COMISIA
EUROPEANĂ

Bruxelles, 27.11.2013
COM(2013) 847 final

# 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

**COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN ŞI CONSILIU**

**privind funcţionarea sferei de siguranţă din punctul de vedere al cetăţenilor UE şi al întreprinderilor stabilite în UE**

## 1. INTRODUCERE

Directiva 95/46/CE din 24 octombrie 1995 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date (denumită în continuare „Directiva privind protecţia datelor") stabileşte normele privind transferurile datelor cu caracter personal din statele membre ale UE către alte ţări din afara UE[1] în măsura în care aceste date intră în domeniul de aplicare al instrumentului amintit[2].

În temeiul directivei, Comisia poate stabili că o ţară terţă asigură un nivel adecvat de protecţie prin legislaţia sa internă sau prin angajamentele internaţionale pe care şi le-a asumat pentru a proteja drepturile persoanelor private, iar în acest caz limitările specifice privind transferurile de date către ţara respectivă nu se aplică. Aceste decizii sunt denumite în mod curent „**decizii privind caracterul adecvat al nivelului de protecţie**".

La 26 iulie 2000, Comisia a adoptat Decizia 520/2000/CE[3] (denumită în continuare „**Decizia privind sfera de siguranţă**"), care recunoaşte că principiile privind confidenţialitatea şi întrebările frecvente privind sfera de siguranţă (denumite în continuare „principiile" şi „întrebările frecvente") publicate de Departamentul Comerţului din Statele Unite ale Americii oferă o protecţie adecvată pentru transferurile de date cu caracter personal provenind din UE. Decizia privind sfera de siguranţă a fost adoptată în urma avizului Grupului de lucru „articolul 29" şi a avizului Comitetului „articolul 31", emise printr-o majoritate calificată a statelor membre. În conformitate cu Decizia 1999/468 a Consiliului, Decizia privind sfera de siguranţă a făcut obiectul controlului prealabil din partea Parlamentului European.

Prin urmare, actuala decizie privind sfera de siguranţă permite transferul liber[4] al informaţiilor cu caracter personal din statele membre ale UE[5] către societăţi comerciale din SUA care au aderat la principii, în circumstanţe în care transferul nu ar îndeplini altfel standardele UE privind nivelul adecvat de protecţie a datelor cu caracter personal, având în vedere diferenţele importante dintre regimurile privind confidenţialitatea dintre cele două ţărmuri ale Atlanticului.

Funcţionarea actuală a sferei de siguranţă se bazează pe angajamentele şi autocertificarea societăţilor care aderă. Semnarea acestor acorduri este voluntară, dar regulile sunt obligatorii pentru cei care aderă. Principiile fundamentale ale unui astfel de acord sunt:

a) transparenţa politicilor de confidenţialitate ale societăţilor care aderă,

---

1 Articolele 25 şi 26 din Directiva privind protecţia datelor stabilesc cadrul juridic pentru transferurile de date cu caracter personal din UE către ţări terţe din afara SEE.

2 Norme suplimentare au fost stabilite prin articolul 13 din Decizia-cadru 2008/977/JAI din 27 noiembrie 2008 privind protecţia datelor cu caracter personal prelucrate în cadrul cooperării poliţieneşti şi judiciare în materie penală, în măsura în care aceste transferuri se referă la date cu caracter personal transmise sau puse la dispoziţie de un stat membru unui alt stat membru, care intenţionează să transfere ulterior datele respective către un stat terţ sau către un organism internaţional în scopul prevenirii, cercetării, descoperirii sau urmăririi penale a infracţiunilor sau al executării pedepselor.

3 Decizia 520/2000/CE a Comisiei din 26 iulie 2000 în temeiul Directivei 95/46/CE a Parlamentului European şi a Consiliului privind caracterul adecvat al protecţiei oferite de principiile „sferei de siguranţă" privind protecţia vieţii private şi întrebările de bază aferente, publicate de Departamentul Comerţului al S.U.A., JO L 215 din 28 august 2000, p. 7.

4 Cele de mai sus nu aduc atingere aplicării, în privinţa prelucrării datelor, a altor cerinţe care pot exista în temeiul legislaţiei naţionale de punere în aplicare a Directivei UE privind protecţia datelor.

5 Transferurile de date din cele trei state care fac parte din SEE sunt afectate în mod similar, în urma extinderii Directivei 95/46/CE la Acordul privind SEE, prin Decizia 38/1999 din 25 iunie 1999, JO L 296/41, 23.11.2000.

b) încorporarea principiilor sferei de siguranță în politicile de confidențialitate ale societăților și

c) asigurarea respectării, exercitată inclusiv de către autoritățile publice.

Este însă necesar ca aceste fundamente ale sferei de siguranță să fie reexaminate, pentru a ține cont de noul context, caracterizat de:

a) creșterea exponențială a unor fluxuri de date care în trecut erau auxiliare, dar au devenit între timp esențiale pentru creșterea rapidă a economiei digitale și evoluțiile foarte importante în ceea ce privește colectarea, prelucrarea și utilizarea datelor;

b) importanța decisivă a fluxurilor de date, în special pentru economia transatlantică;[6]

c) creșterea rapidă a numărului de societăți din SUA care au aderat la sistemul sferei de siguranță, număr care a crescut de opt ori din 2004 (de la 400 în 2004 la 3 246 în 2013).

d) informațiile recente privind programele de supraveghere ale SUA, care ridică noi întrebări cu privire la nivelul de protecție pe care se consideră că îl oferă acordul privind sfera de siguranță.

În acest context, prezenta comunicare examinează funcționarea sistemului sferei de siguranță. Ea **se bazează pe elemente** obținute de Comisie, pe activitatea din 2009 a Grupului de contact UE-SUA privind protecția vieții private, pe un studiu elaborat de un contractant independent în 2008[7], precum și pe informațiile primite în cadrul Grupului de lucru ad-hoc UE-SUA (denumit în continuare „Grupul de lucru") instituit în urma dezvăluirilor privind programele de supraveghere ale SUA (*a se vedea un document paralel*). Prezenta comunicare a fost precedată de două **rapoarte de evaluare ale Comisiei** elaborate în cursul etapei inițiale a acordului privind sfera de siguranță, în 2002[8] și în 2004[9].

## 2. STRUCTURA ȘI FUNCȚIONAREA SFEREI DE SIGURANȚĂ

### 2.1. Structura sferei de siguranță

O societate din SUA care dorește să adere la sfera de siguranță trebuie: (a) să menționeze în politica sa de confidențialitate accesibilă publicului că aderă la principii și că le respectă efectiv, precum și (b) să se autocertifice, și anume să declare Departamentului Comerțului din SUA că respectă principiile. Autocertificarea trebuie să fie prezentată o dată pe an. Principiile în materie de confidențialitate ale sferei de siguranță, cuprinse în anexa I la Decizia privind sfera de siguranță, includ cerințe referitoare atât la protecția materială a datelor personale (principii privind integritatea datelor, securitatea, opțiunea și transferul ulterior), cât și la drepturile procedurale ale persoanelor vizate (principii privind notificarea, accesul și asigurarea respectării).

---

6 Conform unor studii, dacă serviciile și fluxurile de date transfrontaliere ar fi perturbate ca urmare a faptului că nu s-ar mai aplica regulile corporatiste obligatorii, clauzele contractuale tip și sfera de siguranță, impactul negativ asupra PIB-ului UE ar atinge între -0,8 % și -1,3 % , iar exporturile de servicii către SUA ar scădea cu -6,7 %, ca urmare a pierderii competitivității. A se vedea: *The Economic Importance of Getting Data Protection Right*, studiu realizat de Centrul European pentru Economie Politică Internațională pentru Camera de Comerț a SUA, martie 2013.

7 Studiul de evaluare a impactului elaborat pentru Comisia Europeană în 2008 de către *Centre de Recherche Informatique et Droit* (CRID) din cadrul Universității Namur.

8 Documentul de lucru al serviciilor Comisiei intitulat Aplicarea Deciziei 520/2000/CE a Comisiei din 26 iulie 2000 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind caracterul adecvat al protecției datelor cu caracter personal oferit de principiile privind confidențialitatea ale „sferei de siguranță" și de întrebările frecvente aferente, publicate de Departamentul Comerțului al SUA, SEC(2002) 196, 13.12.2002.

9 Documentul de lucru al serviciilor Comisiei intitulat Punerea în aplicare a Deciziei 520/2000/CE a Comisiei privind caracterul adecvat al protecției datelor cu caracter personal oferit de principiile privind confidențialitatea ale „sferei de siguranță" și de întrebările frecvente aferente, publicate de Departamentul Comerțului al SUA, SEC (2004) 1323, 20.10.2004.

În ceea ce privește asigurarea respectării sistemului sferei de siguranță în SUA, două instituții americane joacă un rol major: Departamentul Comerțului și Comisia Federală pentru Comerț.

**Departamentul Comerțului** examinează toate autocertificările și recertificările anuale pe care le primește din partea societăților, pentru a se asigura că acestea includ toate elementele necesare pentru participarea la sistem[10]. Acesta actualizează lista societăților care au transmis scrisori de autocertificare și publică această listă, precum și scrisorile respective, pe site-ul său. De asemenea, acesta monitorizează funcționarea sferei de siguranță și elimină de pe listă societățile care nu respectă principiile.

**Comisia Federală pentru Comerț**, care are competențe în domeniul protecției consumatorilor, intervine în cazul unor practici neloiale sau înșelătoare, în temeiul secțiunii 5 din Legea privind Comisia pentru Liber Schimb. Măsurile de asigurare a respectării luate de Comisia Federală pentru Comerț includ anchete privind declarațiile false de aderare la sfera de siguranță și nerespectarea principiilor de către societățile care participă la sistem. În cazul specific al impunerii respectării principiilor sferei de siguranță în ceea ce privește transportatorii aerieni, organismul competent este Departamentul Transportului al SUA[11].

Actuala Decizie privind sfera de siguranță face parte din legislația UE, care trebuie pusă în aplicare de către autoritățile statelor membre. În temeiul deciziei, **autoritățile naționale pentru protecția datelor** (APD) au dreptul de a suspenda, în anumite cazuri, transferurile de date către societățile certificate în temeiul sferei de siguranță[12]. Conform informațiilor de care dispune Comisia, de la instituirea programului privind sfera de siguranță, în 2000, nu au existat cazuri de suspendare de către o autoritate națională de protecție a datelor. În mod independent față de competențele conferite de Decizia privind sfera de siguranță, autoritățile naționale de protecție a datelor din statele UE au competența de a interveni, inclusiv în cazul transferurilor internaționale, pentru a asigura conformitatea cu principiile generale privind protecția datelor stabilite de Directiva privind protecția datelor din 1995.

