II

(Acte fără caracter legislativ)

DECIZII

DECIZIA DE PUNERE ÎN APLICARE (UE) 2016/1250 A COMISIEI

din 12 iulie 2016

în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind caracterul adecvat al protecției oferite de Scutul de confidențialitate UE-SUA

[notificată cu numărul C(2016) 4176]

(Text cu relevanță pentru SEE)

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere 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 ([1]), în special articolul 25 alineatul (6),

după consultarea Autorității Europene pentru Protecția Datelor ([2]),

1. INTRODUCERE

(1) Directiva 95/46/CE stabilește normele privind transferurile de date cu caracter personal din statele membre către țările terțe, în măsura în care astfel de transferuri intră în domeniul de aplicare a directivei.

(2) Articolul 1 din Directiva 95/46/CE și considerentele 2 și 10 din preambulul acesteia urmăresc să asigure nu numai protecția eficace și completă a drepturilor și libertăților fundamentale ale persoanelor fizice, în special dreptul fundamental la respectarea vieții private în ceea ce privește prelucrarea datelor cu caracter personal, ci și un nivel ridicat de protecție a drepturilor și libertăților fundamentale ([3]).

(3) Importanța dreptului fundamental la respectarea vieții private, garantat de articolul 7, precum și a dreptului fundamental la protecția datelor cu caracter personal, garantat de articolul 8 din Carta drepturilor fundamentale a Uniunii Europene, a fost subliniată în jurisprudența Curții de Justiție ([4]).

(4) În conformitate cu articolul 25 alineatul (1) din Directiva 95/46/CE, statele membre trebuie să prevadă că transferul de date cu caracter personal către o țară terță poate avea loc numai în cazul în care țara terță în cauză asigură un nivel adecvat de protecție și legislațiile statelor membre care pun în aplicare alte dispoziții ale directivei sunt respectate înainte de transfer. Comisia poate constata că o țară terță asigură un nivel adecvat de protecție prin legislația sa internă sau prin angajamentele internaționale pe care și le-a asumat pentru a proteja drepturile persoanelor fizice. În acest caz și fără a aduce atingere conformității cu dispozițiile naționale adoptate în temeiul altor dispoziții ale directivei, datele cu caracter personal pot fi transferate din statele membre fără să fie nevoie de garanții suplimentare.

([1]) JO L 281, 23.11.1995, p. 31.
([2]) A se vedea Avizul 4/2016 referitor la Proiectul de decizie privind caracterul adecvat al Scutului de confidențialitate UE-SUA, publicat la 30 mai 2016.
([3]) Cauza C-362/14, *Maximillian Schrems/Comisarul pentru protecția datelor* (denumită în continuare „Schrems"), EU:C:2015:650, punctul 39.
([4]) Cauza C-553/07, *Rijkeboer*, EU:C:2009:293, punctul 47; cauzele conexe C-293/12 și C-594/12, *Digital Rights Ireland și alții*, EU:C:2014:238, punctul 53; cauza C-131/12, *Google Spain și Google*, EU:C:2014:317, punctele 53, 66 și 74.

(5) În conformitate cu articolul 25 alineatul (2) din Directiva 95/46/CE, nivelul de protecție a datelor oferit de o țară terță trebuie evaluat ținând seama de toate circumstanțele referitoare la o operațiune de transfer de date sau un set de operațiuni de transfer de date, inclusiv normele de drept atât generale, cât și sectoriale în vigoare în țara terță în cauză.

(6) În Decizia 2000/520/CE a Comisiei ([5]), în sensul articolului 25 alineatul (2) din Directiva 95/46/CE, „principiile" sferei de siguranță „privind protecția vieții private", puse în aplicare în conformitate cu orientările oferite de așa-numitele „întrebări de bază" publicate de Departamentul Comerțului al SUA, au fost examinate pentru a asigura un nivel adecvat de protecție a datelor cu caracter personal transferate din Uniune către organizații stabilite în Statele Unite ale Americii.

(7) În comunicările sale COM(2013) 846 final ([6]) și COM(2013) 847 final din 27 noiembrie 2013 ([7]), Comisia a considerat că baza fundamentală a programului privind sfera de siguranță ar trebui să fie revizuită și consolidată în contextul unei serii de factori, inclusiv creșterea exponențială a fluxurilor de date și importanța critică a acestora pentru economia transatlantică, creșterea rapidă a numărului de companii din SUA care aderă la sistemul sferei de siguranță și noile informații privind amploarea și domeniul de aplicare a anumitor programe americane de informații care au ridicat semne de întrebare cu privire la nivelul de protecție pe care acestea îl pot garanta. În plus, Comisia a identificat o serie de lipsuri și deficiențe în cadrul sistemului sferei de siguranță.

(8) Pe baza elementelor de probă colectate de Comisie, inclusiv informațiile care rezultă din activitatea Grupului de contact UE-SUA privind protecția vieții private ([8]) și informațiile cu privire la programele americane de informații primite în cadrul Grupului de lucru ad-hoc UE-SUA ([9]), Comisia a formulat 13 recomandări pentru o revizuire a sistemului sferei de siguranță. Recomandările s-au axat pe consolidarea principiilor esențiale privind protecția vieții private, sporirea transparenței politicilor de confidențialitate ale companiilor autocertificate din SUA, o mai bună supraveghere, monitorizare și punere în aplicare de către autoritățile americane a respectării acestor principii, disponibilitatea unor mecanisme de soluționare a litigiilor, precum și necesitatea de a se asigura că utilizarea excepției pe motivul securității naționale prevăzute în Decizia 2000/520/CE este limitată la măsura în care acest lucru este strict necesar și proporțional.

(9) În hotărârea sa din 6 octombrie 2015 în cauza C-362/14, *Maximillian Schrems/Data Protection Commissioner* ([10]), Curtea de Justiție a Uniunii Europene a declarat invalidă Decizia 2000/520/CE. Fără a examina conținutul principiilor „sferei de siguranță" privind protecția vieții private, Curtea a considerat că, în decizia respectivă, Comisia nu a indicat că Statele Unite „a asigurat" efectiv un nivel adecvat de protecție prin legislația sa internă sau prin angajamentele sale internaționale ([11]).

(10) În această privință, Curtea a precizat că, deși termenul de „nivel de protecție adecvat" de la articolul 25 alineatul (6) din Directiva 95/46/CE nu presupune un nivel de protecție identic cu cel garantat în cadrul ordinii juridice a Uniunii, acesta trebuie să fie înțeles ca o solicitare ca țara terță să asigure un nivel de protecție a drepturilor și libertăților fundamentale „în esență, echivalent" cu cel garantat în interiorul Uniunii în temeiul Directivei 95/46/CE, interpretată având în vedere Carta drepturilor fundamentale. Chiar dacă mijloacele la care țara terță a recurs, în această privință, pot fi diferite de cele utilizate în cadrul Uniunii, aceste mijloace trebuie totuși să se dovedească, în practică, efective ([12]).

(11) Curtea de Justiție a criticat lipsa de constatări suficiente în Decizia 2000/520/CE cu privire la existența, în Statele Unite, a unor norme cu caracter statal destinate să limiteze eventualele ingerințe în drepturile fundamentale ale persoanelor ale căror date sunt transferate din Uniune către Statele Unite, ingerințe în care entitățile de stat din țara respectivă ar fi autorizate să se implice atunci când urmăresc obiective legitime cum ar fi securitatea națională, precum și la protecția juridică eficientă împotriva unor ingerințe de această natură ([13]).

([5]) Decizia 2000/520/CE a Comisiei din 26 iulie 2000 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind caracterul adecvat al protecției oferite de principiile „sferei de siguranță" privind protecția vieții private și întrebările de bază aferente, publicate de Departamentul Comerțului al S.U.A. (JO L 215, 28.8.2000, p. 7).

([6]) Comunicarea Comisiei către Parlamentul European și Consiliu: restabilirea încrederii în fluxurile de date dintre UE și SUA, COM(2013) 846 final din 27 noiembrie 2013.

([7]) Comunicarea Comisiei către Parlamentul European și Consiliu privind funcționarea „sferei de siguranță" din punctul de vedere al cetățenilor UE și al întreprinderilor stabilite în UE, COM(2013) 847 final din 27 noiembrie 2013.

([8]) A se vedea, de exemplu, Consiliul Uniunii Europene, Raportul final al Grupului de contact la nivel înalt UE-SUA privind schimbul de informații, confidențialitatea și protecția datelor cu caracter personal, în nota 9831/08 din 28 mai 2008, disponibil pe internet la adresa: http://www.europarl.europa.eu/document/activities/cont/201010/20101019ATT88359/20101019ATT88359EN.pdf.

([9]) Raportul privind concluziile copreședinților din partea UE în cadrul Grupului de lucru ad-hoc UE-SUA privind protecția datelor, 27 noiembrie 2013, disponibil pe internet la adresa: http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf.

([10]) A se vedea nota de subsol 3.

([11]) *Schrems*, punctul 97.

([12]) Schrems, punctele 73-74.

([13]) *Schrems*, punctele 88-89.

(12) În 2014, Comisia a participat la discuții cu autoritățile SUA pentru a discuta consolidarea sistemului sferei de siguranță în conformitate cu cele 13 recomandări conținute în comunicarea COM(2013) 847 final. În urma hotărârii Curții de Justiție a Uniunii Europene în cauza Schrems, discuțiile au fost intensificate, pentru a se ajunge la o eventuală nouă decizie privind caracterul adecvat care să îndeplinească cerințele prevăzute la articolul 25 din Directiva 95/46/CE, astfel cum a fost interpretată de Curtea de Justiție. Documentele anexate la prezenta decizie și care vor fi publicate, de asemenea, în Registrul federal al SUA sunt rezultatul acestor discuții. Principiile privind protecția vieții private (anexa II), împreună cu declarațiile și angajamentele oficiale ale autorităților americane conținute în documentele din anexa I și anexele III-VII, constituie „Scutul de confidențialitate UE-SUA".

