evaluării globale a sistemului unei anumite țări terțe, care se pot aplica în principiu tuturor transferurilor către sistemul respectiv, aceste baze alternative pentru efectuarea transferurilor au un domeniu de aplicare mai limitat (putând fi utilizate numai pentru anumite fluxuri de date) și o arie de acoperire mai mare (întrucât nu sunt neapărat limitate la o anumită țară). Acestea se aplică fluxurilor de date transferate de anumite entități care au hotărât să recurgă la una din posibilitățile prevăzute la articolul 26 din Directiva 95/46/CE. În plus, dacă efectuează transferuri pe astfel de baze și dacă, în consecință, nu se pot baza pe o decizie a Comisiei care constată că sistemul unei țări terțe este adecvat , exportatorii și importatorii de date au responsabilitatea de a se asigura că transferurile respectă cerințele prevăzute în directivă.

2.1. Soluții contractuale

După cum a evidențiat Grupul de lucru instituit prin articolul 29, pentru a oferi garanții suficiente în sensul articolului 26 alineatul (2) din Directiva 95/46/CE, clauzele contractuale „trebuie să compenseze în mod satisfăcător absența unui nivel general de protecție adecvată prin includerea elementelor de protecție esențiale care lipsesc din situația concretă în cauză”[9]. Pentru a facilita utilizarea acestor instrumente pentru transferurile internaționale, Comisia a aprobat, în conformitate cu articolul 26 alineatul (4) din directivă, patru seturi de CCS care se consideră că îndeplinesc cerințele de la articolul 26 alineatul (2) din directivă. Două dintre seturile de clauze-model se referă la transferurile între operatori[10], iar celelalte două seturi se referă la transferurile dintre un operator și o persoană împuternicită de către operator care acționează la instrucțiunile acestuia[11]. Fiecare set de clauze-model prevede obligațiile exportatorilor și ale importatorilor de date. Printre acestea se numără obligațiile referitoare la măsurile de securitate, informarea persoanei vizate în cazul transferării unor date sensibile, comunicarea către exportatorul de date a cererilor de acces formulate de autoritățile responsabile cu asigurarea respectării legilor din țara terță, orice situație de acces accidental sau neautorizat, drepturile persoanelor vizate la accesarea, corectarea și eliminarea datelor lor cu caracter personal și normele privind despăgubirile acordate persoanei vizate în cazul producerii unor daune cauzate de încălcarea de una dintre părți a CCS. Clauzele-model prevăd, de asemenea, obligația ca persona vizată din UE să aibă posibilitatea de a invoca în fața autorităților pentru protecția datelor și/sau a unei instanțe a statului membru în care este stabilit exportatorul datelor drepturile care derivă din clauzele contractuale, în calitate de

[9] A se vedea Grupul de lucru instituit prin articolul 29, „Transferul datelor cu caracter personal către țări terțe: aplicarea articolelor 25 și 26 din directiva UE privind protecția datelor”, (WP 12), 24 iulie 1998, p. 16.

[10] Decizia 2001/497/CE a Comisiei din 15 iunie 2001 privind clauzele contractuale standard pentru transferul de date cu caracter personal către țările terțe în temeiul Directivei 95/46/CE, JO L 181, 4.7.2001, p. 19 și Decizia 2004/915/CE a Comisiei 27 decembrie 2004 de modificare a Deciziei 2001/497/CE privind introducerea unui set alternativ de clauze contractuale standard pentru transferul de date cu caracter personal către țări terțe, JO L 385, 29.12.2004, p. 74.

[11] Decizia 2002/16/CE a Comisiei din 27 decembrie 2001 privind clauzele contractuale tip pentru transferul de date cu caracter personal către procesatorii de date stabiliți în țări terțe, în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului, JO L 6, 10.1.2002, p. 52 și Decizia 2010/87/UE a Comisiei din 5 februarie 2010 privind clauzele contractuale tip pentru transferul de date cu caracter personal către persoanele împuternicite de către operator stabilite în țări terțe în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului, JO L 39, 12.2.2010, p. 5. Prima decizie, care a fost abrogată de a doua, se aplică numai contractelor încheiate înainte de 15 mai 2010.

beneficiar terț[12]. Menționarea acestor drepturi și obligații în clauzele contractuale este necesară deoarece, spre deosebire de situația în care Comisia a formulat o constatare a caracterului adecvat, nu se poate prezuma că importatorul datelor din țara terță face obiectul unui sistem de supraveghere adecvat și al aplicării normelor în materie de protecție a datelor.

Întrucât deciziile Comisiei sunt obligatorii în toate elementele lor în statele membre, încorporarea CCS într-un contract înseamnă că autoritățile naționale au în principiu obligația de a accepta clauzele respective. Prin urmare, autoritățile în cauză nu pot refuza transferul datelor într-o țară terță dacă singura lor motivație este faptul că aceste CCS nu ar oferi suficiente garanții. Aceasta nu aduce atingere competenței acestor autorități de a examina clauzele respective în lumina cerințelor formulate de Curte în hotărârea pronunțată în cauza Schrems. Dacă există dubii, autoritățile respective ar trebui să sesizeze o instanță națională, care la rândul său poate solicita Curții de Justiție să pronunțe o hotărâre preliminară. Deși legislațiile de transpunere a Directivei 95/45/CE ale celor mai multe state membre nu prevăd obligația unui autorizații naționale prealabile pentru transfer, în anumite state membre există un sistem de notificare și/sau preautorizare pentru utilizarea CCS. În astfel de cazuri, autoritățile naționale pentru protecția datelor trebuie să compare clauzele contractului în cauză cu CCS și să verifice că nu s-a efectuat nicio modificare[13]. Dacă clauzele au fost utilizate fără a fi fost schimbate[14], autorizația se acordă în principiu[15] automat[16]. După cum se detaliază mai jos (a se vedea secțiunea 2.4), aceasta nu aduce atingere măsurilor suplimentare pe care exportatorul datelor ar putea fi nevoit să le ia, în special în urma primirii de la importatorul datelor a unor informații privind modificări intervenite la nivelul sistemului juridic al țării terțe care ar putea împiedica importatorul datelor să își îndeplinească obligațiile derivate din contract. În procesul de aplicare a CCS, atât exportatorii de date, cât și – prin faptul că se angajează să respecte contractul – importatorii de date se supun supravegherii din partea autorităților pentru protecția datelor.