Astfel cum se reamintește în actuala Decizie privind sfera de siguranță, este de **competența Comisiei** - hotărând în conformitate cu procedura de examinare stabilită în Regulamentul 182/2011 - de a adapta decizia, de a o suspenda sau de a-i limita domeniul de aplicare în orice moment, având în vedere experiența dobândită în punerea în aplicare a acesteia. Acest lucru este prevăzut în special în eventualitatea unei disfuncționalități sistemice din partea SUA, de exemplu în cazul în care un organism din SUA responsabil pentru asigurarea respectării principiilor în materie de confidențialitate ale sferei de siguranță nu își îndeplinește funcția în mod corespunzător sau în cazul în care cerințele legislației SUA afectează nivelul de protecție oferit de principiile sferei de siguranță. La fel ca oricare altă decizie a Comisiei, aceasta poate fi de asemenea modificată din alte motive sau chiar revocată.

---

10 Dacă certificarea sau recertificarea unei societăți nu respectă cerințele sferei de siguranță, Departamentul Comerțului transmite o notificare societății, indicând măsurile care trebuie luate (de exemplu clarificări, modificarea descrierii politicii) pentru ca certificarea să poată fi finalizată.

11 În temeiul titlului 49 secțiunea 41712 din Codul SUA.

12 Mai precis, suspendarea transferurilor de date poate fi impusă în două situații:
(a) organismul administrativ din SUA a constatat că societatea încalcă principiile privind confidențialitatea ale sferei de siguranță; sau
(b) este foarte probabil ca principiile privind confidențialitatea ale sferei de siguranță să fie încălcate; există motive serioase pentru a crede că mecanismul relevant de asigurare a respectării nu ia sau nu va lua din timp măsuri adecvate pentru a soluționa problema respectivă; continuarea transferului ar crea pentru persoanele în cauză un risc iminent de a suferi prejudicii grave; autoritățile competente din statul membru au depus eforturi rezonabile, ținând seama de circumstanțe, de a avertiza organizația și a îi oferi posibilitatea de a răspunde.

## 2.2. Funcționarea sferei de siguranță

Cele **3 246**[13] **de întreprinderi certificate** sunt atât societăți mici, cât și mari[14]. În timp ce serviciile financiare și sectorul telecomunicațiilor nu intră în competențele de asigurare a respectării ale Comisiei Federale pentru Comerț și, prin urmare, sunt excluse din sfera de siguranță, în cadrul societăților certificate sunt reprezentate un număr mare de sectoare industriale și de servicii, inclusiv societăți cunoscute din domeniul internetului și din sectoare de la servicii informatice la produse farmaceutice, servicii de voiaj și turism, asistență medicală sau servicii de cărți de credit[15]. Acestea sunt în principal societăți din SUA care furnizează servicii pe piața internă a UE, dar și filiale ale unor societăți din UE, precum Nokia sau Bayer. 51 % sunt societăți care prelucrează date ale persoanelor angajate în Europa și transferate în SUA din motive legate de resursele umane[16].

Anumite autorități pentru protecția datelor din UE au manifestat **o preocupare crescândă** în legătură cu transferurile de date în cadrul actualului sistem al sferei de siguranță. Autoritățile pentru protecția datelor din anumite state membre au criticat formularea foarte generală a principiilor și faptul că sistemul se bazează în mare măsură pe autocertificare și autoreglementare. Preocupări similare au fost formulate și de întreprinderi, care au menționat denaturarea concurenței ca urmare a neasigurării respectării.

Actualul acord privind sfera de siguranță se bazează pe aderarea voluntară a societăților, pe autocertificarea acestora și pe asigurarea de către autoritățile publice a respectării angajamentelor care fac obiectul autocertificării. În acest context, orice deficiențe în ceea ce privește transparența sau asigurarea respectării compromit principiile pe baza cărora a fost creat sistemul sferei de siguranță.

Orice deficiențe ale SUA în ceea ce privește transparența sau asigurarea respectării determină transferul responsabilității către autoritățile europene pentru protecția datelor și către societățile care utilizează sistemul. La 29 aprilie 2010, autoritățile pentru protecția datelor din Germania au emis o decizie care impune ca societățile care transferă date din Europa către SUA să verifice în mod activ dacă societățile din SUA care importă datele respectă într-adevăr principiile în materie de confidențialitate ale sferei de siguranță și recomandă ca „cel puțin societatea care exportă datele să stabilească dacă certificarea societății care importă datele continuă să fie valabilă”[17].

La 24 iulie 2013, în urma dezvăluirilor privind programele de supraveghere ale SUA, autoritățile pentru protecția datelor din Germania au făcut încă un pas, exprimându-și îngrijorarea în legătură cu faptul că „este foarte probabil ca principiile formulate în deciziile

---

13 La 26 septembrie 2013, numărul organizațiilor din cadrul sferei de siguranță înregistrate ca „**actuale**” în cadrul listei sferei de siguranță era de **3 246**, iar numărul celor „**care nu mai sunt actuale**” de **935**.

14 Organizații din cadrul sferei de siguranță cu cel mult 250 de angajați: **60 %** (1 925 din 3 246). Organizații din cadrul sferei de siguranță cu cel puțin 251 de angajați: **40 %** (1 295 din 3 246).

15 De exemplu, MasterCard colaborează cu mii de bănci, fiind un exemplu clar de situație în care sfera de siguranță nu poate fi înlocuită de alte instrumente juridice privind transferul de date cu caracter personal, precum regulile corporatiste obligatorii sau dispozițiile contractuale.

16 Organizațiile din sfera de siguranță care tratează date privind resursele umane în virtutea certificării lor în cadrul sferei de siguranță (și, prin urmare, au fost de acord să respecte principiile și să coopereze cu autoritățile UE de protecție a datelor): **51 %** (1 671 din 3 246).

17 A se vedea decizia Düsseldorfer Kreis din 28/29 aprilie 2010. A se vedea: Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April 2010 in Hannover: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile Cu toate acestea, Peter Hustinx, Autoritatea Europeană pentru Protecția Datelor (AEPD), a declarat în cadrul audierii publice organizate de Comisia LIBE a Parlamentului European la 7 octombrie 2013 că în ceea ce privește sfera de siguranță „au fost realizate îmbunătățiri importante și majoritatea problemelor au fost rezolvate”: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-10-07_Speech_LIBE_PH_EN.pdf

Comisiei să fie încălcate”[18]. Unele APD (de exemplu, autoritatea din Bremen) au cerut anumitor societăți care transferau date către furnizori din SUA să informeze APD relevantă dacă și în ce mod furnizorii respectivi împiedică accesul Agenției Naționale de Securitate la datele respective. APD din Irlanda a raportat că a primit recent două plângeri referitoare la programul privind sfera de siguranță, în urma dezvăluirilor privind programele serviciilor de informații din SUA, dar că a refuzat să trateze plângerile respective întrucât transferul de date personale către o țară terță respecta cerințele prevăzute de legislația irlandeză privind protecția datelor. În urma unei plângeri similare, APD din Luxemburg a constatat că Microsoft și Skype respectau cerințele Legii luxemburgheze privind protecția datelor atunci când transferau date către SUA[19]. Cu toate acestea, între timp Curtea Supremă din Irlanda a acceptat o cerere de control judiciar, în cadrul căreia va examina inacțiunea comisarului irlandez pentru protecția datelor în ceea ce privește programele de supraveghere ale SUA. Una dintre cele două plângeri a fost depusă de grupul studențesc „Europe v Facebook” (EvF), care a depus și o plângere similară în Germania împotriva Yahoo, examinată în prezent de către autoritățile relevante de protecție a datelor.

Aceste răspunsuri divergente ale autorităților pentru protecția datelor la dezvăluirile privind programele de supraveghere demonstrează că există un risc real de fragmentare a sistemului sferei de siguranță și ridică semne de întrebare cu privire la măsura în care este garantată respectarea acestuia.

## 3. TRANSPARENȚA POLITICILOR DE CONFIDENȚIALITATE ALE SOCIETĂȚILOR ADERENTE

Potrivit întrebării frecvente nr. 6, care este anexată la Decizia privind sfera de siguranță (anexa II), societățile care doresc să obțină certificarea privind sfera de siguranță trebuie să transmită politica lor de confidențialitate Departamentului Comerțului și să o pună la dispoziția publicului. Aceasta trebuie să includă angajamentul de a adera la principiile privind confidențialitatea. Cerința de **a pune la dispoziția publicului politicile de confidențialitate** ale societăților autocertificate, precum și declarația de aderare la principiile privind confidențialitatea, este esențială pentru funcționarea sistemului.

O accesibilitate insuficientă la politicile de confidențialitate ale societăților respective este în detrimentul persoanelor ale căror date cu caracter personal sunt colectate și prelucrate și poate constitui o **încălcare a principiului notificării**. În astfel de cazuri, este posibil ca persoanele ale căror date sunt transferate din UE să nu-și cunoască drepturile și nici obligațiile societăților autocertificate.

În plus, ca urmare a angajamentului societăților de a respecta principiile privind confidențialitatea, **Comisia Federală pentru Comerț dobândește competența de a impune respectarea acestor principii** de către societăți în cazurile de neconformitate reprezentate de practici neloiale sau înșelătoare. Lipsa de transparență din partea societăților din SUA îngreunează supravegherea exercitată de Comisia Federală pentru Comerț și subminează eficacitatea măsurilor de asigurare a respectării.

De-a lungul anilor, un număr important de societăți autocertificate nu au pus la dispoziția publicului politica lor de confidențialitate și/sau nu au făcut o declarație publică privind aderarea la principiile de confidențialitate. Raportul din 2004 privind sfera de siguranță a

[18] A se vedea o rezoluție a Conferinței comisarilor pentru protecția datelor din Germania, care subliniază faptul că serviciile de informații constituie o amenințare semnificativă la adresa transferului de date din Germania către țările din afara Europei: http://www.bfdi.bund.de/EN/Home/homepage_Kurzmeldungen/PMDSK_SafeHarbor.html?nn=408870

[19] A se vedea comunicatul de presă din 18 noiembrie 2013 al APD din Luxemburg.

indicat necesitatea ca Departamentul Comerțului să aibă **o atitudine mai activă în ceea ce privește verificarea conformității** cu această cerință.