(13) Comisia a analizat cu atenție legislația și practica din SUA, inclusiv respectivele declarații și angajamente oficiale. Pe baza constatărilor dezvoltate în considerentele 136-140, Comisia concluzionează că Statele Unite garantează un nivel adecvat de protecție a datelor cu caracter personal transferate în temeiul Scutului de confidențialitate din UE către organizațiile autocertificate din Statele Unite.

2. „SCUTUL DE CONFIDENȚIALITATE UE-SUA"

(14) Scutul de confidențialitate UE-SUA se bazează pe un sistem de autocertificare prin care organizațiile din SUA se angajează să respecte un set de principii privind protecția vieții private – Principiile cadrului privind scutul de confidențialitate UE-SUA, inclusiv principiile suplimentare (denumite în continuare, împreună: „Principiile"), emise de Departamentul Comerțului al SUA și enunțate în anexa II la prezenta decizie. Acest set se aplică atât operatorilor, cât și persoanelor împuternicite de către operatori (agenți), cu particularitatea că operatorii trebuie să fie obligați prin contract să acționeze numai la instrucțiunile operatorului din UE și furnizează asistență operatorilor pentru a le răspunde persoanelor fizice care își exercită drepturile în conformitate cu principiile ([14]).

(15) Fără a aduce atingere conformității cu dispozițiile naționale adoptate în temeiul Directivei 95/46/CE, prezenta decizie are drept efect faptul că sunt permise transferurile de la un operator sau de la o persoană împuternicită de operator în Uniune către organizații din SUA care și-au autocertificat adeziunea la principii către Departamentul Comerțului și s-au angajat să le respecte. Principiile se aplică numai în ceea ce privește prelucrarea datelor cu caracter personal de către organizația din SUA în măsura în care prelucrarea de către astfel de organizații nu intră în domeniul de aplicare al legislației Uniunii ([15]). Scutul de confidențialitate nu aduce atingere aplicării legislației Uniunii care reglementează prelucrarea datelor cu caracter personal în statele membre ([16]).

([14]) A se vedea anexa II, punctul III.10.a. În conformitate cu definiția de la punctul I.8.c, operatorul din UE va stabili scopul și mijloacele de prelucrare a datelor cu caracter personal. În plus, contractul încheiat cu agentul trebuie să indice în mod clar dacă transferurile ulterioare sunt autorizate (a se vedea punctul III.10.a.ii.2).

([15]) Aceasta se aplică, de asemenea, în cazul în care sunt vizate date privind resursele umane transferate din Uniune în cadrul unui raport de muncă. Deși Principiile subliniază „responsabilitatea principală" a angajatorului din UE (a se vedea anexa II, punctul III.9.d.i.), ele clarifică totodată faptul că nu principiile, ci normele aplicabile în Uniune și/sau în statul membru respectiv vor reglementa comportamentul angajatorului. A se vedea anexa II, punctul III.9.a.i., b.ii., c.i., d.i.

([16]) Acest lucru este valabil și pentru prelucrarea care are loc prin utilizarea echipamentului situat în Uniune, dar utilizate de o organizație stabilită în afara Uniunii [a se vedea articolul 4 alineatul (1) litera (c) din Directiva 95/46/CE]. Începând cu 25 mai 2018, Regulamentul general privind protecția datelor (*General Data Protection Regulation* – GDPR) se va aplica prelucrării datelor cu caracter personal: (i) în cadrul activităților unui sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii (chiar și în cazul în care prelucrarea are loc în Statele Unite); sau (ii) ale unor persoane vizate care se află în Uniune, de către un operator sau o persoană împuternicită de operator care nu este stabilită în Uniune, în cazul în care activitățile de prelucrare sunt legate de: (a) oferirea de bunuri sau servicii, indiferent dacă persoana în cauză trebuie să plătească pentru acestea, unor astfel de persoane vizate în Uniune; sau (b) monitorizarea comportamentului lor, în măsură în care acest comportament se manifestă în Uniune. A se vedea articolul 3 alineatele (1)-(2) din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

(16) Protecția acordată datelor cu caracter personal prin Scutul de confidențialitate se aplică oricărei persoane vizate din UE ([17]) ale cărei date cu caracter personal au fost transferate din Uniune către organizații din SUA care și-au autocertificat adeziunea la principii către Departamentul Comerțului.

(17) Principiile se aplică imediat după certificare. Unica excepție se referă la principiul responsabilității pentru transferurile ulterioare, în cazul în care o organizație care își autocertifică adeziunea la Scutul de confidențialitate are deja relații comerciale preexistente cu părți terțe. Dat fiind că ar putea fi necesară o anumită perioadă de timp pentru ca aceste relații comerciale să se conformeze la normele aplicabile în conformitate cu principiul responsabilității pentru transferul ulterior, organizația va fi obligată să asigure conformitatea cât mai curând posibil și, în orice caz, nu mai târziu de nouă luni de la autocertificare (cu condiția ca asigurarea conformității să aibă loc în primele două luni de la data la care Scutul de confidențialitate devine efectiv). În această perioadă intermediară, organizația trebuie să aplice principiul notificării și principiul opțiunii (permițând astfel persoanei vizate din UE să beneficieze de posibilitatea de renunțare) și, în cazul în care se transferă date cu caracter personal către o parte terță care acționează ca agent, trebuie să se asigure că aceasta din urmă oferă cel puțin același nivel de protecție ca cel impus de principii ([18]). Această perioadă de tranziție stabilește un echilibru rezonabil și adecvat între respectarea dreptului fundamental la protecția datelor și nevoile legitime ale întreprinderilor de a dispune de suficient timp pentru a se adapta la noul cadru, în cazul în care această adaptare depinde, de asemenea, de relațiile lor comerciale cu părți terțe.

(18) Acest sistem va fi gestionat și monitorizat de Departamentul Comerțului, pe baza angajamentelor sale stabilite în cadrul declarațiilor Secretarului american al comerțului (anexa I la prezenta decizie). În ceea ce privește punerea în aplicare a principiilor, Comisia Federală pentru Comerț (FTC) și Departamentul Transporturilor au făcut declarații care figurează în anexa IV și în anexa V la prezenta decizie.

2.1. *Principii în materie de protecție a vieții private*

(19) Ca parte a autocertificării acestora în temeiul Scutului pentru confidențialitate UESUA, organizațiile trebuie să se angajeze să respecte principiile ([19]).

(20) În temeiul *principiului notificării*, organizațiile sunt obligate să furnizeze informații persoanelor vizate cu privire la o serie de elemente esențiale referitoare la prelucrarea datelor lor cu caracter personal (de exemplu, tipul de date colectate, scopul prelucrării, dreptul de acces și de opțiune, condițiile pentru transferurile ulterioare și răspunderea). Se aplică garanții suplimentare, în special cerința ca organizațiile să facă publice politicile lor de confidențialitate (care reflectă principiile) și să pună la dispoziție link-uri către site-ul Departamentului Comerțului (detalii suplimentare cu privire la autocertificare, drepturile persoanelor vizate și mecanisme de recurs disponibile), către lista Scutului de confidențialitate la care se face referire în considerentul 30 și către site-ul unui furnizor corespunzător de mecanisme alternative de soluționare a litigiilor.

(21) În conformitate cu *principiul integrității datelor și limitării scopului*, datele cu caracter personal trebuie limitate la ceea ce este pertinent în scopul prelucrării, trebuie să fie fiabile pentru utilizarea prestabilită a acestora, exacte, complete și actualizate. O organizație nu poate prelucra date cu caracter personal într-un mod incompatibil cu scopul pentru care acestea au fost colectate sau cu scopurile aprobate ulterior de persoana în cauză. Organizațiile trebuie să se asigure că datele cu caracter personal sunt fiabile pentru utilizarea lor prestabilită, exacte, complete și actualizate..

([17]) Prezenta decizie are relevanță pentru SEE. Acordul privind Spațiul Economic European (Acordul privind SEE) prevede extinderea pieței interne a Uniunii Europene la cele trei state SEE, și anume Islanda, Liechtenstein și Norvegia. Legislația Uniunii privind protecția datelor, inclusiv Directiva 95/46/CE, intră sub incidența Acordului SEE și a fost încorporată în anexa XI la acesta. Comitetul mixt al SEE trebuie să decidă cu privire la încorporarea prezentei decizii în Acordul privind SEE. Odată ce prezenta decizie se aplică Islandei, Liechtensteinului și Norvegiei, Scutul de confidențialitate UE-SUA va acoperi, de asemenea, aceste trei țări, iar trimiterile din pachetul privind Scutul de confidențialitate la UE și statele sale membre se interpretează ca incluzând Islanda, Liechtenstein și Norvegia.

([18]) A se vedea anexa II, punctul III.6.e.

([19]) Pentru datele privind resursele umane colectate în contextul ocupării unui loc de muncă, se aplică norme speciale care oferă garanții suplimentare, astfel cum sunt stabilite în principiul suplimentar referitor la „datele privind resursele umane"din principiile privind protecția vieții private (a se vedea anexa II, punctul III.9). De exemplu, angajatorii ar trebui să țină seama de preferințele angajaților cu privire la protecția vieții private prin restricționarea accesului la datele cu caracter personal, anonimizarea anumitor date sau atribuirea de coduri sau pseudonime. În primul rând, organizațiile sunt obligate să coopereze și să respecte recomandările făcute de autoritățile însărcinate cu protecția datelor din Uniunea Europeană în ceea ce privește astfel de date.

(22) În cazul în care prelucrarea are un nou scop (modificat) care diferă în mod semnificativ de scopul inițial, dar rămâne totuși compatibil cu acesta, *principiul opțiunii* conferă persoanelor vizate dreptul de opoziție (renunțare). *Principiul opțiunii* nu înlocuiește interdicția explicită privind prelucrarea incompatibilă ([20]). Norme speciale care permit exercitarea dreptului de renunțare „în orice moment" la utilizarea datelor cu caracter personal se aplică utilizării de date cu caracter personal în scopuri de marketing direct ([21]). În cazul datelor sensibile, organizațiile trebuie să obțină în mod normal consimțământul explicit al persoanei vizate (accept).