---

12 A se vedea, de exemplu, considerentul 6 din Decizia 2004/915/CE a Comisiei și clauza V din anexa la aceasta; clauza 7 din anexa la Decizia 2010/87/UE a Comisiei.

13 Ar trebui remarcat că propunerea de regulament general privind protecția datelor [COM(2012) 11 final] prevede că, pentru transferurile efectuate pe baza CCS sau a RCO, în măsura în care acestea au fost adoptate de Comisie sau în conformitate cu mecanismul pentru asigurarea consecvenței avut în vedere, nu este nevoie de o autorizare suplimentară.

14 Utilizarea unor CCS nu împiedică însă părțile să convină în privința adăugării altor clauze, cu condiția ca acestea să nu intre în mod direct sau indirect în contradicție cu clauzele aprobate de Comisie și să nu aducă atingere drepturilor sau libertăților fundamentale ale persoanelor vizate. A se vedea: Comisia Europeană, „Întrebări frecvente privind transferurile de date cu caracter personal dinspre UE/SEE către țări terțe" (FAQ B.1.9), p. 28 (document disponibil pe web la adresa http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf).

15 Dacă o autoritate pentru protecția datelor are îndoieli în ceea ce privește compatibilitatea dintre CCS și dispozițiile directivei, aceasta ar trebui să sesizeze o instanță națională în privința acestei chestiuni, care poate apoi să solicite Curții să pronunțe o hotărâre preliminară (a se vedea punctele 51, 52, 64 și 65 din hotărârea pronunțată în cauza Schrems).

16 Grupul de lucru instituit prin articolul 29 a stabilit o procedură specifică privind cooperarea dintre autoritățile pentru protecția datelor în vederea aprobării clauzelor contractuale pe care o societate își propune să le utilizeze în diverse state membre. A se vedea: Grupul de lucru instituit prin articolul 29, „Document de lucru privind stabilirea unei proceduri de cooperare pentru emiterea de opinii comune referitoare la clauzele contractuale considerate conforme cu clauzele-model ale CE" (WP 226), 26 noiembrie 2014. A se vedea, de asemenea, clauza VII din anexa la Decizia 2004/915/CE a Comisiei și clauza 10 din anexa la Decizia 2010/87/UE a Comisiei.

Adoptarea unor CCS nu împiedică societățile să se bazeze pe alte instrumente, cum ar fi înțelegerile contractuale ad-hoc, pentru a demonstra că transferurile sunt efectuate cu suficiente garanții în sensul articolului 26 alineatul (2) din Directiva 95/46/CE. În temeiul articolului 26 alineatul (2) din directivă, acestea trebuie aprobate individual de autoritățile naționale. Anumite autorități pentru protecția datelor au elaborat orientări în acest sens, inclusiv sub forma unor contracte standardizate sau a unor norme detaliate care să fie respectate la redactarea clauzelor privind transferurile de date. Majoritatea contractelor utilizate în prezent de societăți pentru efectuarea de transferuri internaționale de date sunt însă bazate pe CCS aprobate de Comisie[17].

2.2. Transferurile intragrup

Pentru transferul de date din UE către filiale situate în afara UE cu respectarea obligațiilor prevăzute la articolul 26 alineatul (2) din Directiva 95/46/CE, o societate multinațională poate adopta RCO. Acest tip de instrument reprezintă o bază doar pentru transferurile efectuate în interiorul unui grup corporativ.

Astfel, utilizarea RCO permite ca datele cu caracter personal să circule liber între diversele entități din întreaga lume ale unui grup corporativ, eliminând nevoia existenței unor înțelegeri contractuale între toate entitățile corporative și garantând în același timp că în întregul grup se respectă același nivel ridicat de protecție a datelor cu caracter personal, asigurat prin intermediul unui set unic de norme obligatorii și aplicabile. Existența unui set unic de norme face ca sistemul să fie mai simplu și mai eficace, ceea ce ușurează aplicarea sa de către personal și înțelegerea de către persoanele vizate. Pentru a ajuta societățile la redactarea de RCO, Grupul de lucru instituit prin articolul 29 a detaliat cerințele de fond și cerințele procedurale pe care trebuie să le respecte RCO bazate pe standardele în materie de protecție a datelor din UE[18]. Din prima categorie de cerințe fac parte, de exemplu, limitarea scopului, securitatea prelucrărilor, transparența informațiilor pentru persoanele vizate, restricțiile asupra transferării în continuare a datelor în afara grupului și drepturile individuale de acces, corectare și opoziție. A doua categorie include, de exemplu, auditurile, monitorizarea conformării, gestionarea reclamațiilor, cooperarea cu autoritățile pentru protecția datelor, responsabilitatea și jurisdicția. Aceste norme sunt obligatorii nu doar pentru membrii grupului corporativ ci, la fel ca în cazul CCS, sunt aplicabile și în UE: persoanele ale căror date sunt prelucrate de o entitate dintr-un grup au dreptul, în calitate de beneficiari terți, să obțină respectarea RCO prin depunerea unei plângeri la autoritatea pentru protecția datelor și prin sesizarea instanțelor dintr-un stat membru. În plus, prin RCO trebuie desemnată o entitate din

[17] A se vedea: Grupul de lucru instituit prin articolul 29, „Document de lucru privind stabilirea unei proceduri de cooperare pentru emiterea de opinii comune referitoare la clauzele contractuale considerate conforme cu clauzele-model ale CE” (WP 226), 26 noiembrie 2014, p. 2.