Din 2004, Departamentul Comerțului a elaborat **noi instrumente de informare**, cu obiectivul de a ajuta societățile să-și respecte obligațiile în materie de transparență. Informațiile relevante privind programul sunt accesibile pe site-ul Departamentului Comerțului consacrat sferei de siguranță[20], care permite și încărcarea de către societăți a politicilor lor de confidențialitate. Departamentul Comerțului a comunicat că societățile au utilizat această posibilitate și și-au publicat politicile de confidențialitate pe site-ul Departamentului Comerțului în momentul cererii de aderare la sfera de siguranță[21]. În plus, în perioada 2009-2013 Departamentul Comerțului a publicat o serie de orientări pentru societățile care doresc să adere la sfera de siguranță, precum ghidul „*Guide to Self-Certification*” și documentul „*Helpful Hints on Self-Certifying Compliance*”[22].

Gradul de respectare a obligațiilor în materie de transparență variază de la o societate la alta. În timp ce anumite societăți se limitează la transmiterea către Departamentul Comerțului a unei descrieri a politicii lor de confidențialitate în cadrul procesului de autocertificare, majoritatea societăților își publică politica de confidențialitate pe propriul site, în afară de a o încărca pe site-ul Departamentului Comerțului. Cu toate acestea, **politicile nu sunt întotdeauna prezentate într-o formă ușor de înțeles și de consultat de către consumatori**. Linkurile către politicile de confidențialitate nu funcționează întotdeauna în mod corespunzător sau nu trimit către paginile corecte.

Din decizie și din anexele la aceasta reiese că cerința ca societățile să-și facă publice politicile de confidențialitate **depășește simpla obligație de a notifica** autocertificarea Departamentului Comerțului. Cerințele privind certificarea prezentate în cadrul întrebărilor frecvente includ comunicarea unei descrieri a politicii de confidențialitate și a unor informații transparente privind locul în care aceasta este disponibilă pentru consultarea de către public[23]. Declarațiile privind politica de confidențialitate trebuie să fie clare și ușor accesibile de către public. Acestea trebuie să includă un link către site-ul Departamentului Comerțului consacrat sferei de siguranță, care prezintă toți membrii „actuali” ai sistemului, precum și un link către entitatea care oferă un mecanism de soluționare alternativă a litigiilor. Cu toate aceste, unele societăți participante la sistem în perioada 2000-2013 nu au îndeplinit aceste cerințe. În cursul contactelor de lucru cu Comisia din februarie 2013, Departamentul Comerțului a confirmat că este posibil ca până la 10 % dintre societățile certificate să nu fi publicat de fapt pe site-ul lor o politică de confidențialitate care să declare în mod afirmativ că aderă la principiile privind sfera de confidențialitate.

Statistici recente demonstrează, de asemenea, problema persistentă a **declarațiilor false privind aderarea la sfera de siguranță**. Circa 10 % dintre societățile care declară că sunt membre ale sferei de siguranță nu sunt incluse de Departamentul Comerțului ca membri actuali ai sistemului[24]. Astfel de declarații false sunt făcute: fie de societăți care nu au participat niciodată la sfera de siguranță, fie de societăți care au aderat în trecut la sistem, dar ulterior nu și-au transmis anual autocertificarea către Departamentul Comerțului. În al doilea

---

20 http://www.export.gov/SafeHarbour/

21 https://SafeHarbour.export.gov/list.aspx

22 Ghidul este disponibil pe site-ul programului, la adresa: http://export.gov/SafeHarbour/ *Helpful Hints*: http://export.gov/SafeHarbour/eu/eg_main_018495.asp

23 La 12 noiembrie 2013, Departamentul Comerțului a confirmat: „În prezent, societățile care au site-uri publice și tratează date privind consumatorii/clienții/vizitatorii trebuie să includă pe site-urile lor o politică de confidențialitate conformă cu principiile sferei de siguranță” (documentul „*U.S.-EU Cooperation to Implement the Safe Harbor Framework*” din 12 nov. 2013).

24 În septembrie 2013, biroul de consultanță australian Galexia a efectuat o comparație între „declarațiile false” ale membrilor sferei de siguranță din 2008 și din 2013. Principala sa concluzie este că, în paralel cu creșterea numărului membrilor sferei de siguranță între 2008 și 2013 (de la 1 109 la 3 246), a crescut și numărul de declarații false, de la 206 la 427. http://www.galexia.com/public/about/news/about_news-id225.html

caz de mai sus, societățile continuă să fie menționate pe site-ul sferei de siguranță, dar cu statutul de certificare „neactual”, însemnând că societatea a fost membră a sistemului și, prin urmare, are obligația de a continua să asigure protecția datelor pe care le-a prelucrat anterior. Comisia Federală pentru Comerț are competența de a interveni în cazul practicilor înșelătoare și al nerespectării principiilor sferei de siguranță (a se vedea secțiunea 5.1). Neclaritatea în legătură cu „declarațiile false” prejudiciază credibilitatea sistemului.

Comisia Europeană a avizat Departamentul Comerțului, cu ocazia contactelor periodice din 2012 și 2013, că pentru ca societățile să îndeplinească obligațiile în materie de transparență nu este suficient ca acestea să transmită Departamentului Comerțului o descriere a politicii lor de confidențialitate. Este, de asemenea, necesar să existe declarații publice privind politica de confidențialitate. De asemenea, Departamentul Comerțului a fost invitat **să-și intensifice controalele periodice ale site-urilor societăților** efectuate ulterior procedurii de verificare în contextul primului proces de autocertificare sau al reînnoirii sale anuale, precum și să ia măsuri împotriva societăților care nu îndeplinesc cerințele în materie de transparență.

Ca prim răspuns la preocupările UE, **din martie 2013 Departamentul Comerțului a introdus obligația** ca o societate membră a sferei de siguranță și care are un site public să-și publice pe site-ul său politica de confidențialitate privind datele clienților/utilizatorilor. În același timp, Departamentul Comerțului a început să comunice tuturor societăților a căror politică de confidențialitate nu includea deja un link către site-ul consacrat sferei de siguranță al Departamentului Comerțului că este necesară introducerea acestui link, astfel încât site-ul și lista privind sfera de siguranță să fie direct accesibile consumatorilor care vizitează site-ul unei societăți. Astfel, toate persoanele vizate din Europa vor putea să verifice imediat, fără a efectua căutări suplimentare pe internet, angajamentele transmise de o societate Departamentului Comerțului. În plus, Departamentul Comerțului a început să comunice societăților că datele de contact ale furnizorului lor independent de servicii de soluționare alternativă a litigiilor trebuie să fie incluse în politica de confidențialitate pe care o publică[25].

**Acest proces va trebui accelerat**, astfel încât toate societățile certificate să îndeplinească pe deplin cerințele sferei de siguranță cel târziu până în martie 2014 (și anume până la data-limită a recertificării anuale a societăților, calculată de la introducerea noilor cerințe în martie 2013).

Cu toate acestea, nu este încă sigur că toate societățile autocertificate îndeplinesc pe deplin cerințele în materie de transparență. Departamentul Comerțului ar trebui să monitorizeze și să examineze mai strict îndeplinirea obligațiilor asumate în momentul autocertificării inițiale și al reînnoirii anuale.

## 4. INTEGRAREA PRINCIPIILOR PRIVIND CONFIDENȚIALITATEA ALE SFEREI DE SIGURANȚĂ ÎN CADRUL POLITICILOR DE CONFIDENȚIALITATE ALE SOCIETĂȚILOR

Pentru a obține și a păstra avantajele sferei de siguranță, societățile autocertificate trebuie să îndeplinească principiile de confidențialitate prezentate în anexa I la decizie.

În raportul din 2004, Comisia a constatat că un număr important de **societăți nu integraseră în mod corect principiile privind confidențialitatea ale sferei de siguranță** în cadrul politicilor lor privind prelucrarea datelor. De exemplu, persoanele vizate nu aveau întotdeauna

[25] Între martie și septembrie 2013, Departamentul Comerțului:
• a comunicat celor 101 societăți *care își încărcaseră deja politicile de confidențialitate conforme cu sfera de siguranță* pe site-ul relevant al Departamentului Comerțului că este de asemenea necesar ca acestea să-și publice politicile de confidențialitate pe propriul site;
• a comunicat celor 154 de societăți care nu făcuseră încă acest lucru că este necesar să includă în politicile lor de confidențialitate un link către site-ul consacrat sferei de siguranță;
• a comunicat unui număr de peste 600 de societăți că este necesar să includă în politicile lor de confidențialitate datele de contact ale furnizorului lor independent de servicii de soluționare a litigiilor.

acces la informații clare și transparente privind scopurile în care sunt prelucrate datele lor sau nu aveau posibilitatea de a refuza ca datele lor să fie comunicate unei părți terțe sau să fie utilizate într-un scop incompatibil cu scopurile în care au fost colectate inițial. Raportul din 2004 al Comisiei a considerat că Departamentul Comerțului *„ar trebui să fie mai proactiv în ceea ce privește accesul la sfera de siguranță și informarea în legătură cu principiile sale”*[26].

Au existat progrese limitate în această privință. De la 1 ianuarie 2009, orice societate care dorește să-și reînnoiască certificarea pentru sfera de siguranță - care trebuie efectuată anual - face obiectul unei evaluări prealabile a politicii sale de confidențialitate de către Departamentul Comerțului. Cu toate acestea, evaluarea are un domeniu de aplicare limitat. **Nu există o evaluare completă a practicilor efective** ale societăților autocertificate, care ar îmbunătăți considerabil credibilitatea procesului de autocertificare.

În urma solicitărilor Comisiei în legătură cu o supraveghere mai sistematică și riguroasă de către Departamentul Comerțului a societăților autocertificate, **în prezent se acordă o atenție sporită noilor certificări**. Numărul noilor certificări care nu au fost acceptate, fiind retrimise societăților pentru efectuarea unor îmbunătățiri ale politicii de confidențialitate, a crescut în mod considerabil între 2010 și 2013: s-a dublat pentru societățile care au solicitat reînnoirea certificării și s-a triplat pentru noii aderenți la sfera de siguranță[27]. Departamentul Comerțului a asigurat Comisia că o certificare sau recertificare nu poate fi finalizată decât dacă politica de confidențialitate a societății îndeplinește toate cerințele, în special dacă include un angajament afirmativ de a adera la setul relevant de principii privind confidențialitatea ale sferei de siguranță și dacă politica de confidențialitate este disponibilă publicului. Societățile sunt obligate să indice, printre informațiile care figurează în lista membrilor sferei de securitate, locul în care este publicată politica de confidențialitate relevantă. De asemenea, societățile trebuie să indice pe site-ul lor un furnizor de servicii de soluționare alternativă a litigiilor și să includă un link către informațiile privind autocertificarea în cadrul sferei de siguranță publicate pe site-ul Departamentului Comerțului. Cu toate acestea, s-a estimat că peste 30 % dintre membrii sferei de siguranță nu furnizează informații privind soluționarea litigiilor în politicile de confidențialitate de pe site-urile lor[28].