(23) Tot în temeiul *principiul integrității datelor și limitării scopului*, informațiile cu caracter personal pot fi stocate într-o formă care identifică o persoană sau permite identificarea sa (așadar, sub formă de date cu caracter personal) numai atât timp cât această stocare servește atingerii scopului (scopurilor) în care informațiile au fost culese inițial sau a scopurilor aprobate ulterior. Această obligație nu împiedică organizațiile aderente la Scutul de confidențialitate să continue prelucrarea informațiilor cu caracter personal pe perioade mai lungi, dar numai pe perioada și în măsura în care o astfel de prelucrare servește în mod rezonabil la atingerea unuia dintre următoarele scopuri specifice: arhivarea în interes public, jurnalismul, literatura și arta, cercetarea științifică și istorică și analiza statistică. Păstrarea pe o perioadă mai îndelungată a datelor cu caracter personal într-unul din aceste scopuri va avea loc în conformitate cu garanțiile prevăzute de principii.

(24) În conformitate cu *principiul securității*, organizațiile care creează, administrează, utilizează sau difuzează date cu caracter personal trebuie să adopte măsuri de securitate „rezonabile și adecvate", ținând seama de riscurile implicate în procesul de prelucrare, precum și de natura datelor. În cazul subcontractării serviciilor de prelucrare a datelor, organizațiile trebuie să încheie un contract cu subcontractantul care garantează același nivel de protecție în conformitate cu principiile și ia măsuri pentru a asigura punerea în aplicare corespunzătoare a acestuia.

(25) În conformitate cu *principiul accesului* ([22]), persoanele vizate au dreptul, fără necesitatea unei justificări și numai pe baza unei taxe neexcesive, să obțină din partea unei organizații confirmarea dacă aceasta prelucrează date cu caracter personal referitoare la acestea și să dispună comunicarea datelor într-un interval de timp rezonabil. Acest drept poate fi restrâns numai în circumstanțe excepționale; orice refuz sau limitare a dreptului de acces trebuie să fie necesar și justificat în mod corespunzător, organizația având sarcina de a demonstra că aceste cerințe sunt îndeplinite. Persoanele vizate trebuie să poată corecta, modifica sau șterge date cu caracter personal în cazul în care acestea sunt inexacte sau au fost prelucrate cu încălcarea principiilor. În domeniile în care întreprinderile recurg, cel mai probabil, la prelucrarea automatizată a datelor cu caracter personal pentru a lua decizii care afectează persoanele (de exemplu, acordarea de credite, oferte de credite ipotecare, ocuparea forței de muncă), legislația SUA oferă măsuri specifice de protecție specifică împotriva deciziilor nefavorabile ([23]). Aceste acte prevăd, de regulă, că persoanele au dreptul de a fi informate cu privire la motivele specifice care au stat la baza deciziei (de exemplu, refuzarea unui credit), de a contesta informațiile incomplete sau inexacte (precum și faptul că decizia s-a bazat pe factori ilegali) și de a exercita căi de atac împotriva deciziei nefavorabile. Aceste norme oferă protecție în cazurile – probabil, destul de rare – în care ar deciziile automatizate ar fi luate de organizații aderente la Scutul de confidențialitate ([24]). Cu toate acestea, având în vedere utilizarea tot mai răspândită a prelucrării automatizate (inclusiv crearea de profiluri) ca bază pentru luarea de decizii care privesc persoanele în economia digitală modernă, acesta este un domeniu care trebuie să fie monitorizat îndeaproape. Pentru a facilita această monitorizare, s-a convenit cu autoritățile SUA ca prima reexaminare anuală, precum și revizuirile ulterioare, după caz, să cuprindă un dialog cu privire la procesul decizional automatizat, inclusiv un schimb de opinii cu privire la similitudinile și diferențele dintre abordările practicate de UE și, respectiv, de SUA în acest sens.

([20]) Acest lucru este valabil pentru toate transferurile de date în temeiul Scutului de confidențialitate, inclusiv în cazul în care acestea vizează date colectate prin intermediul raportului de muncă. Deși o organizație autocertificată din SUA ar putea, în principiu, să utilizeze date privind resursele umane în scopuri diferite, care nu au legătură cu raportul de muncă (de exemplu, pentru anumite comunicații comerciale), aceasta trebuie să respecte interdicția privind prelucrarea incompatibilă și, în plus, poate face acest lucru numai în conformitate cu *principiile notificării și opțiunii*. Interdicția impusă organizației din SUA de a lua sancțiuni împotriva angajatului pentru exercitarea unor astfel de opțiuni, inclusiv orice restrângere a oportunităților profesionale, va oferi asigurarea că, în pofida raportului de subordonare și dependenței inerente, angajatul nu va fi supus niciunei presiuni și poate exercita, astfel, o veritabilă libertate de alegere.

([21]) A se vedea anexa II, punctul III.12.

([22]) A se vedea, de asemenea, principiul suplimentar privind „accesul" (anexa II, punctul III.8).

([23]) A se vedea, de exemplu, Legea privind egalitatea de șanse în materie de credit (*Equal Credit Opportunity Act* – ECOA, 15 U.S.C., 1691 et seq.), Legea privind imparțialitatea rapoartelor privind solvabilitatea creditorilor (*Fair Credit Reporting Act* – FRCA, 15 USC § 1681 et seq.), Legea privind egalitatea de șanse în materie de locuințe sau Fair (*Fair Housing Act* – FHA, 42 U.S.C. 3601 et seq.).

([24]) În contextul unui transfer de date cu caracter personal care au fost colectate în UE, persoana fizică (clientul) se va afla, în majoritatea cazurilor, într-o relație contractuală cu controlorul de date din UE, care trebuie să respecte normele UE de protecție a datelor. Astfel, orice decizie bazată pe prelucrarea automată va fi, de regulă, luate de către controlorul din UE. Acest context include scenariile în care prelucrarea este efectuată de o organizație aderentă la Scutul de confidențialitate care acționează ca agent în numele operatorului din UE.

(26) În temeiul *principiului recursului, punerii în aplicare și responsabilității* ([25]), organizațiile participante trebuie să pună la dispoziție mecanisme solide pentru a asigura respectarea principiilor privind protecția vieții private și alte căi de atac pentru cetățenii UE ale căror date cu caracter personal au fost prelucrate într-un mod neconform, inclusiv căi de atac eficiente. Odată ce o organizație a decis în mod voluntar să se autocertifice ([26]) în temeiul Scutului de confidențialitate UE-SUA, respectarea efectivă a principiilor este obligatorie. Pentru a avea în continuare dreptul să beneficieze de protecția vieții private să primească date cu caracter personal din partea Uniunii, organizațiile trebuie să își recertifice anual participarea la cadru. De asemenea, organizațiile trebuie să ia măsuri pentru a verifica ([27]) dacă politicile de confidențialitate publicate sunt conforme cu principiile și sunt respectate efectiv. Acest lucru poate fi realizat fie prin intermediul unui sistem de autoevaluare, care trebuie să includă proceduri interne care asigură că angajații beneficiază de formare privind punerea în aplicare a politicilor de confidențialitate ale organizației și că gradul de respectare este revizuit periodic în mod obiectiv sau prin intermediul unor controale externe ale conformității, metode care pot include auditul și verificările aleatorii. În plus, organizația trebuie să instituie un mecanism eficient de recurs pentru a trata orice plângeri (a se vedea, de asemenea, în acest sens, considerentul 43) și să facă obiectul competențelor de investigare și de aplicare a legii ale Comisiei Federale pentru Comerț (FTC), ale Departamentului Transporturilor sau ale altui organism oficial al SUA care va asigura punerea în aplicare cu eficacitate a principiilor.

(27) Pentru așa-numitele „transferuri ulterioare”, și anume transferuri de date cu caracter personal de la o organizație către o parte terță care este operatorul sau persoana împuternicită de operator, indiferent dacă aceasta din urmă este situată în Statele Unite sau într-o țară terță față de Statele Unite (și de Uniunea Europeană) se aplică norme speciale. Scopul acestor norme este de a asigura faptul că protecția garantată pentru datele cu caracter personal referitoare ale persoanelor vizate din UE nu va fi compromisă și nu poate fi eludată prin transferarea acestor date către părți terțe. Acest lucru este relevant în special în lanțuri de prelucrare mai complexe, care sunt tipice pentru economia digitală din epoca noastră.

(28) În temeiul principiului transferul responsabilității pentru transferurile ulterioare ([28]), orice transfer ulterior nu poate avea loc decât (i) în scopuri limitate și specificate, (ii) pe baza unui contract (sau a unui acord asemănător în cadrul unui grup de întreprinderi ([29])) și (iii) numai în cazul în care contractul respectiv prevede același nivel de protecție precum cel garantat de principii, care include cerința ca aplicarea principiilor să nu poată fi restrânsă decât în măsura în care acest lucru este necesar pentru respectarea securității naționale, a aplicării legii și în alte scopuri de interes public ([30]). Acest principiu ar trebui interpretat ca fiind coroborat cu principiul *notificării* și, în cazul unui transfer ulterior către un terț operator ([31]), cu *principiul opțiunii*, potrivit căruia persoanele vizate trebuie să fie informate, printre altele, cu privire la tipul/identitatea oricărui terț beneficiar, la scopul transferului ulterior, precum și cu privire la posibilitățile de alegere oferite și se pot opune („opt out”) sau, în cazul datelor sensibile, trebuie să își dea „consimțământului explicit” („opt in”) în ceea ce privește transferurile ulterioare. Având în vedere *principiul integrității datelor și limitării scopului*, obligația de a oferi același nivel de protecție ca cel garantat de principii presupune că partea terță poate prelucra doar informațiile cu caracter personal transmise în scopuri care nu sunt incompatibile cu scopurile în care informațiile au fost colectate inițial sau cu scopurile aprobate ulterior de persoana în cauză.