[18] A se vedea: Grupul de lucru instituit prin articolul 29, „Document de lucru de stabilire a unui tabel cu elementele și principiile care trebuie să facă parte din regulile corporatiste obligatorii” (WP 153), 24 iunie 2008; „Document de lucru de stabilire a unui cadru privind structura regulilor corporatiste obligatorii” (WP 154), 24 iunie 2008 și „Document de lucru privind întrebările frecvente referitoare la regulile corporatiste obligatorii” (WP 155), 24 iunie 2008.

UE care acceptă să fie răspunzătoare pentru încălcarea normelor de către orice membru al grupului din afara UE care are obligația de a respecta aceste norme.

În legile de transpunere a directivei din majoritatea statelor membre, transferurile de date pe baza RCO trebuie să fie autorizate de autoritățile pentru protecția datelor în fiecare stat membru din care o societate multinațională intenționează să transfere date. Pentru a facilita și a accelera acest proces, precum și pentru a reduce sarcina administrativă suportată de solicitanți, Grupul de lucru instituit în temeiul articolului 29 a elaborat un formular-tip de cerere[19] și o procedură de cooperare specifică între autoritățile pentru protecția datelor implicate[20], care include desemnarea unei autorități principale responsabile cu gestionarea procedurii de aprobare.

2.3. Derogări

În absența unei decizii privind caracterul adecvat adoptată în temeiul articolului 25 alineatul (6) din Directiva 95/46/CE și chiar dacă nu se utilizează CCS și/sau RCO, datele cu caracter personal pot fi totuși transferate către entități stabilite într-o țară terță în măsura în care se aplică una dintre derogările alternative prevăzute la articolul 26 alineatul (1) din Directiva 95/46/CE[21]:

- persoana vizată și-a dat consimțământul ferm la transferul avut în vedere;

- transferul este necesar pentru executarea unui contract între persoana vizată și operator sau pentru aducerea la îndeplinire a măsurilor precontractuale luate ca răspuns la cererea persoanei vizate;

- transferul este necesar pentru încheierea sau executarea unui contract încheiat sau care urmează să fie încheiat în interesul persoanei vizate între operator și un terț;

- transferul este necesar sau impus prin lege pentru apărarea unui interes public important[22] sau pentru constatarea, exercitarea sau apărarea unui drept în justiție;

---

19 Grupul de lucru instituit prin articolul 29, „Cerere-tip pentru aprobarea regulilor corporatiste obligatorii pentru transferul datelor cu caracter personal” (WP 133), 10 ianuarie 2007.

20 Grupul de lucru instituit prin articolul 29, „Document de lucru de stabilire a unei proceduri de cooperare pentru emiterea de opinii comune privind garanțiile adecvate rezultate din regulile corporatiste obligatorii” (WP 107), 14 aprilie 2005.

21 După cum a subliniat Grupul de lucru instituit prin articolul 29, în măsura în care alte dispoziții ale Directivei 95/46/CE conțin cerințe suplimentare relevante pentru utilizarea acestor derogări (de exemplu limitările prevăzute la articolul 8 în ceea ce privește prelucrarea datelor sensibile), acestea trebuie să fie respectate. A se vedea: Grupul de lucru instituit prin articolul 29, „Document de lucru privind o interpretare comună a articolului 26 alineatul (1) din Directiva 95/46/CE din 24 octombrie 1995” (WP 114), 25 noiembrie 2005, p. 8. A se vedea, de asemenea: Comisia Europeană, „Întrebări frecvente privind transferurile de date cu caracter personal dinspre UE/SEE către țări terțe” (FAQ D.2), p. 50.

22 Acesta se poate referi, de exemplu, la transferurile de date între administrațiile fiscale sau vamale sau între serviciile competente în materie de securitate socială (a se vedea considerentul 58 din Directiva 95/46/CE). Transferurile dintre organismele de supraveghere din sectorul serviciilor financiare pot beneficia, la rândul lor, de derogări. A se vedea: Grupul de lucru instituit prin articolul 29, „Document de lucru: transferurile de date cu caracter personal către țările terțe: aplicarea articolelor 25 și 26 din directiva UE privind protecția datelor”, (WP 12), 24 iulie 1998, p. 25.

– transferul este necesar pentru apărarea intereselor vitale ale persoanei vizate;

– transferul este făcut dintr-un registru public care, în conformitate cu dispozițiile legale sau de reglementare, este destinat informării publicului și este deschis spre consultare publicului sau oricărei persoane care demonstrează un interes legitim, în măsura în care se îndeplinesc condițiile prevăzute prin lege pentru consultări în cazurile particulare.

Aceste situații reprezintă derogări de la interdicția generală de a transfera date cu caracter personal către entități stabilite într-o țară terță în absența unui nivel de protecție adecvat. În astfel de cazuri exportatorul datelor nu trebuie să se asigure că importatorul va garanta un nivel de protecție adecvat și, de obicei, nu trebuie să obțină de la autoritățile naționale relevante o autorizație prealabilă pentru transfer. Cu toate acestea, din cauza caracterului excepțional al acestor derogări, Grupul de lucru instituit prin articolul 29 consideră că aceste derogări trebuie să fie interpretate în mod strict[23].