În cazul majorității societăților pe care Departamentul Comerțului le-a eliminat din lista sferei de siguranță, acest lucru s-a întâmplat la cererea societăților respective (de exemplu, societăți care au fuzionat sau au fost achiziționate, și-au modificat domeniul de activitate sau și-au încetat activitatea). Înregistrările unui număr mai mic de societăți au fost eliminate când s-a constatat că site-urile indicate pe listă nu funcționau și că statutul de certificare al acestora era „neactual” de mai mulți ani[29]. Este important de precizat că niciuna dintre aceste eliminări nu a fost efectuată din cauză că verificarea Departamentului Comerțului a determinat identificarea unor probleme de conformitate.

Lista membrilor sferei de siguranță îndeplinește rolul de aviz public și de înregistrare a angajamentelor societăților care fac parte din sfera de siguranță. **Angajamentul de a adera la**

---

26 A se vedea pagina 8 din Raportul din 2004, SEC(2004) 1323.

27 Conform statisticilor furnizate în septembrie 2013 de Departamentul Comerțului, în 2010 acesta a transmis notificări către 18 % (93) dintre cele 512 societăți care au solicitat certificarea pentru prima dată și către 16 % (231) dintre cele 1 417 societăți care au solicitat recertificarea, cerând îmbunătățirea politicilor lor de confidențialitate și/sau a cererilor de participare la sfera de siguranță. În urma cererilor Comisiei privind o examinare strictă, atentă și sistematică a tuturor cererilor, începând cu jumătatea lunii septembrie 2013 Departamentul Comerțului a transmis notificări către 56 % (340) dintre cele 602 societăți care au solicitat certificarea pentru prima dată și către 27 % (493) dintre cele 1 809 societăți care au solicitat recertificarea, cerând îmbunătățirea politicilor lor de confidențialitate.

28 Declarațiile domnului Chris Connolly (Galexia) în cadrul audierii organizate de către Comisia LIBE a Parlamentului European la 7 octombrie 2013.

29 În decembrie 2011, Departamentul Comerțului din SUA eliminase 323 de societăți din lista sferei de siguranță. 94 de societăți au fost eliminate deoarece și-au încetat activitatea, 88 de societăți au fost eliminate ca urmare a achiziționării sau a fuziunii, iar 95 la cererea societății-mamă; 41 de societăți au fost eliminate ca urmare a netransmiterii în mai multe rânduri a cererii de recertificare, iar 5 societăți din motive diverse.

**principiile sferei de siguranță nu este limitat în timp** în privința datelor primite în cursul perioadei în care societatea a beneficiat de avantajele sferei de siguranță, iar societatea trebuie să continue să aplice principiile în ceea ce privește aceste date atâta timp cât le stochează, le utilizează sau le comunică, chiar în cazul în care a încetat să facă parte din sfera de siguranță, din orice motiv.

**Societățile care au solicitat să facă parte din sfera de siguranță, dar a căror cerere a fost respinsă în urma verificării administrative** de către Departamentul Comerțului și, prin urmare, care nu au fost niciodată incluse în listă, sunt repartizate după cum urmează. **În 2010**, numai **6 %** (33) dintre cele 513 societăți care au solicitat certificarea pentru prima dată nu au fost incluse niciodată în lista sferei de siguranță din motiv că nu îndeplineau standardele de autocertificare ale Departamentului Comerțului. **În 2013**, **12 %** (75) dintre cele 605 societăți care au solicitat certificarea pentru prima dată nu au fost incluse niciodată în lista sferei de siguranță din motiv că nu îndeplineau standardele de autocertificare ale Departamentului Comerțului.

Ca o cerință minimă pentru a îmbunătăți transparența procesului de supraveghere, Departamentul Comerțului ar trebui să indice pe site-ul său toate societățile care au fost eliminate din sfera de siguranță, precum și motivele pentru care certificarea nu a fost reînnoită. Mențiunea „neactual" din lista societăților care fac parte din sfera de siguranță nu ar trebui considerată doar o informație, ci ar trebui să fie însoțită de un **avertisment clar** - atât scris, cât și grafic - privind faptul că societatea nu îndeplinește în prezent cerințele sferei de siguranță.

În plus, unele societăți încă nu au integrat pe deplin toate principiile sferei de siguranță. În afară de problema transparenței, tratată în secțiunea 3 de mai sus, adesea politicile de confidențialitate ale societăților autocertificate nu prezintă în mod clar motivele pentru care sunt colectate datele și dreptul de a alege dacă datele să fie sau nu comunicate unor părți terțe; acest lucru determină probleme de conformitate cu principiile de confidențialitate privind „Notificarea" și „Opțiunea". Notificarea și opțiunea sunt esențiale pentru a garanta că persoanele mențin controlul asupra a ceea ce se întâmplă cu informațiile care le vizează.

Primul pas esențial în cadrul procesului de asigurare a conformității, integrarea principiilor de confidențialitate ale sferei de siguranță în politicile de confidențialitate ale societăților, nu este îndeplinit în mod suficient. Departamentul Comerțului ar trebui să abordeze acest aspect în mod prioritar, prin elaborarea unei metodologii de asigurare a conformității de către societăți, atât în cadrul practicilor lor de funcționare, cât și al interacțiunilor cu clienții. **Departamentul Comerțului trebuie să monitorizeze în mod activ integrarea principiilor sferei de siguranță în cadrul politicilor de confidențialitate ale societăților**, în loc ca măsurile de asigurare a respectării să fie declanșate numai dacă se primesc plângeri din partea persoanelor.

## 5. MĂSURI DE ASIGURARE A RESPECTĂRII ALE AUTORITĂȚILOR PUBLICE

Există o serie de mecanisme pentru a asigura în mod efectiv respectarea sistemului sferei de siguranță și pentru a oferi măsuri reparatorii persoanelor în cazul în care protecția informațiilor care le vizează este afectată de neconformitatea cu principiile de confidențialitate.

Conform principiului privind asigurarea respectării, politicile de confidențialitate ale organizațiilor autocertificate trebuie să includă mecanisme efective de asigurare a conformității. Conform principiului de confidențialitate referitor la asigurarea respectării, astfel cum acesta este clarificat de întrebările frecvente 11, 5 și 6, această cerință poate fi îndeplinită prin aderarea la **mecanisme independente de tratare a plângerilor** care și-au

declarat public competența de a trata plângeri individuale privind nerespectarea principiilor. Alternativ, acest lucru poate fi realizat prin angajamentul organizației de a coopera cu **Grupul UE pentru protecția datelor**[30]. În plus, societățile autocertificate sunt supuse jurisdicției Comisiei Federale pentru Comerț, în temeiul secțiunii 5 din Legea privind Comisia Federală pentru Comerț, care interzice actele sau practicile incorecte sau înșelătoare în domeniul comercial sau care afectează comerțul[31].

În raportul din 2004 au fost formulate preocupări în legătură cu asigurarea respectării sistemului sferei de siguranță, mai precis s-a recomandat o atitudine mai proactivă a Comisiei Federale pentru Comerț în ceea ce privește lansarea investigațiilor și informarea persoanelor în legătură cu drepturile lor. O altă preocupare este lipsa de claritate în legătură cu competența Comisiei Federale pentru Comerț de a asigura respectarea principiilor în cazul datelor privind resursele umane.

Organismul de tratare a plângerilor responsabil pentru datele privind resursele umane - Grupul UE pentru protecția datelor - a primit o plângere referitoare la datele privind resursele umane[32]. Cu toate acestea, absența plângerilor nu permite să se formuleze concluzii cu privire la funcționarea de ansamblu a sistemului. Ar trebui introduse verificări din oficiu privind respectarea principiilor de către societăți, pentru a controla îndeplinirea efectivă a angajamentelor în materie de protecție a datelor. Autoritățile UE pentru protecția datelor ar trebui, de asemenea, să ia măsuri de îmbunătățire a nivelului de informare în legătură cu existența grupului.

Au fost indicate probleme referitoare la modul de funcționare a mecanismelor de soluționare alternativă a litigiilor în calitate de organisme de asigurare a respectării. Unele dintre aceste organisme nu au mijloace adecvate pentru a lua măsuri reparatorii în cazul nerespectării principiilor. Este necesară remedierea acestei deficiențe.

### 5.1. Comisia Federală pentru Comerț

Comisia Federală pentru Comerț poate lua măsuri de asigurare a respectării în cazul neîndeplinirii de către societăți a angajamentelor luate în legătură cu sfera de siguranță. Când a fost instituită sfera de siguranță, Comisia Federală pentru Comerț s-a angajat să examineze în mod prioritar toate dosarele transmise de autoritățile statelor membre ale UE[33]. Dat fiind că în cursul primilor zece ani de aplicare a acordului nu a primit nicio plângere, Comisia Federală pentru Comerț a decis să verifice dacă există încălcări ale sferei de siguranță în cadrul fiecărei investigații privind confidențialitatea și securitatea datelor pe care o desfășoară. Din 2009, Comisia Federală pentru Comerț a deschis 10 acțiuni de impunere a respectării împotriva unor societăți, pentru încălcări ale sferei de siguranță. Aceste acțiuni au dus în principal la tranzacții judiciare interzicând - sub rezerva unor penalizări importante -

---

30 Grupul UE pentru protecția datelor este un organism competent pentru investigarea și soluționarea plângerilor depuse de persoane private cu privire la încălcarea presupusă a principiilor sferei de siguranță de către o societate din SUA care este membră a sferei de siguranță. Societățile care certifică respectarea principiilor sferei de siguranță trebuie să opteze pentru aderarea la un mecanism independent de tratare a plângerilor sau pentru cooperarea cu Grupul UE pentru protecția datelor, în vederea soluționării problemelor determinate de neîndeplinirea principiilor sferei de siguranță. Cooperarea cu Grupul UE pentru protecția datelor este însă obligatorie în cazul în care societatea din SUA prelucrează date personale privind resursele umane transferate din UE în contextul unui raport de muncă. Dacă societatea se angajează să coopereze cu Grupul UE pentru protecția datelor, ea trebuie să se angajeze, de asemenea, să îndeplinească orice recomandare formulată de grupul menționat în cazul în care acesta consideră că societatea trebuie să ia măsuri specifice pentru a respecta principiile sferei de siguranță, inclusiv măsuri reparatorii sau de compensare.

31 Departamentul Transportului exercită o jurisdicție similară asupra transportatorilor aerieni, în temeiul titlului 49 secțiunea 41712 din Codul Statelor Unite.