(29) Obligația de a furniza același nivel de protecție ca cel impus de principii se aplică oricăreia și fiecăreia dintre părțile terțe implicate în prelucrarea datelor astfel transferate, indiferent de locul în care se află (în SUA sau într-o altă țară terță), precum și în cazul în care terțul beneficiar inițial transferă el însuși datele respective către un alt terț beneficiar, de exemplu în scopuri de subcontractare a serviciilor de prelucrare a datelor. În toate cazurile, contractul cu terțul beneficiar trebuie să prevadă că acesta din urmă va transmite o notificare organizației aderente la Scutul de confidențialitate în cazul în care ajunge la concluzia că nu mai poate îndeplini această

([25]) A se vedea, de asemenea, principiul suplimentar privind soluționarea litigiilor și punerea în aplicare a deciziilor (anexa II, punctul III.11).
([26]) A se vedea, de asemenea, principiul suplimentar privind „autocertificarea” (anexa II, punctul III.6).
([27]) A se vedea, de asemenea, principiul suplimentar privind „verificarea” (anexa II, punctul III.7).
([28]) A se vedea, de asemenea, principiul suplimentar privind „Contractele obligatorii pentru transferurile ulterioare” (anexa II, punctul III.10).
([29]) A se vedea principiul suplimentar privind „Contractele obligatorii pentru transferurile ulterioare” (anexa II, punctul III.10.b.). Deși acest principiu permite și efectuarea de transferuri bazate pe instrumente necontractuale (de exemplu, programe de conformitate și control din cadrul aceluiași grup de întreprinderi), textul clarifică faptul că aceste instrumente trebuie să asigure întotdeauna „continuitatea programelor de protecție a informațiilor cu caracter personal în temeiul principiilor”. În plus, dat fiind că organizația autocertificată din SUA va fi în continuare responsabilă pentru respectarea principiilor, ea va fi puternic încurajată să utilizeze instrumente care sunt într-adevăr eficace în practică.
([30]) A se vedea anexa II, punctul I.5.
([31]) Persoanele fizice nu vor dispune de dreptul de renunțare în cazul în care datele cu caracter personal sunt transmise către o parte terță care acționează ca agent pentru a îndeplini sarcini în numele și pe baza instrucțiunilor organizației din SUA. În acest scop, este totuși necesar să se încheie un contract cu agentul, iar organizația din Statele Unite ale Americii va fi răspunzătoare pentru garantarea măsurilor de protecție acordate în temeiul principiilor prin exercitarea competențelor sale de a da instrucțiuni.

obligație. În cazul în care se ajunge la o astfel de concluzie, prelucrarea de către terț va înceta sau trebuie luate alte măsuri rezonabile și adecvate pentru a remedia situația ([32]). În cazul în care apar probleme legate de conformitate de-a lungul lanțului de contractare (subcontractare) a serviciilor de prelucrare, organizația aderentă la Scutul de confidențialitate care acționează în calitate de operator de date cu caracter personal va trebui să dovedească că nu este responsabilă pentru fapta care a provocat prejudiciul sau, în caz contrar, va trebui să răspundă pentru consecințe, astfel cum se specifică în *principiul recursului, punerii în aplicare și responsabilității*. În cazul unui transfer ulterior către un agent terț se aplică măsuri de protecție suplimentare ([33]).

2.2. *Transparența, gestionarea și supravegherea Scutului de confidențialitate UE-SUA*

(30) Scutul de confidențialitate UE-SUA prevede mecanisme de supraveghere și de asigurare a aplicării legii, menite să verifice și să asigure faptul că societățile autocertificate din SUA respectă principiile și că orice încălcare este remediată. Aceste mecanisme sunt prezentate în cadrul principiilor (anexa II) și al angajamentelor asumate de Departamentul Comerțului (anexa I), FTC (anexa IV) și de Departamentul Transporturilor (anexa V).

(31) Pentru a asigura buna aplicare a Scutului de confidențialitate UE-SUA, părțile interesate, cum ar fi persoanele vizate, exportatorii de date și autoritățile naționale pentru protecția datelor (APD), trebuie să poată identifica organizațiile care aderă la principii. În acest scop, Departamentul Comerțului s-a angajat să mențină și să pună la dispoziția publicului o listă a organizațiilor care și-au autocerificat aderarea la principii și care intră sub jurisdicția a cel puțin uneia dintre autoritățile de aplicare a legii enumerate în anexele I și II la prezenta decizie („lista Scutului de confidențialitate") ([34]). Departamentul Comerțului va actualiza lista pe baza cererilor de recertificare depuse anual de organizații și ori de câte ori o organizație se retrage sau este eliminată din Scutul de confidențialitate UE-SUA. De asemenea, acesta va menține și va pune la dispoziția publicului un registru oficial al organizațiilor care au fost eliminate de pe listă, în fiecare caz identificând motivul aflat la baza unei astfel de măsuri. În cele din urmă, va furniza un link către lista menținută pe site-ul FTC care enumeră cazurile de asigurare a respectării programului deschise de FTC în legătură cu Scutul de confidențialitate.

(32) Departamentul Comerțului va pune la dispoziția publicului, pe un site internet special, atât lista Scutului de confidențialitate, cât și cererile de recertificare. La rândul său, organizațiile autocertificate trebuie să furnizeze adresa site-ului consacrat de departament listei Scutului de confidențialitate. În plus, în cazul în care este disponibilă online, politica de confidențialitate a unei organizații trebuie să includă un link către site-ul Scutului de confidențialitate, precum și un link către site-ul internet sau formularul de depunere a plângerii al instanței independente de recurs care poate ancheta plângerile nesoluționate. Departamentul Comerțului va verifica în mod sistematic, în contextul certificării și recertificării unei organizații la cadru, că politicile de confidențialitate ale acesteia respectă principiile.

(33) Organizațiile care au încălcat în mod persistent principiile vor fi eliminate de pe lista Scutului de confidențialitate și trebuie să returneze sau să șteargă datele cu caracter personal primite în temeiul Scutului de confidențialitate UE-SUA. În alte cazuri de eliminare, precum retragerea voluntară sau lipsa recertificării, organizația poate păstra datele în cazul în care declară anual Departamentului Comerțului angajamentul de a continua să aplice principiile sau oferă o protecție adecvată a datelor cu caracter personal prin alte mijloace autorizate (de exemplu, folosind un contract care reflectă pe deplin cerințele clauzelor contractuale standard aprobate de către Comisie). În acest caz, o organizație trebuie să identifice un punct de contact în cadrul organizației pentru toate întrebările legate de Scutul de confidențialitate.

(34) În plus, Departamentul Comerțului va monitoriza organizațiile care nu mai participă la Scutul de confidențialitate UE-SUA, fie pentru că s-au retras în mod voluntar, fie pentru că le-a expirat certificarea, pentru a verifica dacă acestea vor returna, șterge sau păstra ([35]) datele cu caracter personal primite anterior în temeiul cadrului. În cazul

([32]) Situația diferă în funcție de faptul că terțul este un operator sau o persoană împuternicită de către operator (agent). În prima ipoteză, contractul încheiat cu partea terță trebuie să prevadă că aceasta din urmă încetează prelucrarea sau ia alte măsuri rezonabile și adecvate pentru a remedia situația. În cea de a doua ipoteză, sarcina de a lua aceste măsuri revine organizației aderente la Scutul de confidențialitate, ea controlând prelucrarea și dând instrucțiunile pe baza cărora agentul își desfășoară activitatea.

([33]) În acest caz, organizația din SUA trebuie, de asemenea, să ia măsuri rezonabile și adecvate (i) pentru a se asigura că agentul prelucrează efectiv informațiile cu caracter personal transferate într-un mod compatibil cu obligațiile care îi revin organizației în temeiul principiilor și (ii) pentru a opri și a remedia prelucrarea neautorizată, în urma notificării.

([34]) În anexa I și anexa II (punctul I.3, punctul I.4, III.6.d și punctul III.11.g) se oferă informații privind gestionarea listei Scutului de confidențialitate.

([35]) A se vedea, de exemplu anexa II, punctul I.3, punctul III.6.f. și punctul III.11.g.i.

în care păstrează aceste date, organizațiile sunt obligate să continue să aplice principiile în privința datelor respective. În cazurile în care Departamentul Comerțului a eliminat organizații din cadru din cauza încălcării sistematice a principiilor privind protecția vieții private, acesta se va asigura că organizațiile respective sunt obligate să returneze sau să șteargă datele cu caracter personal primite în temeiul cadrului.

(35) Atunci când o organizație părăsește Scutul de confidențialitate UE-SUA din orice motiv, aceasta trebuie să elimine toate declarațiile publice care dau de înțeles că aceasta participă în continuare la Scutul de confidențialitate UE-SUA sau are dreptul la beneficiile acestuia, în special orice trimiteri la Scutul de confidențialitate UE-SUA publicate în politica sa de confidențialitate publicată. Departamentul Comerțului va căuta în mod activ și va soluționa declarațiile false privind participarea la cadru, inclusiv cele ale foștilor participanți ([36]). Orice declarație falsă adresată publicului general cu privire la aderarea unei organizații la principiile privind protecția vieții private sub forma unor afirmații sau practici înșelătoare poate fi sancționată de către FTC, Departamentul Transporturilor sau de alte autorități de aplicare a legii din SUA; declarațiile falsă adresate Departamentului Comerțului pot da naștere unei acțiuni intentate în temeiul Legii privind declarațiile false (18 U.S.C § 1001) ([37]).

(36) Departamentul Comerțului va monitoriza *ex officio* orice declarații false de participare la Scutul de confidențialitate sau utilizarea necorespunzătoare a mărcii de certificare Scutul de confidențialitate, iar autoritățile pentru protecția datelor pot trimite organizațiile pentru control la un punct de contact special din cadrul departamentului. În cazul în care o organizație s-a retras din programul privind Scutul de confidențialitate UE-SUA, nu se recertifică sau este eliminată de pe lista Scutului de confidențialitate, Departamentul Comerțului va verifica în permanență dacă aceasta a eliminat din politica de confidențialitate publicată orice trimiteri la Scutul de confidențialitate care dau de înțeles că aceasta continuă să participe și, în cazul în care organizația continuă să prezinte declarații false, acesta sesizează FTC, Departamentul Transporturilor sau o altă autoritate competentă pentru posibile măsuri de asigurare a respectării. De asemenea, Departamentul Comerțului va trimite chestionare organizațiilor ale căror autocertificări expiră sau care s-au retras în mod voluntar din Scutul de confidențialitate UE-SUA pentru a verifica dacă organizația va returna, va șterge sau va continua să aplice principiile privind protecția vieții private la datele cu caracter personal pe care le-a primit în perioada în care a participat la Scutul de confidențialitate UE-SUA și, în cazul în care datele cu caracter personal sunt păstrate, acesta verifică identitatea persoanei din cadrul organizației care va servi drept punct de contact permanent pentru întrebări legate de Scutul de confidențialitate.