Grupul de lucru instituit prin articolul 29 a publicat mai multe documente de orientare fără caracter obligatoriu privind aplicarea articolului 26 alineatul (1) din Directiva 95/46/CE[24]. Printre acestea se numără o serie de reguli privind cele mai bune practici, care sunt destinate să ofere autorităților pentru protecția datelor orientări privind măsurile de asigurare a respectării legislației[25]. În particular, grupul de lucru recomandă ca transferurile de date cu caracter personal care ar putea fi calificate drept repetate, masive sau structurale să fie efectuate cu condiția oferirii unor garanții suficiente și, dacă se poate, utilizând un cadru juridic specific, cum ar fi CCS sau RCO[26].

În prezenta comunicare, Comisia va trata numai derogările care par deosebit de relevante pentru transferurile comerciale în urma hotărârii prin care a fost invalidată decizia privind sfera de siguranță.

---

[23] Grupul de lucru instituit prin articolul 29, „Document de lucru privind o interpretare comună a articolului 26 alineatul (1) din Directiva 95/46/CE din 24 octombrie 1995” (WP 114), 25 noiembrie 2005, p. 7 și 17.

[24] Grupul de lucru instituit prin articolul 29, „Document de lucru: transferurile de date cu caracter personal către țările terțe: aplicarea articolelor 25 și 26 din directiva UE privind protecția datelor” (WP 12), 24 iulie 1998; „Document de lucru privind o interpretare comună a articolului 26 alineatul (1) din Directiva 95/46/CE din 24 octombrie 1995” (WP 114), 25 noiembrie 2005. A se vedea, de asemenea: Comisia Europeană, „Întrebări frecvente privind transferurile de date cu caracter personal dinspre UE/SEE către țări terțe” (FAQ D.1-D.9), p. 48-54.

[25] Grupul de lucru instituit prin articolul 29, „Document de lucru privind o interpretare comună a articolului 26 alineatul (1) din Directiva 95/46/CE din 24 octombrie 1995” (WP 114), 25 noiembrie 2005, p. 8-10.

[26] Grupul de lucru instituit prin articolul 29, „Document de lucru privind o interpretare comună a articolului 26 alineatul (1) din Directiva 95/46/CE din 24 octombrie 1995” (WP 114), 25 noiembrie 2005, p. 9. Potrivit grupului de lucru, transferurile masive sau repetate pot fi efectuate pe baza unei derogări numai dacă este imposibil din punct de vedere practic să se recurgă la CCS sau RCO și dacă riscurile la adresa persoanelor vizate sunt mici (de exemplu în cazul transferurilor internaționale de bani). A se vedea, de asemenea: Comisia Europeană, „Întrebări frecvente privind transferurile de date cu caracter personal dinspre UE/SEE către țări terțe” (FAQ D.1), p. 49.

2.3.1. Transferurile necesare pentru executarea unui contract încheiat sau pentru aducerea la îndeplinire a măsurilor precontractuale luate ca răspuns la cererea persoanei vizate [articolul 26 alineatul (1) litera (b)]

Această derogare s-ar putea aplica, de exemplu, în cazul unei rezervări la hotel sau când informații privind plata sunt transmise către o țară terță în vederea efectuării unui virament bancar. Cu toate acestea, Grupul de lucru instituit prin articolul 29 consideră că în fiecare astfel de caz trebuie să existe o conexiune strânsă și de fond și o legătură directă și obiectivă între persoana vizată și scopurile contractului sau ale măsurii precontractuale (testul necesității)[27]. De asemenea, derogarea nu poate fi aplicată transferurilor de informații suplimentare care nu sunt necesare pentru îndeplinirea scopurilor transferului și nici transferurilor care au alt scop decât executarea contractului (de exemplu marketingului post-vânzare)[28]. În ceea ce privește măsurile precontractuale, Grupul de lucru instituit prin articolul 29 este de părere că ar fi incluse numai contactele inițiate de persoana vizată (de exemplu printr-o cerere de informații referitoare la un anumit serviciu), nu și cele care sunt urmarea unor abordări în scopuri de marketing efectuate de operatorul de date[29].

2.3.2. Transferuri necesare pentru încheierea sau executarea unui contract încheiat sau care urmează să fie încheiat în interesul persoanei vizate între operator și un terț [articolul 26 alineatul (1) litera (c)]

Această derogare s-ar putea aplica, de exemplu, atunci când persoana vizată este beneficiara unui virament bancar internațional sau atunci când o agenție de voiaj transmite unei companii aeriene detaliile unei rezervări a unui zbor. Și în această situație se aplică testul necesității, care în acest caz impune să existe o legătură strânsă și de fond între interesul persoanei vizate și scopul contractului.

2.3.3. Transferuri necesare sau impuse prin lege pentru constatarea, exercitarea sau apărarea unui drept în justiție [articolul 26 alineatul (1) litera (d)]

Această derogare s-ar putea aplica, de exemplu, dacă o societate are nevoie să transfere date pentru se apăra în justiție sau pentru a sesiza o instanță sau o autoritate publică în vederea apărării unui drept. La fel ca în cazul celor două derogări de mai sus, și aceasta este supusă testului necesității[30]: ar trebui să existe o conexiune strânsă cu proceduri contencioase sau judiciare (inclusiv administrative).

---

[27] Grupul de lucru instituit prin articolul 29, „Document de lucru privind o interpretare comună a articolului 26 alineatul (1) din Directiva 95/46/CE din 24 octombrie 1995” (WP 114), 25 noiembrie 2005, p. 13. A se vedea, de asemenea, „Avizul 6/2002 privind transmiterea informațiilor din listele de pasageri și a altor date de către liniile aeriene Statelor Unite ale Americii” (WP 66), 24 octombrie 2002.

[28] Grupul de lucru instituit prin articolul 29, „Document de lucru: transferurile de date cu caracter personal către țările terțe: aplicarea articolelor 25 și 26 din directiva UE privind protecția datelor”, (WP 12), 24 iulie 1998, p. 24; „Document de lucru privind o interpretare comună a articolului 26 alineatul (1) din Directiva 95/46/CE din 24 octombrie 1995” (WP 114), 25 noiembrie 2005, p. 13.