32 Plângerea a fost depusă de un cetățean elvețian și, prin urmare, a fost transmisă de Grupul UE pentru protecția datelor către autoritatea elvețiană pentru protecția datelor (SUA aplică un sistem al sferei de siguranță separat pentru Elveția).

33 A se vedea anexa V la Decizia 2000/520/CE a Comisiei din 26 iulie 2000.

declarațiile false privind protecția confidențialității, inclusiv privind conformitatea cu sfera de siguranță, și impunând societăților programe cuprinzătoare de protecție a confidențialității și audituri pentru o perioadă de 20 de ani. Societățile trebuie să accepte evaluări independente ale programelor lor de confidențialitate, la cererea Comisiei Federale pentru Comerț. Constatările acestor evaluări sunt comunicate în mod regulat Comisiei Federale pentru Comerț. Ordinele Comisiei Federale pentru Comerț interzic, de asemenea, ca societățile să facă declarații false privind practicile lor în materie de confidențialitate și participarea lor la sfera de siguranță sau la sisteme similare. Acesta a fost, de exemplu, cazul investigațiilor Comisiei Federale pentru Comerț împotriva Google, Facebook și Myspace.[34] În 2012, Google a acceptat să plătească o amendă de 22,5 milioane USD pentru a pune capăt acuzațiilor privind încălcarea unui acord voluntar. În toate investigațiile sale privind confidențialitatea, Comisia Federală pentru Comerț verifică din oficiu dacă a existat o încălcare a sferei de siguranță.

Comisia Federală pentru Comerț a reiterat recent declarațiile sale și angajamentul de a examina, în mod prioritar, toate dosarele transmise de organisme de autoreglementare din domeniul confidențialității și de statele membre ale UE cu privire la presupusa neîndeplinire de către o societate a principiilor sferei de siguranță[35]. În cursul ultimilor trei ani, Comisia Federală pentru Comerț a primit numai câteva dosare din partea autorităților pentru protecția datelor din UE.

Cooperarea transatlantică dintre autoritățile pentru protecția datelor a început să se dezvolte în cursul ultimelor luni. De exemplu, la 26 iunie 2013 Comisia Federală pentru Comerț a semnat un memorandum de înțelegere cu autoritatea pentru protecția datelor din Irlanda, cu privire la asistența reciprocă pentru asigurarea respectării legislației care protejează informațiile personale în sectorul privat. Memorandumul stabilește un cadru pentru o cooperare consolidată, simplificată și mai eficace în materie de asigurare a respectării legislației privind confidențialitatea[36].

În august 2013, Comisia Federală pentru Comerț a anunțat o intensificare suplimentară a verificărilor efectuate asupra societăților care exercită controlul asupra unor baze de date personale de mari dimensiuni. De asemenea, comisia a creat un portal în cadrul căruia consumatorii pot depune plângeri referitoare la încălcarea confidențialității de către o societate din SUA[37].

Comisia Federală pentru Comerț ar trebui, de asemenea, să își intensifice eforturile de investigare a declarațiilor false de aderare la sfera de siguranță. O societate care declară pe site-ul său că respectă cerințele sferei de siguranță, dar nu este inclusă în lista Departamentului Comerțului ca membru „actual" al sistemului înșeală consumatorii și abuzează de încrederea acestora. Afirmațiile false compromit credibilitatea sistemului în ansamblul său și, prin urmare, ar trebui eliminate imediat de pe site-urile societăților. Societățile ar trebui să fie supuse unei obligații executorii de a nu înșela consumatorii.

---

34 În perioada 2009-2012, Comisia Federală pentru Comerț a încheiat zece acțiuni de asigurare a respectării angajamentelor sferei de siguranță: Comisia Federală pentru Comerț / Javian Karnani și Balls of Kryptonite, LLC (2009), World Innovators, Inc. (2009), Expat Edge Partners, LLC (2009), Onyx Graphics, Inc. (2009), Directors Desk LLC (2009), Progressive Gaitways LLC (2009), Collectify LLC (2009), Google Inc. (2011), Facebook, Inc. (2011), Myspace LLC (2012). A se vedea: „*Federal Trade Commission of Safe Harbour Commitments*": http://export.gov/build/groups/public/@eg_main/@SafeHarbour/documents/webcontent/eg_main_052211.pdf . A se vedea, de asemenea: „*Case Highlights*": http://business.ftc.gov/us-eu-Safe-Harbour-framework Majoritatea cazurilor au vizat societăți care au aderat la sfera de siguranță dar care, ulterior, au continuat să se prezinte drept membre fără a-și reînnoi însă certificarea anuală.

35 Acest angajament a fost reiterat în cadrul unei întâlniri dintre Julie Brill, membră a Comisiei Federale pentru Comerț, și autoritățile pentru protecția datelor din statele UE (Grupul de lucru „articolul 29"), care a avut loc în Bruxelles la 17 aprilie 2013.

36 http://www.dataprotection.ie/viewdoc.asp?Docid=1317&Catid=66&StartDate=1+January+2013&m=n

37 Consumatorii pot depune plângeri prin intermediul asistentului pentru plângeri din cadrul Comisiei Federale pentru Comerț (https://www.ftccomplaintassistant.gov/), iar consumatorii internaționali pot depune plângeri prin intermediul site-ului econsumer.gov (http://www.econsumer.gov).

Comisia Federală pentru Comerț ar trebui să continue să detecteze declarațiile false de aderare la sfera de siguranță, precum cea care a făcut obiectul dosarului *Karnani*, care a dus la închiderea de către Comisia Federală pentru Comerț a unui site din California, ca urmare a declarației false privind înregistrarea în sfera de siguranță și a unor practici frauduloase de comerț electronic care vizau consumatorii europeni[38].

La 29 octombrie 2013, Comisia Federală pentru Comerț a anunțat că în ultimele luni a deschis „un număr mare de investigații privind conformitatea cu sfera de siguranță" și că se estimează că „în cursul lunilor următoare" vor fi luate măsuri suplimentare de asigurare a respectării. De asemenea, Comisia Federală pentru Comerț a confirmat că „se angajează să caute modalități de a-și îmbunătăți eficacitatea", precum și că va „continua să primească pozitiv orice informații fundamentate, precum plângerea primită în cursul lunii trecute din partea unui apărător al drepturilor consumatorilor în legătură cu un mare număr de presupuse încălcări legate de sfera de siguranță".[39] Comisia Federală pentru Comerț s-a angajat și să „monitorizeze în mod sistematic respectarea ordonanțelor referitoare la sfera de siguranță, la fel ca în cazul tuturor celorlalte ordonanțe"[40].

La 12 noiembrie 2013, Comisia Federală pentru Comerț a informat Comisia Europeană că „**dacă politica de confidențialitate a unei societăți afirmă că oferă protecția garantată de sfera de siguranță, faptul că societatea respectivă nu se înregistrează sau nu își reînnoiește înregistrarea nu exclude impunerea de către Comisia Federală pentru Comerț a respectării angajamentelor respective privind sfera de siguranță**"[41].

În noiembrie 2013, Departamentul Comerțului a informat Comisia Europeană că „pentru a se asigura că societățile nu fac declarații false de participare la sfera de siguranță, Departamentul Comerțului va începe să contacteze participanții la sfera de siguranță cu o lună înainte de data-limită a recertificării lor, pentru a le indica etapele pe care trebuie să le urmeze în cazul în care ar decide să nu solicite recertificarea". **Departamentul Comerțului „va avertiza societățile** din această categorie că trebuie să elimine orice referire la participarea la sfera de siguranță, inclusiv utilizarea siglei de certificare a sferei de siguranță, din cadrul politicilor de confidențialitate ale societăților și de pe site-urile lor, **și le va comunica în mod clar că neîndeplinirea acestor obligații ar putea atrage luarea de către Comisia Federală pentru Comerț a unor măsuri de impunere a respectării**"[42].

Pentru a combate declarațiile false de aderare la sfera de siguranță, politicile de confidențialitate de pe site-urile societăților autocertificate ar trebui să includă întotdeauna un link către site-ul Departamentului Comerțului consacrat sferei de siguranță, unde sunt indicați toți membrii „actuali" ai sistemului. În acest fel, persoanele vizate din Europa vor putea să verifice imediat, fără a efectua căutări suplimentare pe internet, dacă o societate este, în momentul respectiv, membră a sferei de siguranță. Departamentul Comerțului a instituit din martie 2013 obligația ca societățile să respecte această cerință, dar acest proces ar trebui intensificat.

Monitorizarea continuă și asigurarea consecventă de către Comisia Federală pentru Comerț a respectării efective a principiilor sferei de siguranță - în plus față de măsurile luate de Departamentul Comerțului, descrise mai sus - continuă să fie o prioritate esențială pentru a

38 http://www.ftc.gov/os/caselist/0923081/090806karnanicmpt.pdf

39 http://www.ftc.gov/speeches/brill/131029europeaninstituteremarks.pdf și http://www.ftc.gov/speeches/ramirez/131029tacdremarks.pdf

40 Scrisoarea președintelui Comisiei Federale pentru Comerț, doamna Edith Ramirez, adresată vicepreședintelui Comisiei Europene, doamna Viviane Reding.

41 Scrisoarea președintei Comisiei Federale pentru Comerț, Edith Ramirez, adresată vicepreședintei Comisiei Europene,Viviane Reding.

42 „*U.S.-EU Cooperation to Implement the Safe Harbor Framework*", 12 noiembrie 2013.

garanta funcționarea corectă și eficientă a sistemului. În special, este necesară intensificarea **verificărilor și a investigațiilor din oficiu privind conformitatea societăților** cu principiile sferei de siguranță. De asemenea, ar trebui să se ia măsuri suplimentare de facilitare a transmiterii plângerilor către Comisia Federală pentru Comerț.

### 5.2. Grupul UE pentru protecția datelor

Grupul UE pentru protecția datelor este un organism creat în temeiul Deciziei privind sfera de siguranță. Acesta are competența de a investiga plângeri depuse de persoane private în legătură cu datele care le vizează colectate în contextul unui raport de muncă, precum și dosare referitoare la societăți certificate care au ales această opțiune pentru soluționarea litigiilor referitoare la sfera de siguranță (53 % din totalul societăților). Grupul este compus din reprezentanți ai diferitor autorități de protecție a datelor din UE.

Până în prezent, grupul a primit patru plângeri (două în 2010 și două în 2013). Cele două plângeri primite în 2010 au fost transmise autorităților naționale de protecție a datelor (din Regatul Unit și din Elveția). A treia și a patra plângere sunt în curs de examinare. Numărul mic de plângeri poate fi explicat prin faptul că, așa cum se explică mai sus, competențele grupului se limitează în general la un anumit tip de date.