(37) În mod regulat, Departamentul Comerțului va efectua evaluări *ex officio* ale conformității ([38]) organizațiilor autocertificate, inclusiv prin trimiterea de chestionare detaliate. De asemenea, acesta va efectua în mod sistematic analize în cazul în care a primit o plângere (serioasă) specifică, în cazul în care o organizație nu furnizează răspunsuri satisfăcătoare la întrebările sale sau atunci când există dovezi credibile care sugerează că este posibil ca o organizație să nu respecte principiile. După caz, Departamentul Comerțului se va consulta și cu autoritățile pentru protecția datelor cu privire la astfel de controale de conformitate.

2.3. *Mecanismele de recurs, de tratare a plângerilor și de asigurare a respectării legii*

(38) Scutul de confidențialitate UE-SUA, prin *principiul recursului, punerii în aplicare și responsabilității*, impune organizațiilor să ofere posibilitatea de recurs persoanelor care au fost afectate de nerespectarea principiilor și, prin urmare, posibilitatea ca persoanele vizate din UE să depună plângeri privind nerespectarea principiilor de către companiile americane autocertificate și ca aceste plângeri să fie soluționate, dacă este cazul, printr-o decizie care prevede o acțiune corectivă eficace.

(39) Ca parte a autocertificării, organizațiile trebuie să îndeplinească cerințele principiul recursului, punerii în aplicare și responsabilității, punând la dispoziție mecanisme independente de recurs, eficace și ușor accesibile, care să permită investigarea și soluționarea în mod rapid și gratuit a oricăror plângeri și litigii ale persoanelor fizice.

(40) Organizațiile pot opta pentru mecanisme independente de recurs fie în Uniune, fie în Statele Unite. Acest lucru include posibilitatea de a își asuma în mod voluntar angajamentul de a coopera cu autoritățile pentru protecția

([36]) A se vedea anexa I, punctul referitor la „Identificarea și abordarea afirmațiilor false de participare".
([37]) A se vedea anexa II, punctul III.6.h. și punctul III.11.f.
([38]) A se vedea anexa I.

datelor din UE. Cu toate acestea, nu există o astfel de opțiune în cazul în care organizațiile prelucrează date privind resursele umane, cooperarea cu DPA fiind obligatorie. Alte opțiuni includ sistemul independent de soluționare alternativă a litigiilor (SAL) sau *programe privind protecția vieții private* elaborate de sectorul privat care integrează principiile privind confidențialitatea în regulile lor. Acestea din urmă trebuie să includă mecanisme eficiente de asigurare a respectării principiilor, în conformitate cu cerințele principiului recursului, punerii în aplicare și responsabilității. Organizațiile sunt obligate să remedieze orice probleme de neconformitate. Ele trebuie să precizeze, de asemenea, că fac obiectul competențelor de investigare și de asigurare a executării ale FTC, ale Departamentului Transporturilor sau ale oricărui alt organism de reglementare autorizat din Statele Unite ale Americii.

(41) Prin urmare, cadrul Scutului de confidențialitate oferă persoanelor vizate o serie de posibilități de a-și exercita drepturile, de a depune plângeri privind nerespectarea de către societățile autocertificate din SUA și de a beneficia de soluționarea plângerilor lor, dacă este necesar printr-o decizie care prevede o acțiune corectivă eficace. Persoanele fizice pot depune plângeri adresate direct unei organizații, la un organism independent de soluționare a litigiilor desemnat de către organizație, la APD naționale sau la FTC.

(42) În cazul în care reclamațiile lor nu au putut fi soluționate de către oricare dintre aceste mecanisme de recurs sau de asigurare a respectării principiilor, persoanele au, de asemenea, dreptul de a recurge la procedura de arbitraj obligatoriu efectuată de „comitetul pentru Scutul de confidențialitate” (anexa 1 la anexa II la prezenta decizie). Cu excepția comitetului de arbitraj, care solicită ca anumite căi de atac să fie epuizate înainte de a putea fi sesizat, persoanele sunt libere să aleagă oricare sau fiecare mecanism de recurs și nu sunt obligate să opteze pentru un anumit mecanism în locul altuia sau să urmeze o anumită secvență. Cu toate acestea, există o anumită ordine logică și este recomandabil să fie urmată, conform celor prezentate mai jos.

(43) În primul rând, cetățenii UE pot să urmărească cazurile de nerespectare a principiilor prin contacte directe cu *compania americană autocertificată*. Pentru a facilita soluționarea, organizația trebuie să instituie un mecanism eficient de recurs pentru a trata astfel de plângeri. Astfel, politica de confidențialitate a unei organizații trebuie să informeze în mod clar persoanele în legătură cu existența unui punct de contact, fie în cadrul, fie în afara organizației, care va gestiona plângerile (inclusiv orice sediu din Uniune care poate răspunde la solicitările de informații sau plângeri) și cu privire la mecanismele independente pentru soluționarea plângerilor.

(44) La primirea unei plângeri individuale, direct de la persoana respectivă sau prin intermediul Departamentului Comerțului în urma sesizării acestuia de către o autoritate pentru protecția datelor, organizația trebuie să furnizeze un răspuns persoanei vizate din UE în termen de 45 de zile. Răspunsul trebuie să includă o evaluare a temeiniciei plângerii și informații cu privire la modul în care organizația va remedia problema. În mod similar, organizațiile trebuie să răspundă prompt la solicitările de informații și alte cereri de informații din partea Departamentului Comerțului sau a unei APD ([39]) (în cazul în care organizația și-a luat angajamentul de a coopera cu APD) legate de aderarea la principii. Organizațiile trebuie să păstreze evidențe cu privire la punerea în aplicare a politicilor lor în materie de confidențialitate și să le pună la dispoziție, la cerere, mecanismului independent de recurs sau FTC (ori altor autorități americane cu competența de a ancheta practicile neloiale și frauduloase) în cadrul unei anchete sau al unei plângeri pentru neconformitate.

(45) În al doilea rând, persoanele pot depune plângeri direct la *organismul independent de soluționare a litigiilor* (fie în Statele Unite, fie în Uniune) desemnat de organizație să ancheteze și să soluționeze plângeri individuale (cu excepția cazului în care acestea sunt în mod evident nefondate sau abuzive) și să asigure persoanei vizate căi de atac corespunzătoare cu titlu gratuit. Sancțiunile și căile de atac impuse de un astfel de organism trebuie să fie suficient de severe pentru a garanta respectarea principiilor și ar trebui să prevadă o inversare sau o corectare de către organizație a efectelor nerespectării și, în funcție de circumstanțe, încheierea prelucrării ulterioare a datelor cu caracter personal în cauză și/sau ștergerea acestora, precum și publicarea nerespectărilor constatate. Organismele independente de soluționare a litigiilor desemnate de o organizație trebuie să includă pe site-urile lor publice informații relevante cu privire la Scutul de confidențialitate UE-SUA și serviciile pe care le furnizează în temeiul acestuia. În fiecare an, statele membre trebuie să publice un raport anual cu statistici agregate cu privire la aceste servicii ([40]).

([39]) Aceasta este autoritatea de gestionare desemnată de comitetul APD prevăzut în principiul suplimentar privind „Rolul autorităților pentru protecția datelor”) (anexa II, punctul III.5).

([40]) Raportul anual trebuie să conțină: (1) numărul total de plângeri legate de Scutul de confidențialitate primite în cursul anului de raportare; (2) tipurile de plângeri primite de soluționare a litigiilor; (3) măsurile de asigurare a calității, cum ar fi perioada de timp pentru prelucrarea reclamațiilor; și (4) rezultatele plângerilor primite, în special numărul și tipul de măsuri corective sau sancțiuni impuse.

(46) În cadrul procedurilor sale de control al conformității, Departamentul Comerțului va verifica dacă întreprinderile americane autocertificate și-au înregistrat efectiv participarea la mecanismele independente de recurs la care susțin că sunt înregistrate. Atât organizațiile, cât și mecanismele independente de recurs competente trebuie să răspundă prompt la întrebările și cererile de informații din partea Departamentului Comerțului referitoare la Scutul de confidențialitate.

(47) În cazurile în care organizația nu a respectat hotărârea pronunțată de organismul de soluționare a litigiilor și de autoreglementare, acesta din urmă trebuie să notifice neconformitatea către Departamentul Comerțului și FTC (sau alte autorități din SUA cu competențe să investigheze practicile neloiale și frauduloase) sau unei instanțe competente ([41]). În cazul în care o organizație refuză să se conformeze unei decizii definitive luate de un organism de autoreglementare în vederea protejării vieții private, de o instanță independentă de soluționare a litigiilor sau de un organism guvernamental ori în care un astfel de organism constată că aceasta încalcă frecvent principiile, se va considera că este vorba de o nerespectare sistematică, care va avea drept consecință radierea de pe listă a organizației de către Departamentul Comerțului, însă numai după ce a acordat organizației în cauză un preaviz de 30 de zile și posibilitatea de a răspunde ([42]). În cazul în care, după radierea de pe listă, organizația continuă să pretindă certificarea Scutului de confidențialitate, Departamentul va sesiza FTC sau o altă agenție de aplicare a legii ([43]).

(48) În al treilea rând, persoanele fizice pot depune, de asemenea, plângeri la o *autoritate de protecție a datelor* la nivel național. Organizațiile sunt obligate să coopereze în cadrul anchetei și al soluționării plângerii de către o autoritate pentru protecția datelor fie în cazul în care plângerea se referă la prelucrarea datelor referitoare la resurse umane colectate în cadrul unui raport de muncă, fie în cazul în care organizația respectivă s-a oferit în mod voluntar să fie supravegheată de către APD. În special, organizațiile trebuie să răspundă la solicitările de informații, să se conformeze avizului emis de autoritatea pentru protecția datelor, inclusiv măsurile reparatorii sau compensatorii, și să trimită autorității pentru protecția datelor confirmarea scrisă că au fost întreprinse astfel de acțiuni.