[29] Grupul de lucru instituit prin articolul 29, „Document de lucru: transferurile de date cu caracter personal către țările terțe: aplicarea articolelor 25 și 26 din directiva UE privind protecția datelor”, (WP 12), 24 iulie 1998, p. 24.

[30] Grupul de lucru instituit prin articolul 29, „Document de lucru privind o interpretare comună a articolului 26 alineatul (1) din Directiva 95/46/CE din 24 octombrie 1995” (WP 114), 25 noiembrie 2005, p. 15. De

Potrivit Grupului de lucru instituit prin articolul 29, derogarea poate fi aplicată numai dacă au fost respectate normele internaționale privind cooperarea în materie penală sau civilă aplicabile tipului de transfer în cauză, în special cele care derivă din dispozițiile Convenției de la Haga din 18 martie 1970 (Convenția privind obținerea de probe)[31].

2.3.4. Consimțământul prealabil ferm al persoanei vizate la transferul avut în vedere [articolul 26 alineatul (1) litera (a)]

Consimțământul poate fi utilizat ca temei pentru transferurile de date, însă trebuie avute în vedere o serie de aspecte. Întrucât consimțământul trebuie dat la transferul „avut în vedere", aceasta implică un consimțământ prealabil pentru un anumit transfer (sau o anumită categorie de transferuri). Dacă procedura se desfășoară online, Grupul de lucru instituit prin articolul 29 recomandă utilizarea căsuțelor care trebuie bifate (și nu a căsuțelor bifate din oficiu)[32]. Întrucât consimțământul trebuie să fie ferm, dacă există vreo îndoială că acesta a fost efectiv exprimat, derogarea ar înceta să mai fie aplicabilă. Aceasta înseamnă că multe situații în care consimțământul este în cel mai bun caz subînțeles (de exemplu din cauză că persoanei i s-a adus la cunoștință transferul, iar aceasta nu a exprimat obiecții) nu ar îndeplini condițiile necesare. Derogarea poate fi, în schimb, utilizată în cazurile în care entitatea care efectuează transferul a avut un contact direct cu persoana vizată, informațiile necesare pot fi furnizate cu ușurință și s-a obținut un consimțământ ferm[33].

În plus, în conformitate cu articolul 2 litera (h) din Directiva 95/46/CE, consimțământul trebuie să fie liber manifestat, specific și informat. Potrivit Grupului de lucru instituit prin articolul 29, prima dintre aceste cerințe înseamnă că orice „presiune" poate conduce la invalidarea consimțământului. Acest lucru este deosebit de relevant în contextul relațiilor de muncă, în care raportul de subordonare și dependența inerentă a angajatului de angajator va pune de obicei sub semnul întrebării valabilitatea consimțământului[34]. Într-o perspectivă mai

---

exemplu, această derogare nu poate fi utilizată în contextul unor relații de muncă pentru a transfera dosarele tuturor angajaților către societatea-mamă din grup, dacă aceasta este stabilită într-o țară terță, iar justificarea ar fi eventualele proceduri juridice viitoare.

31 Convenția de la Haga privind obținerea de probe în străinătate în materie civilă sau comercială, *deschisă spre semnare* la 18 martie 1970, 23 U.S.T. 2555, 847 U.N.T.S. 241. Această convenție se referă, de exemplu, la utilizarea elementelor de probă în etapa anterioară procesului sau la cererile formulate de autoritățile judiciare dintr-un stat către autoritățile competente dintr-un alt stat vizând obținerea de dovezi care ar urma să fie utilizate în proceduri judiciare din statul care a formulat cererea.

32 Grupul de lucru instituit prin articolul 29, „Document de lucru privind o interpretare comună a articolului 26 alineatul (1) din Directiva 95/46/CE din 24 octombrie 1995" (WP 114), 25 noiembrie 2005, p.10, cu trimitere la „Avizul 5/2004 privind comunicările de marketing direct nesolicitate care intră sub incidența articolului 13 din Directiva 2002/58/CE" (WP, 90), 27 februarie 2004, punctul 3.2.

33 Grupul de lucru instituit prin articolul 29, „Document de lucru: transferurile de date cu caracter personal către țările terțe: aplicarea articolelor 25 și 26 din directiva UE privind protecția datelor", (WP 12), 24 iulie 1998, p. 24.

34 Grupul de lucru instituit prin articolul 29, „Avizul 8/2001 privind prelucrarea datelor cu caracter personal în contextul relațiilor de muncă" (WP 48), 13 septembrie 2001, p. 3, 23 și 26. Potrivit grupului de lucru, ar trebui să se recurgă la consimțământ numai în cazurile în care lucrătorul are realmente posibilitatea unei alegeri libere și, prin urmare, poate să își retragă ulterior consimțământul fără să existe consecințe negative. A se vedea, de asemenea: Grupul de lucru instituit prin articolul 29, „Document de lucru privind o

generală, consimțământul dat de o persoană vizată care nu a avut ocazia să facă realmente o alegere sau care a fost pusă în fața unui fapt împlinit nu poate fi considerat valid[35].

Este deosebit de important ca persoanei vizate să îi fie comunicate în prealabil în mod adecvat faptul că datele pot fi transferate în afara UE, țara terță de destinație și condițiile transferului (scopul acestuia, identitatea destinatarului sau a destinatarilor și detalii referitoare la aceștia etc.). Aceste informații ar trebui să se refere în mod specific la riscul ca datele persoanei vizate să fie transferate către o țară terță care nu asigură o protecție adecvată[36]. În plus, după cum a subliniat Grupul de lucru instituit prin articolul 29, retragerea consimțământului exprimat de persoana vizată nu acționează retroactiv, dar ar trebui, în principiu, să împiedice orice prelucrare ulterioară a datelor cu caracter personal[37]. Având în vedere aceste limitări, potrivit opiniei Grupului de lucru instituit prin articolul 29, consimțământul nu este susceptibil să constituie un cadru adecvat pe termen lung pentru operatorii de date în cazul transferurilor structurale[38].