Volumul redus de dosare ar putea fi parțial explicat și de nivelul insuficient de informare cu privire la existența grupului. Din 2004, Comisia a îmbunătățit vizibilitatea informațiilor de pe site-ul său privind grupul[43].

Pentru a mări utilitatea grupului, societățile din SUA care au ales să coopereze cu grupul și să respecte deciziile sale, pentru unele sau pentru toate categoriile de date personale acoperite de autocertificările lor, ar trebui să indice în mod clar și ușor de observat în cadrul politicilor lor de confidențialitate că sunt de acord ca Departamentul Comerțului să supravegheze acest aspect. Pe site-ul fiecărei autorități pentru protecția datelor din UE ar trebui să se creeze o pagină specifică privind sfera de siguranță, pentru a îmbunătăți nivelul de informare al societăților și al persoanelor vizate din Europa.

### 5.3. Îmbunătățirea asigurării respectării

Deficiențele legate de transparență și de asigurarea respectării identificate mai sus determină preocupări ale societăților europene referitoare la impactul negativ al sistemului sferei de siguranță asupra competitivității societăților europene. În cazul în care o societate europeană concurează cu o societate din SUA care este membră a sferei de siguranță dar, în practică, nu aplică principiile acesteia, societatea europeană va avea un dezavantaj concurențial față de societatea respectivă din SUA.

În plus, competența Comisiei Federale pentru Comerț acoperă actele sau practicile neloiale sau înșelătoare „din domeniul comercial sau care afectează comerțul”. Secțiunea 5 din Legea privind Comisia Federală pentru Comerț a instituit excepții de la autoritatea comisiei asupra actelor sau practicilor neloiale sau înșelătoare în ceea ce privește, printre altele,

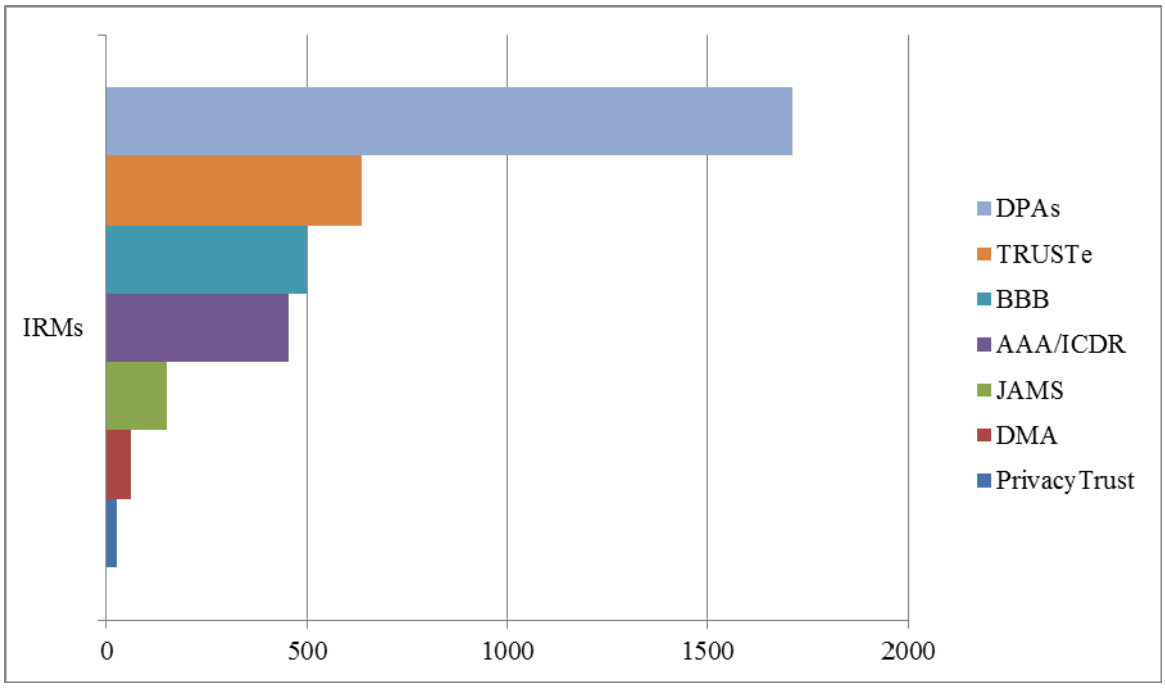
[43] În urma raportului din 2004, o notă de informare redactată de Grupul UE pentru protecția datelor, sub forma unor întrebări și răspunsuri, a fost publicată pe site-ul Comisiei (secțiunea DG Justiție) în scopul de a îmbunătăți nivelul de informare al persoanelor și de a le ajuta să depună o plângere în cazul în care consideră că datele care le vizează au fost prelucrate într-un mod neconform cu sfera de siguranță: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/information_Safe_harbour_en.pdf
Formularul tip pentru depunerea unei plângeri este disponibil la adresa http://ec.europa.eu/justice/policies/privacy/docs/adequacy/complaint_form_en.pdf

**sectorul telecomunicațiilor**. Nefiind supuse competenței Comisiei Federale pentru Comerț în vederea impunerii respectării, societățile de telecomunicații nu pot adera la sfera de siguranță. Cu toate acestea, în contextul convergenței tot mai mari a tehnologiilor și serviciilor, mulți dintre concurenții lor direcți din sectorul TIC din SUA sunt membri ai sferei de siguranță. Excluderea societăților de telecomunicații din schimburile de date din cadrul sferei de siguranță constituie un motiv de preocupare pentru unii operatori de telecomunicații europeni. Potrivit Asociației Europene a Operatorilor de Rețele de Telecomunicații (ETNO), „acest lucru se opune în mod clar celei mai importante cereri a operatorilor de telecomunicații, privind necesitatea de a asigura condiții de concurență echitabile”[44].

## 6. CONSOLIDAREA PRINCIPIILOR PRIVIND CONFIDENȚIALITATEA ALE SFEREI DE SIGURANȚĂ

### 6.1. Procedurile alternative de soluționare a litigiilor

Principiul privind asigurarea respectării solicită existența unor „**mecanisme ușor accesibile și abordabile de tratare a plângerilor**, care să permită examinarea tuturor plângerilor depuse de persoane și a tuturor litigiilor”. În acest scop, sfera de siguranță prevede un sistem de soluționare alternativă a litigiilor (SAL) de către o parte terță independentă[45], care să ofere persoanelor soluții rapide. Cele mai importante trei organisme care oferă mecanisme de tratare a plângerilor sunt Grupul UE pentru protecția datelor, BBB (Better Business Bureaus) și TRUSTe.




44 „Considerațiile ETNO” primite de serviciile Comisiei la 4 octombrie 2013 abordează, de asemenea: 1) definiția datelor cu caracter personal în cadrul sferei de siguranță; 2) lipsa monitorizării sferei de siguranță; 3) faptul că „societățile din SUA pot să transfere date cu mult mai puține restricții decât societățile europene”, ceea ce „constituie o discriminare clară a societăților europene și afectează competitivitatea acestora”. Conform regulilor sferei de siguranță, pentru a comunica informații unei părți terțe, societățile trebuie să aplice principiul notificării și principiul opțiunii. În cazul în care o organizație dorește să transfere informații către o parte terță care acționează ca agent, societatea trebuie fie să se asigure în prealabil că partea terță aderă la principii sau că este supusă dispozițiilor directivei sau altui mecanism de asigurare a conformității, fie să încheie un acord scris cu partea terță, în care să solicite ca partea terță să furnizeze cel puțin același nivel de protecție a confidențialității ca cel cerut de principiile relevante.

45 Directiva 2013/11/UE privind SAL în materie de consum subliniază importanța unor proceduri de soluționare a litigiilor care să fie independente, imparțiale, transparente, eficace, rapide și echitabile.

Utilizarea SAL s-a intensificat din 2004, iar Departamentul Comerțului a consolidat monitorizarea furnizorilor americani de servicii SAL, pentru a se asigura că informațiile oferite de aceștia în legătură cu procedura de depunere a plângerilor este clară, accesibilă și ușor de înțeles. Cu toate acestea, eficacitatea sistemului rămâne a fi demonstrată, având în vedere numărul limitat de dosare tratate până în prezent[46].

Deși Departamentul Comerțului a reușit să obțină reducerea tarifelor furnizorilor de servicii SAL, doi dintre principalii șapte furnizori continuă să perceapă un tarif din partea persoanelor care depun o plângere[47]. Furnizorii respectivi sunt utilizați de circa 20 % dintre societățile care fac parte din sfera de siguranță. Prin urmare, aceste societăți au ales un furnizor de servicii SAL care percepe un tarif din partea consumatorilor care doresc să depună o plângere. Aceste practici nu respectă principiul privind asigurarea respectării prevăzut de sfera de siguranță, conform căruia persoanele au dreptul de a avea acces la „mecanisme independente de tratare a plângerilor ușor accesibile și abordabile". În Uniunea Europeană, accesul la serviciul independent de soluționare a litigiilor oferit de Grupul UE pentru protecția datelor este gratuit pentru toate persoanele vizate.

La 12 noiembrie 2013, Departamentul Comerțului a confirmat că „va continua să sprijine drepturile cetățenilor UE în materie de confidențialitate și să colaboreze cu furnizorii de servicii SAL pentru a examina dacă tarifele acestora pot fi reduse și mai mult".

În ceea ce privește sancțiunile, nu toți furnizorii de servicii SAL dispun de instrumentele necesare pentru remedierea cazurilor de nerespectare a principiilor de confidențialitate. În plus, publicarea constatărilor privind cazurile de nerespectare nu pare a fi inclusă printre sancțiunile și măsurile avute în vedere de furnizorii de servicii SAL.

Furnizorii de servicii SAL trebuie, de asemenea, să transmită dosarele Comisiei Federale pentru Comerț în cazul în care o societate nu se conformează concluziilor procesului de SAL sau respinge decizia furnizorului de servicii SAL, astfel încât Comisia Federală pentru Comerț să examineze, să investigheze și, dacă este necesar, să ia măsuri de asigurare a respectării. Cu toate acestea, până în prezent furnizorii de servicii SAL nu au transmis Comisiei Federale pentru Comerț niciun caz de neconformitate[48].