(49) Avizul autorităților pentru protecția datelor va fi transmis prin intermediul unui comitet neoficial al APD înființat la nivelul Uniunii ([44]), ceea ce va contribui la asigurarea unei abordări armonizate și coerente a unei plângeri date. Avizul va fi emis după ce ambele părți implicate în litigiu au avut posibilitatea de a-și prezenta observațiile și de a aduce toate dovezile pe care doresc să le prezinte. Comitetul își va transmite avizul cât mai repede posibil, respectând totodată principiile procesului echitabil și, ca regulă generală, în termen de 60 de zile după primirea unei plângeri. În cazul în care o organizație nu se conformează în termen de 25 de zile de la furnizarea avizului și nu oferă o explicație satisfăcătoare pentru întârziere, comitetul ar putea decide să înainteze chestiunea către FTC (sau o altă autoritate de executare competentă din SUA) sau să constate că angajamentul de cooperare a fost grav încălcat. În primul caz, acest lucru poate conduce la măsuri de punere în aplicare în temeiul articolului 5 din Legea FTC (sau o lege similară). În al doilea caz, comitetul informează Departamentul Comerțului, care va considera că refuzul organizației de a da curs avizului Comitetului APD constituie o nerespectare sistematică, ceea ce va conduce la eliminarea organizației de pe lista Scutului de confidențialitate.

(50) În cazul în care autoritatea pentru protecția datelor căreia i-a fost adresată plângerea nu a luat măsuri sau a luat măsuri insuficiente pentru a soluționa o plângere, reclamantul are posibilitatea de a contesta o astfel de (lipsă de) acțiune în fața instanțelor naționale din statul membru respectiv.

(51) De asemenea, persoanele pot depune plângeri la APD chiar și în cazul în care Comitetul APD nu a fost desemnat ca organism de soluționare a litigiilor de către organizație. În aceste cazuri, APD poate înainta aceste plângeri fie către Departamentul Comerțului, fie către FTC. Pentru a facilita și a consolida cooperarea în chestiuni legate de plângeri individuale și de nerespectarea principiilor de către organizațiile aderente la Scutul de confidențialitate, Departamentul Comerțului va stabili un punct de contact special care să acționeze ca un punct de legătură și să asiste anchetele APD cu privire la conformitatea organizației cu principiile ([45]). De asemenea, FTC s-a angajat să ofere un punct de contact special ([46]) și să acorde APD asistență de investigare în conformitate cu Legea SUA „SAFE WEB") ([47]).

([41]) A se vedea anexa II, punctul III.11.e.
([42]) A se vedea anexa II, punctul III.11.g, în special subpunctele (ii) and (iii).
([43]) A se vedea anexa I, punctul referitor la „Identificarea și abordarea afirmațiilor false de participare".
([44]) Regulamentul de procedură al comitetului informal al APD ar trebui să fie stabilit de autoritățile pentru protecția datelor pe baza competenței lor de a-și organiza activitatea lor și de a coopera între ele.
([45]) A se vedea anexa I secțiunile privind „Intensificarea cooperării cu autoritățile pentru protecția datelor" și „Facilitarea soluționării plângerilor referitoare la nerespectarea principiilor" și anexa II, punctul II.7.e.
([46]) A se vedea anexa IV, p. 6.
([47]) *ibid*.

(52) În al patrulea rând, Departamentul Comerțului s-a angajat să primească, să examineze și să depună toate eforturile pentru soluționarea plângerilor legate de nerespectarea principiilor de către o organizație. În acest scop, Departamentul Comerțului prevede proceduri speciale pentru transmiterea plângerilor către un punct de contact, urmărirea acestora și contactarea companiilor pentru a facilita soluționarea. Pentru a accelera prelucrarea plângerilor individuale, punctul de contact va lua legătura direct cu DPA pe marginea aspectelor legate de conformitate, în special, cu privire la statutul plângerilor în termen de cel mult 90 zile de la sesizare. Acest lucru permite persoanelor vizate să depună plângeri de nerespectare de către companiile autocertificate direct la autoritatea lor națională pentru protecția datelor, iar acestea vor fi direcționate către Departamentul Comerțului al SUA, în calitate de autoritate care gestionează Scutul de confidențialitate UE-SUA. De asemenea, Departamentul Comerțului s-a angajat să furnizeze, în cadrul evaluării anuale a funcționării Scutului de confidențialitate, un raport care analizează sub formă agregată plângerile pe care le primește în fiecare an ([48]).

(53) În cazul în care, în baza verificărilor ex officio, a plângerilor sau a oricăror altor informații, Departamentul Comerțului concluzionează că o organizație a încălcat în mod sistematic principiile privind protecția vieții private, acesta va elimina organizația respectivă de pe lista Scutului de confidențialitate. Refuzul de a se supune unei decizii finale a oricărui organism de autoreglementare în materie de protecție a vieții private, organism independent de soluționare a litigiilor sau organism public, inclusiv o autoritate pentru protecția datelor, va fi considerat ca fiind o încălcare sistematică.

(54) În al cincilea rând, organizațiile aderente la Scutul de confidențialitate trebuie să facă obiectul competențelor de investigare și de asigurare a respectării ale autorităților americane, în special ale *Comisiei Federale pentru Comerț* ([49]), care va asigura punerea în aplicare cu eficacitate a principiilor. FTC va acorda prioritate cazurilor de nerespectare a principiilor privind protecția vieții private primite de la organisme independente de soluționare a litigiilor sau de la organisme de autoreglementare, Departamentul Comerțului și autoritățile pentru protecția datelor (care acționează din proprie inițiativă sau în urma unei plângeri) pentru a stabili dacă s-a încălcat secțiunea 5 din Legea Comisiei Federale pentru Comerț (*Federal Trade Commission Act*) ([50]). FTC s-a angajat să creeze un proces de sesizare standardizat, să desemneze un punct de contact în cadrul agenției pentru sesizările APD și să facă schimb de informații cu privire la sesizări. În plus, FTC va accepta plângeri direct de la persoane fizice și va iniția din proprie inițiativă anchete privind Scutul de confidențialitate, în special în cadrul anchetelor sale mai ample privind aspectele legate de viața privată.

(55) FTC poate asigura conformitatea prin ordine administrative („ordonanțe prin consimțământ") și va monitoriza în mod sistematic respectarea acestor ordine. În cazul în care organizațiile nu se conformează, FTC poate sesiza instanța competentă în vederea unei eventuale sancțiuni civile și a altor căi de atac, inclusiv pentru orice prejudiciu cauzat de comportamentul ilicit. De asemenea, FTC poate solicita direct un ordin judecătoresc preliminar sau permanent sau alte măsuri corective din partea unui tribunal federal. Fiecare ordonanță prin consimțământ adresată unei organizații care aderă la Scutul de confidențialitate va include dispoziții de autoraportare ([51]) și organizațiile vor trebui să facă publice toate secțiunile relevante cu privire la Scutul de confidențialitate din orice raport de conformitate sau de evaluare transmis către FTC. În cele din urmă, FTC va menține o listă online a companiilor care fac obiectul ordinelor judecătorești sau ale FTC în cazuri privind Scutul de confidențialitate.

(56) În al șaselea rând, ca mecanism de recurs „de ultimă instanță", în cazul în care niciuna dintre celelalte căi de atac disponibile nu a soluționat în mod satisfăcător o plângere, persoana vizată din UE poate recurge la procedura de arbitraj obligatoriu efectuată de *„comitetul pentru Scutul de confidențialitate*". Organizațiile trebuie să informeze persoanele fizice cu privire la posibilitatea, în anumite condiții, de a invoca un arbitraj obligatoriu, fiind obligate să răspundă atunci când o persoană a apelat la această opțiune transmițând o notificare organizației în cauză ([52]).

([48]) A se vedea anexa I, punctul referitor la „Facilitarea soluționării plângerilor referitoare la nerespectarea principiilor".

([49]) Organizațiile aderente la Scutul de confidențialitate trebuie să își declare în mod public angajamentul de a respecta principiile, să își facă publice politicile de confidențialitate în conformitate cu aceste principii și să le pună pe deplin în aplicare. Nerespectarea principiilor este executorie în temeiul secțiunii 5 din Legea privind Comisia Federală pentru Comerț, care interzice practicile neloiale sau frauduloase în domeniul comerțului sau care afectează comerțul.

([50]) Potrivit informațiilor furnizate de FTC, aceasta nu are competența de a realiza inspecții la fața locului în materie de protecție a vieții private. Cu toate acestea, FTC are puterea de a obliga organizațiile să prezinte înscrisuri și să furnizeze declarații ale martorilor (a se vedea secțiunea 20 din Legea privind Comisia Federală pentru Comerț) și poate apela la sistemul judiciar pentru a executa aceste ordine în caz de nerespectare.

([51]) FTC sau hotărârile judecătorești pot solicita companiilor să pună în aplicare programe cu privire la protecția vieții private și să prezinte periodic rapoarte de conformitate sau evaluări independente externe ale programelor puse la dispoziția FTC.

([52]) A se vedea anexa II, punctul II.1.xi și III.7.c.

(57) Acest comitet de arbitraj va consta într-un grup de cel puțin 20 de arbitri desemnați de către Departamentul Comerțului și Comisia Europeană selectați pe criterii de independență, integritate și expertiză în ceea ce privește legislația SUA privind confidențialitatea și legislația Uniunii privind protecția datelor. Pentru fiecare caz, părțile vor selecta din această rezervă un juriu format din unul sau trei ([53]) arbitri. Acțiunea va fi reglementată de regulile standard de arbitraj care urmează a fi convenite între Departamentul Comerțului și Comisie. Aceste norme vor completa cadrul deja convenit, care conține mai multe caracteristici care vor spori posibilitățile de acces al persoanelor vizate din UE la acest mecanism: (i) persoana vizată poate fi asistată de APD națională din țara sa atunci când se pregătește să aducă o plângere în atenția comitetului; (ii) deși arbitrajul va avea loc în Statele Unite, persoanele vizate din UE pot alege să participe prin teleconferință sau videoconferință, servicii care trebuie furnizate cu titlu gratuit persoanei în cauză; (iii) deși limba folosită în cadrul arbitrajului va fi limba engleză, în urma unei cereri motivate, serviciile de interpretare și de traducere în cadrul ședinței de arbitraj vor fi furnizate, de regulă ([54]), cu titlu gratuit persoanei vizate; (iv) în fine, deși fiecare parte trebuie să suporte onorariul propriului avocat, în cazul în care este reprezentată de un avocat în fața comitetului, Departamentul Comerțului va institui un fond alimentat din contribuții anuale de organizațiile participante la Scutul de confidențialitate, care acoperă costurile eligibile ale procedurii de arbitraj, până la o anumită valoare maximă, care urmează să fie stabilită de către autoritățile americane în consultare cu Comisia.