2.4. Rezumat privind alternativele pentru transferul datelor cu caracter personal

Din elementele prezentate mai sus rezultă că o companie poate utiliza o serie de instrumente alternative pentru efectuarea unor transferuri internaționale de date către țări terțe care se consideră că nu asigură un nivel de protecție adecvat în sensul articolului 25 alineatul (2) din Directiva 95/46/CE. În urma hotărârii pronunțate în cauza Schrems, Grupul de lucru instituit prin articolul 29 a clarificat în special faptul că CCS și RCO pot fi utilizate pentru transferul de date către SUA, însă grupul de lucru își continuă evaluarea și nu aduce atingere competențelor autorităților pentru protecția datelor de a investiga cazuri concrete[39]. La rândul lor, agenții economici au reacționat în diverse moduri la hotărârea Curții, inclusiv prin recurgerea la aceste instrumente alternative ca bază pentru transferurile de date[40].

---

interpretare comună a articolului 26 alineatul (1) din Directiva 95/46/CE din 24 octombrie 1995” (WP 114), 25 noiembrie 2005, p. 11.

35 Grupul de lucru instituit prin articolul 29, „Document de lucru privind o interpretare comună a articolului 26 alineatul (1) din Directiva 95/46/CE din 24 octombrie 1995” (WP 114), 25 noiembrie 2005, p. 11. A se vedea, de asemenea, „Avizul 6/2002 privind transmiterea informațiilor din listele de pasageri și a altor date de către liniile aeriene Statelor Unite ale Americii” (WP 66), 24 octombrie 2002.

36 Grupul de lucru instituit prin articolul 29, „Document de lucru: transferurile de date cu caracter personal către țările terțe: aplicarea articolelor 25 și 26 din directiva UE privind protecția datelor”, (WP 12), 24 iulie 1998, p. 24.

37 Grupul de lucru instituit prin articolul 29, „Avizul 15/2011 privind definiția consimțământului” (WP 187), 13 iulie 2011, p. 9.

38 Grupul de lucru instituit prin articolul 29, „Document de lucru privind o interpretare comună a articolului 26 alineatul (1) din Directiva 95/46/CE din 24 octombrie 1995” (WP 114), 25 noiembrie 2005, p. 11.

39 A se vedea declarația Grupului de lucru instituit prin articolul 29 din 16 octombrie 2015 (nota de subsol 8 de mai sus).

40 O serie de societăți multinaționale au declarat că vor utiliza instrumente alternative ca bază pentru transferurile de date către SUA. A se vedea, de exemplu, declarațiile date de societățile Microsoft (http://blogs.microsoft.com/on-the-issues/2015/10/06/a-message-to-our-customers-about-eu-us-safe-harbor/) și Salesforce (http://www.salesforce.com/company/privacy/data-processing-addendum-faq.jsp). Alte societăți din SUA, cum ar fi Oracle, au declarat că le oferă clienților serviciilor de tip *cloud* posibilitatea de a-și stoca datele în Europa, astfel încât acestea să nu fie trimise în altă parte pentru stocare: http://www.irishtimes.com/business/technology/oracle-keeps-european-data-within-its-eu-based-data-centres-1.2408505?mode=print&ot=example.AjaxPageLayout.ot.

Trebuie însă subliniate două condiții importante. Mai întâi, ar trebui reamintit că, indiferent de temeiul juridic la care se recurge, transferurile către o țară terță pot fi efectuate în mod legal numai dacă datele în cauză au fost colectate și prelucrate de operatorul de date stabilit în UE în conformitate cu legile în vigoare de transpunere la nivel național a Directivei 95/46/CE. Directiva prevede în mod expres faptul că activitatea de prelucrare anterioară transferului, în aceeași măsură ca și transferul însuși, trebuie să se conformeze pe deplin normelor adoptate de statele membre în temeiul celorlalte dispoziții ale directivei[41]. În al doilea rând, în absența constatării de către Comisie a caracterului adecvat, le revine operatorilor de date responsabilitatea de a se asigura că transferurile de date sunt însoțite de garanții suficiente în conformitate cu articolul 26 alineatul (2) din directivă. Această evaluare trebuie să fie efectuată ținând cont de toate împrejurările relevante pentru transferul în cauză. În particular, atât în CCS, cât și în RCO se prevede că, dacă importatorul datelor are motive să creadă că legislația aplicabilă în țara de destinație îl poate împiedica să își îndeplinească obligațiile, acesta trebuie să informeze imediat exportatorul datelor din UE. Într-o astfel de situație, îi revine exportatorului responsabilitatea de a avea în vederea luarea măsurilor adecvate necesare pentru protecția datelor cu caracter personal[42]. Acestea pot include măsuri tehnice, organizaționale, referitoare la modelul de afaceri sau legale[43], mergând până la posibilitatea de a suspenda transferul datelor sau de a rezilia contractul. Exportatorii de date trebuie ca, ținând cont de toate împrejurările în care se desfășoară transferul, să asigure garanții suplimentare, în completarea celor conferite de temeiul juridic aplicabil, pentru ca transferul să îndeplinească cerințele de la articolul 26 alineatul (2) din directivă.