Furnizorii de servicii SAL publică pe site-urile lor liste cu societățile (participanții la soluționarea litigiilor) care utilizează serviciile lor. Aceste liste permit consumatorilor să verifice cu ușurință dacă - în cazul unui litigiu cu o societate - o persoană poate transmite o plângere unui organism identificat de soluționare a litigiilor. Astfel, de exemplu, BBB publică lista tuturor societăților care au aderat la sistemul de soluționare a litigiilor oferit de acest organism. Cu toate acestea, există un număr mare de societăți care declară că au aderat la un

---

46 De exemplu, unul dintre principalii furnizori de servicii SAL (TRUSTe) a raportat că în 2010 a primit 881 de cereri, dar că numai trei dintre acestea au fost considerate admisibile și întemeiate; societății care a făcut obiectul cererilor respective i s-a solicitat să-și modifice politica de confidențialitate și site-ul. În 2011 s-au primit 879 de cereri, iar într-un caz societății i s-a solicitat să-și modifice politica de confidențialitate. Potrivit Departamentului Comerțului, majoritatea covârșitoare a plângerilor transmise furnizorilor de servicii SAL constituie cereri din partea consumatorilor, de exemplu utilizatori care și-au uitat parola și nu au reușit să o obțină de la furnizorul de servicii internet. La cererea Comisiei, Departamentul Comerțului a elaborat noi criterii de raportare a statisticilor, care să fie utilizate de toți furnizorii SAL. Criteriile fac distincția între simplele cereri, pe de o parte, și plângeri, pe de altă parte, oferind clarificări suplimentare cu privire la tipurile de plângeri primite. Cu toate acestea, noile criterii trebuie să facă obiectul unor discuții suplimentare, pentru a garanta că noile statistici din 2014 vor acoperi toți furnizorii de servicii SAL, vor fi comparabile și vor oferi informații relevante pentru evaluarea eficacității mecanismului de tratare a plângerilor.

47 Centrul Internațional pentru Soluționarea Litigiilor / Asociația Americană de Arbitraj (ICDR/AAA) și JAMS percep un tarif de depunere a dosarului de 200 USD și, respectiv, 250 USD. Departamentul Comerțului a informat Comisia că a colaborat cu AAA, cel mai costisitor furnizor de servicii SAL pentru persoane private, în vederea elaborării unui program specific pentru sfera de siguranță cu costuri reduse pentru consumatori, de la câteva mii de dolari la o sumă fixă de 200 USD.

48 A se vedea întrebarea frecventă nr. 11.

anumit sistem de soluționare a litigiilor, dar nu sunt incluse în listele organismelor de soluționare a litigiilor ca participanți la sistemele oferite de acestea[49].

Mecanismele SAL ar trebui să fie ușor accesibile, independente și abordabile pentru persoanele vizate. O persoană vizată ar trebui să poată depune o plângere fără constrângeri semnificative. Toate organismele SAL ar trebui să publice pe site-urile lor statistici privind plângerile tratate, precum și informații specifice privind rezultatul acestora. În fine, aceste organisme ar trebui monitorizate, pentru a se asigura că informațiile oferite în legătură cu procedura și cu modalitățile de depunere a plângerilor sunt clare și ușor de înțeles, astfel încât soluționarea litigiilor să devină un mecanism eficace și fiabil și să dea rezultate. De asemenea, este oportun să se reamintească faptul că publicarea constatărilor privind nerespectarea ar trebui inclusă printre sancțiunile obligatorii ale organismelor SAL.

### 6.2. Transferul ulterior

În contextul creșterii exponențiale a fluxurilor de date, există necesitatea de a asigura protecția continuă a datelor personale în toate etapele prelucrării datelor, inclusiv în cazul în care datele sunt transferate de către o societate membră a sferei de siguranță pentru a fi **prelucrate de o parte terță**. Prin urmare, necesitatea de a optimiza asigurarea respectării include nu numai membrii sferei de siguranță, ci și subcontractanții acestora.

Sistemul sferei de siguranță permite transferurile ulterioare către părți terțe care acționează în calitate de „agenți" în cazul în care societatea - membră a sferei de siguranță - „certifică faptul că terțul subscrie la principiile «sferei de siguranță» sau se supune dispozițiilor directivei sau altui mecanism care atestă nivelul adecvat de protecție sau în cazul în care încheie un acord scris cu acest terț prin care acesta se angajează să ofere cel puțin același nivel de protecție ca acela prevăzut în principii"[50]. De exemplu, Departamentul Comerțului cere ca un furnizor de servicii de tip cloud să încheie un contract chiar dacă acesta „respectă principiile sferei de siguranță" și primește date personale în vederea prelucrării[51]. Această cerință nu este însă prezentată în mod clar în anexa II la Decizia privind sfera de siguranță.

Având în vedere că în ultimii ani s-a recurs din ce în ce mai frecvent la subcontractanți, în special în contextul serviciilor de tip cloud, atunci când o societate încheie un astfel de contract aceasta ar trebui să notifice Departamentul Comerțului și să fie obligată să facă publice garanțiile în materie de confidențialitate[52].

Cele trei aspecte menționate anterior: mecanismul de soluționare alternativă a litigiilor, supravegherea consolidată și transferurile ulterioare ale datelor ar trebui să fie clarificate suplimentar.

---

49 Exemple: Amazon a informat Departamentul Comerțului că utilizează BBB ca organism de soluționare a litigiilor. Cu toate acestea, Amazon nu a fost inclus de BBB în lista participanților la sistemul său de soluționare a litigiilor. Invers, Arsalon Technologies (www.arsalon.net), un furnizor de cloud hosting, figurează pe lista BBB, însă societatea nu este un membru actual al sferei de siguranță (situația la 1 octombrie 2013). BBB, TRUSTe și alți furnizori de servicii SAL ar trebui să șteargă sau să corecteze informațiile privind certificarea. Aceștia ar trebui să facă obiectul unei obligații de a acorda certificarea numai societăților care sunt membre ale sferei de siguranță.

50 A se vedea Decizia 2000/520/CE a Comisiei, pagina 7 (Transferul ulterior).

51 A se vedea: „*Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing*": http://export.gov/static/Safe%20Harbor%20and%20Cloud%20Computing%20Clarification_April%2012%202013_Latest_eg_main_060351.pdf

52 Aceste observații sunt valabile pentru furnizorii de servicii de tip cloud care nu fac parte din sfera de siguranță. Potrivit firmei de consultanță Galexia, „nivelul de participare la sfera de siguranță (și de respectare) în rândul furnizorilor de servicii de tip cloud este destul de ridicat. Furnizorii de servicii de tip cloud au de obicei mai multe niveluri de protecție a confidențialității, combinând adesea contracte directe cu clienții și politici de confidențialitate generale. Cu una sau două excepții importante, furnizorii de servicii de tip cloud care fac parte din sfera de siguranță respectă principalele dispoziții referitoare la soluționarea litigiilor și la asigurarea respectării. În momentul de față nu există furnizori majori de servicii de tip cloud pe lista declarațiilor false privind statutul de membru." (declarațiile domnului Chris Connolly, Galexia, în cadrul audierii organizate de Comisia LIBE privind „Supravegherea electronică în masă a cetățenilor UE").

## 7. ACCESUL LA DATELE TRANSFERATE ÎN CADRUL SISTEMULUI SFEREI DE SIGURANȚĂ

În cursul anului 2013, informațiile privind amploarea programelor de supraveghere ale SUA au ridicat semne de întrebare cu privire la continuitatea protecției datelor personale transferate în mod legal către SUA în cadrul sistemului sferei de siguranță. De exemplu, toate societățile implicate în programul PRISM și care oferă autorităților din SUA acces la datele stocate și prelucrate în SUA au statutul de societăți certificate în sistemul sferei de siguranță. Din acest motiv, sfera de siguranță a constituit unul dintre canalele prin care s-a permis serviciilor de informații din SUA să colecteze date personale prelucrate inițial în UE.

Decizia privind sfera de siguranță prevede, în anexa 1, că aderarea la principiile de confidențialitate poate fi limitată, dacă acest lucru este justificat de securitatea națională, de interesul public, de cerințe legate de aplicarea legii sau de texte legislative, regulamente administrative sau jurisprudență. Pentru ca limitările și restricțiile referitoare la exercitarea drepturilor fundamentale să fie valabile, acestea trebuie să fie interpretate în mod strict, să fie prevăzute într-un act normativ accesibil publicului și să fie necesare și proporționale într-o societate democratică. În special, Decizia privind sfera de siguranță precizează că aceste limitări sunt permise numai „**în măsura necesară**" pentru îndeplinirea unor cerințe de securitate națională, de interes public sau de aplicare a legii[53]. În timp ce prelucrarea datelor în mod excepțional în scopuri legate de securitatea națională, de interesul public sau de aplicarea legii este prevăzută de sistemul sferei de siguranță, accesul pe scară largă al serviciilor de informații la datele transferate către SUA în contextul unor tranzacții comerciale nu putea fi prevăzut la momentul adoptării sferei de siguranță.

În plus, din motive de transparență și securitate juridică, Departamentul Comerțului ar trebui să notifice Comisiei Europene orice texte legislative sau regulamente administrative care ar afecta aderarea la principiile privind confidențialitatea ale sferei de siguranță[54]. Utilizarea derogărilor ar trebui monitorizată atent, iar acestea nu trebuie utilizate într-un mod care să compromită protecția garantată de **principii**[55]. În special, accesul pe scară largă al autorităților din SUA la datele prelucrate de societățile autocertificate în cadrul sferei de siguranță riscă să compromită confidențialitatea comunicațiilor electronice.

### 7.1. Proporționalitatea și necesitatea

Conform constatărilor Grupului de lucru ad-hoc UE-SUA pentru protecția datelor, o serie de temeiuri juridice din legislația SUA permit colectarea și prelucrarea pe scară largă a datelor cu caracter personal care sunt stocate sau prelucrate de societățile cu sediul în SUA. Acest lucru poate include date transferate anterior din UE către SUA în cadrul sistemului sferei de siguranță și ridică întrebări cu privire la continuarea respectării principiilor sferei de siguranță. Scara largă a acestor programe poate permite ca datele transferate să fie accesate și prelucrate ulterior de către autoritățile SUA depășind ceea ce este strict necesar și proporțional cu

---

53 A se vedea anexa 1 la Decizia privind sfera de siguranță: „Aderarea la aceste principii poate fi limitată de: (a) cerințele privind securitatea națională, interesul public și respectarea legilor; (b) textele legislative, regulamentele administrative sau jurisprudența care creează obligații contradictorii sau prevăd autorizații exprese, cu condiția ca organizația care a recurs la o asemenea autorizație să poată demonstra că nerespectarea principiilor se limitează la măsurile necesare pentru garantarea intereselor legitime superioare pe care această autorizație urmărește să le servească; sau (c) excepțiile sau derogările prevăzute de directivă sau de legislația statului membru, cu condiția ca aceste excepții sau derogări să fie aplicate în contexte comparabile. În conformitate cu obiectivul de a consolida protecția vieții private, organizațiile ar trebui să facă eforturi să aplice aceste principii integral și transparent, inclusiv să indice în politicile lor de confidențialitate domeniile în care excepțiile menționate la litera (b) de mai sus se vor aplica cu regularitate. Din același motiv, atunci când principiile și/sau legile Statelor Unite ale Americii permit organizațiilor să aleagă, acestea sunt invitate să opteze, în limita posibilului, pentru nivelul cel mai înalt de protecție."