(58) Comitetul pentru Scutul de confidențialitate va avea competența de a impune „măsuri nemonetare, echitabile, personalizate" ([55]) necesare pentru remedierea cazurilor de nerespectare a principiilor. Deși comitetul va lua în considerare alte măsuri deja obținute prin alte mecanisme ale Scutului de confidențialitate la formularea soluției sale, persoanele pot să recurgă la arbitraj dacă acestea consideră că respectivele căi de atac alternative sunt insuficiente. Acest lucru le va permite persoanelor vizate să recurgă la procedura de arbitraj în toate cazurile în care acțiunea sau lipsa de acțiune a autorităților americane competente (de exemplu, FTC) nu le-a soluționat în mod satisfăcător reclamațiile. Procedura de arbitraj nu poate fi invocată în cazul în care o autoritate pentru protecția datelor are autoritatea legală de a soluționa chestiunea în cauză cu privire la compania americană autocertificată, și anume în cazurile în care organizația fie este obligată să coopereze și să se conformeze avizului emis de DPA în ceea ce privește prelucrarea datelor privind resursele umane colectate în contextul ocupării unui loc de muncă, fie s-a angajat voluntar să facă acest lucru.

(59) În al șaptelea rând, în cazul în care o organizație nu își îndeplinește angajamentul de a respecta principiile privind protecția vieții private și politica de confidențialitate publicată, pot fi disponibile alte căi de atac judiciare în temeiul legislației SUA care prevede căi de atac în temeiul legii privind delictele civile și în cazurile de falsificare frauduloasă, acte sau practici neloiale sau frauduloase sau încălcarea contractului.

(60) În plus, dacă o APD, la primirea unei reclamații depuse de o persoană vizată din UE, consideră că transferul de date cu caracter personal ale unei persoane către o organizație din Statele Unite este efectuat prin încălcarea legislației UE în domeniul protecției datelor, inclusiv atunci când exportatorul de date din UE are motive să creadă că organizația nu respectă principiile, aceasta poate, de asemenea, să își exercite competențele față de exportatorul de date și, dacă este necesar, să dispună suspendarea transferului de date.

(61) Având în vedere informațiile din această secțiune, Comisia consideră că principiile emise de Departamentul Comerțului al SUA asigură, ca atare, un nivel de protecție a datelor cu caracter personal care este, în esență, echivalent cu cel garantat de principiile de bază stabilite în Directiva 95/46/CE.

(62) În plus, aplicarea efectivă a principiilor este garantată de obligațiile privind transparența și de gestionarea Scutului de confidențialitate și controlul conformității cu acesta de către Departamentul Comerțului.

(63) De asemenea, Comisia consideră că, luate în ansamblu, mecanismele de supraveghere, de recurs și de asigurare a respectării principiilor prevăzute de Scutul de confidențialitate permit identificarea și pedepsirea în practică a încălcărilor principiilor de către organizațiile care aderă la Scutul de confidențialitate și oferă căi de atac persoanei vizate pentru a avea acces la datele cu caracter personal care o privesc și, în cele din urmă, pentru a obține rectificarea sau ștergerea datelor respective.

([53]) Numărul de arbitri din comitet va trebui convenit de părți.

([54]) Cu toate acestea, Comitetul poate considera că, în împrejurările unei anumite proceduri de arbitraj, acoperirea ar duce la costuri nejustificate sau disproporționate.

([55]) Persoanele fizice nu pot solicita despăgubiri în cadrul procedurii de arbitraj, dar, în schimb, invocarea procedurii de arbitraj nu exclude posibilitatea de a solicita despăgubiri în instanțele obișnuite americane.

3. ACCESUL ȘI UTILIZAREA DATELOR CU CARACTER PERSONAL TRANSFERATE ÎN TEMEIUL SCUTULUI DE CONFIDENȚIALITATE UE-SUA DE CĂTRE AUTORITĂȚILE PUBLICE AMERICANE

(64) Astfel cum rezultă din anexa II, secțiunea I.5, aderarea la principii private este limitată la ceea ce este necesar pentru respectarea securității naționale, a interesului public sau a cerințelor de aplicare a legii.

(65) Comisia a evaluat limitările și garanțiile disponibile în legislația SUA în ceea ce privește accesul și utilizarea datelor cu caracter personal transferate în temeiul Scutului de confidențialitate UE-SUA către autoritățile publice americane pentru scopuri de securitate națională, aplicarea legii și alte scopuri de interes public. În plus, guvernul SUA, prin intermediul cabinetului directorului Serviciului național de informații (ODNI) ([56]), a oferit Comisiei asigurări cu declarații și angajamente detaliate, care figurează în anexa VI la prezenta decizie. Prin scrisoarea semnată de secretarul de stat prevăzută în anexa III la prezenta decizie, guvernul SUA s-a angajat, de asemenea, să instituie un nou mecanism de supraveghere pentru imixtiunea în scopul securității naționale, și anume Ombudsmanul pentru Scutul de confidențialitate, care este independent de serviciile de informații. În sfârșit, o declarație a Departamentului de Justiție al SUA, care figurează în anexa VII la prezenta decizie, descrie limitările și garanțiile aplicabile în ceea ce privește accesul și utilizarea datelor de către autoritățile publice în scopul aplicării legii sau în alte scopuri de interes public. Pentru a spori transparența și pentru a reflecta natura juridică a acestor angajamente, fiecare dintre documentele enumerate și anexate la prezenta decizie vor fi publicate în Registrul federal al SUA.

(66) În continuare sunt detaliate constatările Comisiei privind limitările privind accesul și utilizarea datelor cu caracter personal transferate din Uniunea Europeană către Statele Unite ale Americii de către autorități publice americane și existența unei protecții juridice efective.

3.1. *Accesul și utilizarea de către autoritățile publice americane în scopuri de securitate națională*

(67) Analiza Comisiei arată că legislația SUA conține o serie de limitări clare cu privire la accesul și utilizarea datelor cu caracter personal transferate în temeiul Scutului de confidențialitate UE-SUA în scopuri de securitate națională, precum și mecanisme de supraveghere și de recurs care oferă garanții suficiente pentru ca aceste date să fie protejate eficient împotriva intervențiilor ilicite și a riscului de abuz ([57]). Din 2013, când Comisia a publicat două comunicări (a se vedea considerentul 7), acest cadru juridic a fost consolidat în mod semnificativ, potrivit descrierii de mai jos.

3.1.1. Limitări.

(68) În conformitate cu Constituția Statelor Unite ale Americii, asigurarea securității naționale intră sub autoritatea Președinției în calitate de comandant-șef, de șef al executivului și, în ceea ce privește serviciile de informații externe, de a conduce activitatea de afaceri externe a SUA ([58]). Deși Congresul are competența de a impune limitări, iar acest lucru s-a întâmplat în mai multe privințe, în cadrul limitelor respective, președintele poate coordona activitățile comunității serviciilor de informații americane, în special prin decrete sau directive prezidențiale. Aceasta se aplică, de asemenea, în domeniile în care nu există orientări ale Congresului. În prezent, cele două instrumente juridice esențiale în acest sens sunt Ordinul executiv nr. 12333 („O.E. 12333") ([59]) și Directiva nr. 28 privind politica prezidențială.

([56]) Directorul Serviciului național de informații (DNI) exercită rolul de șef al comunității serviciilor de informații și acționează în calitate de consilier principal al președintelui și al Consiliului de securitate națională. A se vedea Legea privind reforma serviciilor de informații si prevenirea terorismului din 2004, Pub. L. 108-458 din 17 decembrie 2004. Printre altele, ODNI stabilește cerințele pentru serviciile de informații și gestionează și stabilește sarcinile, colectarea, analiza, elaborarea și difuzarea de informații naționale de către serviciile de informații, inclusiv prin elaborarea de orientări pentru modul în care informațiile sau datele operative sunt accesate, utilizate și partajate. A se vedea secțiunea 1.3 (a), (b) din O.E. 12333.

([57]) A se vedea Schrems, punctul 91.

([58]) Constituția SUA, articolul II. A se vedea, de asemenea, introducerea la PPD-28.

([59]) E.O. 12333: Activitățile de spionaj ale Statelor Unite, Registrul Federal Vol. 40. nr. 235 (8 decembrie 1981). În măsura în care decretul prezidențial este accesibil publicului, acesta definește obiectivele, instrucțiunile și responsabilitățile serviciilor de informații americane (inclusiv rolul diverselor elemente ale comunității serviciilor de informații) și stabilește parametrii generali pentru desfășurarea activităților de spionaj (în special necesitatea de a adopta norme procedurale specifice). În conformitate cu secțiunea 3.2 din O.E. 12333, Președintele, susținut de Consiliul de securitate națională, și DNI emit astfel de directive, proceduri și orientări adecvate după cum sunt necesare pentru a pune în aplicare decretul.