În ultimă instanță, respectarea acestor cerințe va fi evaluată de autoritățile pentru protecția datelor de la caz la caz în cadrul exercitării funcțiilor lor de supraveghere și asigurare a respectării legislației, inclusiv în contextul aprobării înțelegerilor contractuale și a RCO sau ca reacție la plângeri individuale. Deși anumite autorități pentru protecția datelor și-au exprimat îndoieli privind posibilitatea utilizării unor instrumente de transfer precum CCS și RCO pentru fluxurile de date transatlantice[44], Grupul de lucru instituit prin articolul 29 a anunțat, în

---

41 A se vedea considerentul 60 și articolul 25 alineatul (1) din Directiva 95/46/CE.

42 A se vedea, de exemplu, clauza 5 din anexa la Decizia 2010/87/UE a Comisiei și Grupul de lucru instituit prin articolul 29 „Document de lucru pentru stabilirea unui cadru privind structura regulilor corporatiste obligatorii" (WP 154), 24 iunie 2008, p. 8.

43 A se vedea, de exemplu, orientările publicate de Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA): https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf.

44 A se vedea, de exemplu, documentul de poziție publicat de Conferința privind protecția datelor a autorităților pentru protecția datelor din Germania de la nivel federal și statal din 26.10.2015: https://www.datenschutz.hessen.de/ft-europa.htm#entry4521. Subliniind faptul că hotărârea pronunțată în cauza Schrems conține „cerințe de fond stricte", pe care atât Comisia, cât și autoritățile pentru protecția datelor trebuie să le respecte, documentul de poziție precizează că autoritățile pentru protecția datelor din Germania vor evalua legalitatea transferurilor de date bazate pe instrumente alternative (CCS și RCO) și nu vor mai acorda noi autorizații pentru utilizarea acestor instrumente. În paralel, anumite autorități pentru protecția datelor din Germania au emis avertismente clare în care se preciza că instrumentele alternative de transfer fac obiectul unei examinări juridice. A se vedea, de exemplu, documentele de poziție publicate de autoritățile pentru protecția datelor din Schleswig-Holstein: https://www.datenschutzzentrum.de/artikel/981-ULD-Position-Paper-on-the-Judgment-of-the-Court-of-Justice-of-the-European-Union-of-6-October-2015,-C-36214.html și din Rheinland-Pfalz: https://www.datenschutz.rlp.de/de/aktuell/2015/images/20151026_Folgerungen_des_LfDI_RLP_zum_EuGH-Urteil_Safe_Harbor.pdf.

declarația publicată în urma hotărârii pronunțate în cauza Schrems, că va continua analiza impactului hotărârii asupra altor instrumente de transfer[45]. Aceasta nu aduce atingere competențelor autorităților pentru protecția datelor de a investiga anumite cazuri și de a-și exercita competențele pentru protejarea cetățenilor.

3. CONSECINȚELE HOTĂRÂRII PRONUNȚATE ÎN CAUZA SCHREMS ASUPRA DECIZIILOR PRIVIND CARACTERUL ADECVAT

În hotărârea sa, Curtea de Justiție nu pune sub semnul întrebării competența Comisiei, conferită prin articolul 25 alineatul (6) din Directiva 95/46/CE, de a constata că o țară terță asigură un nivel de protecție adecvat, cu condiția să fie respectate cerințele stabilite de Curte. În acord cu aceste cerințe, propunerea de regulament general privind protecția datelor din 2012[46], destinat să înlocuiască Directiva 95/46/CE, clarifică și detaliază condițiile în care pot fi adoptate deciziile privind caracterul adecvat. În hotărârea pronunțată în cauza Schrems, Curtea a precizat, de asemenea, că o decizie privind caracterul adecvat adoptată de Comisie este obligatorie pentru toate statele membre și organele acestora, inclusiv pentru autoritățile pentru protecția datelor, până când este retrasă, anulată sau invalidată de Curtea de Justiție – singura care are competențe în această privință. Autoritățile pentru protecția datelor își păstrează competența de a examina plângerile, în sensul articolului 28 alineatul (4) din Directiva 95/46/CE, referitoare la conformarea procesului de transfer al datelor la cerințele prevăzute în directivă (astfel cum a fost interpretată de Curtea de Justiție), dar nu au dreptul de a pronunța o constatare definitivă. Statele membre trebuie în schimb să prevadă posibilitatea sesizării unei instanțe naționale în privința cauzei respective, ceea ce poate antrena implicarea Curții de Justiție, căreia i se poate solicita să pronunțe o hotărâre preliminară în temeiul articolului 267 din Tratatul privind funcționarea Uniunii Europene (TFUE).

În plus, Curtea de Justiție a confirmat în mod expres că utilizarea de către o țară terță a unui sistem de autocertificare (cum este cazul principiilor sferei de siguranță privind protecția vieții private) nu exclude o constatare a caracterului adecvat realizată în temeiul articolului 25 alineatul (6) din Directiva 95/46/CE, cu condiția să existe mecanisme de detecție și supraveghere eficace care să facă posibile în practică identificarea și sancționarea oricăror încălcări ale normelor privind protecția datelor.

---

45 A se vedea declarația Grupului de lucru instituit prin articolul 29 din 16 octombrie 2015 (nota de subsol 8 de mai sus).

46 Comisia Europeană, Propunere 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). A se vedea, de asemenea, Rezoluția legislativă a Parlamentului European din 12 martie 2014 referitoare la 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) 0011 – C7-0025/2012 – 2012/0011(COD); Consiliul, Propunere 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), Pregătirea unei abordări generale, 9565/15. Această propunere se află actualmente în etapa finală a procesului legislativ.