54 Avizul nr. 4/2000 privind nivelul de protecție oferit de „principiile sferei de siguranță" adoptat de Grupul de lucru „articolul 29" pentru protecția datelor la 16 mai 2000.

55 Avizul nr. 4/2000 privind nivelul de protecție oferit de „principiile sferei de siguranță" adoptat de Grupul de lucru „articolul 29" pentru protecția datelor la 16 mai 2000.

protecția securității naționale, conform derogării prevăzute de Decizia privind sfera de siguranță.

### 7.2. Limitări și posibilități de remediere

Potrivit constatărilor Grupului de lucru ad-hoc UE-SUA pentru protecția datelor, garanțiile prevăzute de legislația SUA sunt valabile în principal pentru cetățenii SUA sau persoanele care își au reședința legală în această țară. În plus, nu există posibilități pentru persoanele vizate, din UE sau din SUA, să obțină accesul, rectificarea sau ștergerea datelor și nici măsuri reparatorii administrative sau judiciare, în ceea ce privește colectarea și prelucrarea ulterioară a datelor lor personale în cadrul programelor de supraveghere ale SUA.

### 7.3. Transparență

Societățile nu indică în mod sistematic în politicile lor de confidențialitate când aplică derogări de la principii. Prin urmare, persoanele și societățile nu sunt informate în legătură cu modul în care sunt utilizate datele lor. Acest lucru este deosebit de relevant în raport cu desfășurarea programelor de supraveghere ale SUA. Astfel, europenii ale căror date sunt transferate către o societate din SUA în temeiul sferei de siguranță pot să nu fie informați de societățile respective că accesul la datele respective este posibil[56]. Acest lucru ridică întrebări în legătură cu respectarea principiilor sferei de siguranță privind transparența. Transparența ar trebui garantată în cea mai mare măsură posibilă fără a compromite securitatea națională. Pe lângă cerința existentă ca societățile să indice în politicile lor de confidențialitate cazurile în care principiile pot fi limitate de texte legislative, regulamente administrative sau jurisprudență, ele ar trebui să fie încurajate să indice, de asemenea, în politicile lor de confidențialitate cazurile în care aplică derogări de la principii pentru a îndeplini cerințe legate de securitatea națională, de interesul public sau de aplicarea legii.

## 8. CONCLUZII ȘI RECOMANDĂRI

De la adoptarea sa, în 2000, sfera de siguranță a devenit un mijloc de transmitere a fluxurilor de date cu caracter personal între UE și SUA. Necesitatea unei protecții eficiente în cazul transferurilor de date cu caracter personal a devenit mai importantă ca urmare a creșterii exponențiale a fluxurilor de date cu o importanță majoră pentru economia digitală, precum și a evoluțiilor semnificative în ceea ce privește colectarea, prelucrarea și utilizarea datelor. Furnizorii de servicii internet precum Google, Facebook, Microsoft, Apple sau Yahoo au sute de milioane de clienți în Europa și transferă date personale în vederea prelucrării în SUA pe o scară care era de neconceput în 2000, când a fost creată sfera de siguranță.

Din cauza deficiențelor privind transparența și asigurarea respectării acordului, continuă să existe probleme specifice care ar trebui abordate:

a) transparența politicilor de confidențialitate ale membrilor sferei de siguranță;

b) aplicarea efectivă a principiilor privind confidențialitatea de către societățile din SUA și

c) asigurarea eficace a respectării.

---

56 Unele societăți europene care fac parte din sfera de siguranță oferă informații relativ transparente în această privință. De exemplu, Nokia, care are activități în SUA și este membră a sferei de siguranță, a inclus în politica sa de confidențialitate următorul aviz: *„Putem fi obligați, potrivit prevederilor legale obligatorii, să dezvăluim datele dumneavoastră cu caracter personal către anumite autorități sau alți terți, de exemplu, către autoritățile competente să aplice legea din țările unde ne desfășurăm activitatea noi sau terții care acționează în numele nostru."*

În plus, **accesul pe scară largă al serviciilor de informații la datele transferate către SUA de societățile certificate în sistemul sferei de siguranță** ridică întrebări suplimentare importante cu privire la continuitatea respectării drepturilor în materie de protecție a datelor ale cetățenilor europeni atunci când datele lor sunt transferate către SUA.

Pe baza celor de mai sus, Comisia formulează următoarele **recomandări**.

**Transparență**

1. *Societățile autocertificate ar trebui să facă publice politicile lor de confidențialitate.* Nu este suficient ca societățile să transmită Departamentului Comerțului o descriere a politicii lor de confidențialitate. Politicile de confidențialitate ar trebui să fie făcute publice pe site-urile societăților, într-un limbaj clar și ușor de înțeles.

2. *Politicile de confidențialitate de pe site-urile societăților autocertificate ar trebui să includă întotdeauna un link către site-ul Departamentului Comerțului consacrat sferei de siguranță, unde sunt indicați toți membrii „actuali" ai sistemului.* În acest fel, persoanele vizate din Europa vor putea să verifice imediat, fără a efectua căutări suplimentare pe internet, dacă o societate este, în momentul respectiv, membră a sferei de siguranță. Acest lucru ar contribui la îmbunătățirea nivelului de credibilitate al sistemului, prin reducerea posibilității de a face declarații false privind aderarea la sfera de siguranță. Departamentul Comerțului a instituit din martie 2013 obligația ca societățile să respecte această cerință, dar acest proces ar trebui intensificat.

3. *Societățile autocertificate ar trebui să publice condițiile privind confidențialitatea pe care le aplică în contractele încheiate cu subcontractanți, de exemplu cu servicii informatice de tip cloud.* Sfera de siguranță permite transferuri ulterioare de la societăți certificate în sistemul de siguranță către părți terțe care acționează ca „agenți", de exemplu furnizori de servicii de tip cloud. Conform interpretării noastre, în astfel de cazuri Departamentul Comerțului solicită ca societățile autocertificate să încheie un contract. Cu toate acestea, în momentul încheierii unui astfel de contract, o societate membră a sferei de siguranță ar trebui să notifice, de asemenea, Departamentul Comerțului și să fie obligată să publice garanțiile în materie de confidențialitate.

4. *Indicarea clară pe site-ul Departamentului Comerțului a tuturor societăților care nu sunt membri actuali ai sistemului.* Statutul „neactual" din cadrul listei Departamentului Comerțului privind membrii sferei de siguranță ar trebui să fie însoțit de un avertisment clar cu privire la faptul că o societate nu îndeplinește la momentul respectiv cerințele sferei de siguranță. Cu toate acestea, în cazul statutului „neactual", societatea este obligată să continue să aplice cerințele sferei de siguranță pentru datele pe care le-a primit în temeiul acestui sistem.

**Măsuri reparatorii**

5. *Politicile de confidențialitate de pe site-urile societăților ar trebui să includă un link către furnizorul unui mecanism de soluționare alternativă a litigiilor (SAL) și/sau către grupul UE.* Acest lucru va permite cetățenilor europeni vizați ca, în cazul în care se confruntă cu probleme, să contacteze imediat organismul SAL sau grupul UE. Departamentul Comerțului a instituit din martie 2013 obligația ca societățile să respecte această cerință, dar acest proces ar trebui intensificat.

6. *Soluționarea alternativă a litigiilor ar trebui să fie ușor accesibilă și abordabilă.* Unele organisme de soluționare alternativă a litigiilor din cadrul sistemului sferei de siguranță continuă să perceapă tarife - care pot fi destul de ridicate pentru utilizatorii individuali - pentru tratarea unei plângeri (între 200 și 250 USD). În schimb, în Europa accesul la Grupul pentru protecția datelor, în vederea soluționării plângerilor referitoare la sfera de siguranță, este gratuit.

7. *Departamentul Comerțului ar trebui să monitorizeze mai sistematic furnizorii de mecanisme de soluționare alternativă a litigiilor, în ceea ce privește transparența și accesibilitatea informațiilor oferite de aceștia în legătură cu procedura utilizată și măsurile luate ca urmare a plângerilor primite.* În acest fel s-ar asigura faptul că soluționarea litigiilor este un mecanism eficace, fiabil și care dă rezultate. De asemenea, este oportun să se reamintească faptul că publicarea constatărilor privind nerespectarea ar trebui inclusă printre sancțiunile obligatorii ale organismelor SAL.

**Asigurarea respectării**

8. *Ca urmare a certificării sau a recertificării societăților în cadrul sferei de siguranță, un anumit procent dintre aceste societăți ar trebui să facă obiectul unor investigații din oficiu privind respectarea efectivă a politicilor lor în materie de confidențialitate (care să nu se limiteze la respectarea cerințelor formale).*

9. *Ori de câte ori este detectat un caz de neconformitate, în urma unei plângeri sau a unei investigații, societatea ar trebui să facă obiectul unor investigații ulterioare specifice după un an.*

10. *În cazul unor îndoieli cu privire la conformitatea unei societăți sau al existenței unor plângeri în curs de soluționare, Departamentul Comerțului ar trebui să informeze autoritatea pentru protecția datelor competentă din UE.*

11. *Declarațiile false privind aderarea la sfera de siguranță ar trebui să fie investigate în continuare.* O societate care declară pe site-ul său că respectă cerințele sferei de siguranță, dar nu este inclusă în lista Departamentului Comerțului ca membru „actual” al sistemului înșeală consumatorii și abuzează de încrederea acestora. Afirmațiile false compromit credibilitatea sistemului în ansamblul său și, prin urmare, ar trebui eliminate imediat de pe site-urile societăților.

**Accesul de către autoritățile SUA**

12. *Politicile de confidențialitate ale societăților autocertificate ar trebui să includă informații cu privire la măsura în care legislația SUA permite autorităților publice să colecteze și să prelucreze datele transferate în cadrul sferei de siguranță. În special, societățile ar trebui încurajate să indice în politicile lor de confidențialitate cazurile în care aplică derogări de la principii pentru a îndeplini cerințe legate de securitatea națională, de interesul public sau de aplicarea legii.*

*13 .Este important ca derogarea pe motive de securitate națională prevăzută de Decizia privind sfera de siguranță să fie utilizată numai în măsura în care acest lucru este strict necesar sau proporțional.*