Având în vedere faptul că decizia privind sfera de siguranță nu conține suficiente constatări în această privință, Curtea de Justiția a invalidat-o. Astfel, este clar că transferurile de date dintre UE și Statele Unite ale Americii nu mai pot fi efectuate în temeiul acelei decizii, cu alte cuvinte numai prin invocarea respectării principiilor sferei de siguranță privind protecția vieții private. Întrucât transferurile datelor către o țară terță care nu asigură un nivel de protecție adecvat [sau care nu a făcut cel puțin obiectul unei decizii a Comisiei adoptate în temeiul articolului 25 alineatul (6) din Directiva 95/46/CE] sunt în principiu interzise[47], aceste transferuri vor fi legale numai dacă exportatorul datelor se poate baza pe unul din instrumentele alternative descrise mai sus, în secțiunea 2. În absența unei decizii privind caracterul adecvat, este responsabilitatea exportatorului de date să se asigure – sub controlul autorității pentru protecția datelor – că sunt îndeplinite, în ceea ce privește respectivul transfer de date, condițiile pentru a recurge la (unul din) aceste instrumente.

Domeniul de aplicare al hotărârii Curții este limitat la decizia Comisiei privind sfera de siguranță. Cu toate acestea, restul deciziilor privind caracterul adecvat[48] conțin fiecare o limitare a competențelor autorităților pentru protecția datelor care este identică cu articolul 3 din decizia privind sfera de siguranță, pe care Curtea de Justiție a invalidat-o[49]. În urma pronunțării hotărârii, Comisia va acționa în consecință prin pregătirea în scurt timp a unei decizii, ce urmează să fie adoptată prin procedura comitetelor, aplicabilă în acest caz, prin care va înlocui respectiva dispoziție în toate deciziile privind caracterul adecvat existente. De asemenea, Comisia va întreprinde evaluări regulate ale deciziilor existente și viitoare privind caracterul adecvat, inclusiv prin analize periodice ale funcționării acestora efectuate împreună cu autoritățile competente din țările terțe în cauză.

4. CONCLUZIE

După cum a confirmat Grupul de lucru instituit prin articolul 29, societățile pot utiliza în continuare instrumente alternative pentru transferul legal al datelor către țări terțe, cum ar fi Statele Unite ale Americii. Cu toate acestea, Comisia consideră că un nou cadru, mai solid, pentru transferul datelor cu caracter personal către Statele Unite ale Americii rămâne o prioritate-cheie. Un astfel de cadru ar fi soluția cea mai cuprinzătoare pentru a asigura continuitatea efectivă a protecției datelor cu caracter personal ale cetățenilor europeni care sunt transferate în SUA. Acesta constituie, de asemenea, cea mai bună soluție pentru schimburile comerciale transatlantice, întrucât reprezintă un mecanism de transfer mai simplu, mai puțin împovărător și, prin urmare, mai puțin costisitor, în special pentru IMM-uri.

Comisia a început încă din 2013 negocierile cu guvernul SUA în privința unui nou acord privind transferurile transatlantice de date, bazat pe cele 13 recomandări formulate de

[47] A se vedea considerentul 57 din Directiva 95/46/CE.

[48] Până în prezent au fost adoptate decizii privind caracterul adecvat referitoare la următoarele țări: Andora, Argentina, Canada, Elveția, Guernsey, Insula Man, Insulele Feroe, Israel, Jersey, Noua Zeelandă și Uruguay. A se vedea http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

[49] A se vedea punctele 99-104 din hotărârea pronunțată în cauza Schrems.

Comisie[50]. Cele două părți au înregistrat progrese considerabile în direcția unei apropieri a punctelor lor de vedere, de exemplu în ceea ce privește monitorizarea și aplicarea mai strictă a principiilor sferei de siguranță privind protecția vieții private de către Departamentul Comerțului al SUA. și, respectiv, Comisia Federală pentru Comerț a SUA, creșterea transparenței pentru consumatori referitor la drepturile lor în materie de protecție a datelor, căi de atac mai simple și mai ieftine în cazul existenței unor plângeri și norme mai clare privind transferarea în continuare a datelor din societăți stabilite în țări care intră sub incidența sferei de siguranță către societăți stabilite în țări din afara acesteia (de exemplu în scopuri de prelucrare sau subprelucrare). După invalidarea deciziei privind sfera de siguranță, Comisia și-a intensificat discuțiile cu guvernul SUA pentru a asigura respectarea cerințelor legale formulate de Curte. Obiectivul Comisiei este încheierea acestor discuții și atingerea acestui obiectiv în termen de trei luni.

Până la instituirea noului cadru transatlantic, societățile trebuie să se bazeze pe instrumentele de transfer alternative pe care le au la dispoziție. Această opțiune implică însă asumarea de către exportatorii de date a unor responsabilități, sub supravegherea autorităților naționale pentru protecția datelor.

Spre deosebire de situațiile în care Comisia a constatat că o țară terță asigură un nivel adecvat de protecție a datelor, constatare pe care exportatorii de date se pot baza pentru transferul de date din UE, în cazul utilizării unor instrumente alternative, aceștia au responsabilitatea să verifice că datele cu caracter personal sunt protejate efectiv. Aceasta poate implica, după caz, luarea unor măsuri adecvate.

Autoritățile pentru protecția datelor au un rol central de jucat în această privință. În calitate de principale entități responsabile cu asigurarea respectării drepturilor fundamentale ale persoanelor vizate, autoritățile pentru protecția datelor sunt atât responsabile cu supravegherea în deplină independență a transferurilor de date din UE către țări terțe, cât și competente să efectueze această supraveghere. Comisia invită operatorii de date să coopereze cu autoritățile pentru protecția datelor și să le ajute astfel la îndeplinirea cu succes a rolului lor de supraveghere. Comisia va continua să coopereze strâns cu Grupul de lucru instituit prin articolul 29 pentru a asigura o aplicare consecventă a legislației UE în materie de protecție a datelor.

[50] A se vedea nota de subsol 4 de mai sus.