(69) Directiva nr. 28 privind politica prezidențială („PPD-28"), publicată la 17 ianuarie 2014, prevede o serie de limitări pentru operațiunile de „colectare de informații pe baza semnalelor electromagnetice" ([60]). Directiva prezidențială are forță obligatorie pentru autoritățile americane de informații ([61]) și efectul util al acesteia rămâne valabil în cazul schimbării administrației americane ([62]). PPD-28 este deosebit de importantă pentru persoanele din afara SUA, inclusiv persoanele vizate din UE. Printre altele, aceasta prevede că:

(a) colectarea de informații pe baza semnalelor electromagnetice trebuie să se efectueze în temeiul legii sau al autorizației prezidențiale și trebuie realizată în conformitate cu Constituția Statelor Unite ale Americii (în special cel de al patrulea amendament) și cu legislația SUA;

(b) toate persoanele ar trebui să fie tratate cu demnitate și respect, indiferent de naționalitatea sau locul lor de reședință;

(c) toate persoanele au interese legitime în manipularea informațiilor cu caracter personal ale acestora;

(d) viața privată și libertățile civile sunt parte integrantă din planificarea activităților de colectare de informații pe baza semnalelor electromagnetice din SUA;

(e) activitățile de colectare de informații pe baza semnalelor electromagnetice din SUA trebuie, prin urmare, să includă garanții adecvate pentru informațiile cu caracter personal ale tuturor persoanelor fizice, indiferent de naționalitatea sau locul lor de reședință.

(70) PPD-28 stipulează că informațiile pe baza semnalelor electromagnetice pot fi colectate numai în cazul în care există un scop legat de servicii străine de informații sau contrainformații pentru a sprijini misiunile departamentale și naționale și nu în alt scop (de exemplu, pentru a oferi un avantaj concurențial companiilor americane). În această privință, ODNI oferă explicația potrivit căreia elementele comunității serviciilor de informații „ar trebui să prevadă că, ori de câte ori este posibil, colectarea ar trebui să se concentreze pe ținte sau subiecte specifice de informații externe prin utilizarea unor elemente de discriminare (de exemplu, infrastructuri specifice, termenii de selecție și identificatori)" ([63]). În plus, declarațiile oferă asigurarea că deciziile legate de culegerea informațiilor secrete nu sunt lăsate la discreția agenților de informații individuali, ci fac obiectul diferitelor politici și proceduri pe care elementele comunității serviciilor de informații americane (agenții) trebuie să le instituie pentru a pune în aplicare PPD28 ([64]). În consecință, cercetarea și stabilirea selectoarelor adecvate are loc în baza „Cadrului național de priorități ale serviciilor de informații" (*National Intelligence Priorities Framework* – NIPF) care asigură faptul că prioritățile serviciilor de informații sunt stabilite de factorii de decizie politică de la nivel înalt și sunt revizuite în mod regulat pentru a menține o capacitate de reacție la amenințările la adresa securității naționale și iau în considerare eventualele riscuri, inclusiv riscurile la adresa vieții private ([65]). Pe această bază, personalul agenției cercetează și identifică termeni specifici de selecție pentru a colecta informații externe care să răspundă priorităților ([66]). Termenii de selecție sau „selectoarele" trebuie revizuite periodic pentru a se stabili dacă acestea continuă să furnizeze informații valoroase în conformitate cu prioritățile ([67]).

([60]) În conformitate cu O.E. 12333, directorul Agenției Naționale de Securitate (NSA) este administratorul funcțional pentru obținerea informațiilor pe baza semnalelor electromagnetice și operează o organizație unificată pentru activitățile de colectare de informații pe baza semnalelor electromagnetice.

([61]) Pentru definirea termenului „comunitatea serviciilor de informații", a se vedea secțiunea 3.5(h) din O.E. 12333 cu nr. 1 din PPD-28.

([62]) A se vedea memorandumul Biroului de asistență juridică, Departamentul Justiției (DOJ), adresat Președintelui Clinton, 29 ianuarie 2000. Conform acestui aviz juridic, directivele prezidențiale au „același efect juridic pe fond ca un ordin executiv".

([63]) Declarațiile ODNI (anexa VI), p. 3.

([64]) A se vedea secțiunea 4(b),(c) din PPD-28. Potrivit informațiilor publice, revizuirea din 2015 a confirmat cele șase obiective existente. A se vedea ODNI, Reforma legată de activitățile de colectare de informații pe baza semnalelor electromagnetice, raportul intermediar de activitate pentru anul 2016.

([65]) Observațiile ODNI (anexa VI), p. 6 (cu trimiteri la Directiva nr. 204 privind comunitatea serviciilor de informații – *Intelligence Community Directive 204*). A se vedea, de asemenea, secțiunea 3 din PPD-28.

([66]) Declarațiile ODNI (anexa VI), p. 6. A se vedea, de exemplu, Biroul pentru libertăți civile și viață privată al NSA (NSA CLPO), Măsurile de protecție a libertăților civile și vieții private ale NSA pentru activitățile cu țintă precisă de colectare de informații SIGINT în temeiul Decretului 12333, 7 octombrie 2014. A se vedea, de asemenea, Raportul de situație al ODNI pentru anul 2014. Pentru cererile de acces în temeiul secțiunii 702 din FISA, întrebările sunt reglementate de proceduri de reducere la minimum aprobate de FISC. A se vedea NSA CLPO, Punerea în aplicare de către NSA a secțiunii 702 din Legea privind supravegherea activităților străine de spionaj (Foreign Intelligence Surveillance Act), 16 aprilie 2014.

([67]) A se vedea Reforma legată de activitățile de colectare de informații pe baza semnalelor electromagnetice, raportul aniversar pentru anul 2015. A se vedea, de asemenea, Declarațiile ODNI (anexa VI), paginile 6, 89, 11.

(71) În plus, cerințele stipulate de PPD-28 potrivit cărora colectarea de informații trebuie să fie întotdeauna ([68])„cât mai adaptată posibil", iar serviciile de informații trebuie să acorde prioritate disponibilității altor informații și alternativelor adecvate și fezabile ([69]) exprimă o regulă generală de prioritizare a colectării cu țintă precisă în defavoarea colectării în masă. În conformitate cu asigurarea oferită de ODNI, cerințele asigură în special faptul că colectarea în vrac a datelor nu este efectuată nici „în masă", nici „în mod nediferențiat" și că excepția nu asimilează regula ([70]).

(72) Deși PPD-28 explică faptul că elementele comunității serviciilor de informații trebuie să colecteze uneori informații în masă pe baza semnalelor electromagnetice, în anumite circumstanțe, de exemplu pentru a identifica și a evalua amenințări noi sau emergente, directiva indică elementelor respective să acorde prioritate alternativelor care ar permite desfășurarea de activități cu țintă precisă, de colectare de informații pe baza semnalelor electromagnetice ([71]). Prin urmare, colectarea în masă de date va avea loc numai în cazul în care colectarea cu țintă precisă prin utilizarea unor elemente discriminante, și anume un identificator asociat unei ținte specifice (precum adresa de e-mail sau numărul de telefon al țintei), nu este posibilă „din cauza constrângerilor tehnice sau operaționale" ([72]). Aceasta se referă atât la modul în care sunt colectate informațiile pe baza semnalelor electromagnetice, cât și la ceea ce se colectează efectiv ([72]).

(73) În conformitate cu declarațiile ODNI, chiar și în cazul în care comunitatea serviciilor de informații nu poate utiliza identificatori specifici pentru a direcționa colectarea, aceasta va încerca să restrângă colectarea „cât mai mult posibil". Pentru a asigura acest lucru, aceasta „aplică filtre și alte instrumente tehnice pentru a-și concentra activitatea de colectare asupra instalațiilor care sunt susceptibile să conțină comunicații de informații secrete externe valoroase" [și care vor răspunde, astfel, cerințelor formulate de responsabilii politici din Statele Unite ale Americii în temeiul procedurii explicate la (70)]. În consecință, colectarea de date în masă va fi direcționată în cel puțin două moduri: în primul rând, ea va continua să vizeze anumite ținte specifice de informații externe (de exemplu, să obțină informații secrete prin interceptarea de semnale cu privire la activitățile unui grup terorist care operează într-o anumită regiune) și își va concentra colectarea asupra comunicațiilor care prezintă o legătură cu aceste obiective. În conformitate cu asigurarea oferită de ODNI, acest lucru se reflectă în faptul că „activitățile de colectare de informații secrete prin interceptarea de semnale desfășurate de Statele Unite ating numai o proporție scăzută a comunicațiilor care tranzitează internetul." ([73]) În al doilea rând, declarațiile ODNI oferă explicația potrivit căreia se vor utiliza filtre și alte instrumente tehnice pentru a concentra activitatea de colectare „cât mai exact posibil" și pentru a reduce la minimum cantitatea de „informații irelevante" colectate.

(74) În cele din urmă, inclusiv în cazul în care Statele Unite consideră necesară colectarea informațiilor pe baza semnalelor electromagnetice în masă, în condițiile enunțate în considerentele 70-73, PPD-28 limitează utilizarea acestor informații la o listă specifică de șase scopuri de securitate națională în vederea protejării vieții private și a libertăților civile ale tuturor persoanelor, indiferent de naționalitatea sau locul lor de reședință ([74]). Motivele admisibile cuprind măsuri pentru a depista și a contracara amenințările generate de spionaj, terorism, armele de

([68]) A se vedea nota de subsol 63.

([69]) De asemenea, ar trebui remarcat că, în conformitate cu secțiunea 2.4 din O.E. 12333, elementele comunității serviciilor de informații „trebuie să utilizeze tehnici de colectare cel mai puțin intruzive posibil în Statele Unite". În ceea ce privește limitările care prevăd înlocuirea colectării în masă de date cu operațiuni de colectare direcționate, a se vedea rezultatele unei evaluări de către Consiliul național al cercetării (National Research Council), astfel cum a fost prezentat de Agenția pentru Drepturi Fundamentale a Uniunii Europene: „Supravegherea de către serviciile de informații: garanții privind drepturile fundamentale și căile de atac în UE" (*Surveillance by intelligence services:fundamental rights, safeguards and remedies in the EU*) (2015), p. 18.

([70]) Declarațiile ODNI (anexa VI), p. 4.

([71]) A se vedea, de asemenea, secțiunea 5(d) din PPD-28 care indică directorului Serviciului național de informații, în coordonare cu șefii elementelor comunității serviciilor de informații relevante și Biroul pentru politica în domeniul științei și tehnologiei, să ofere președintelui un „raport de evaluare a fezabilității creării de software, care ar permite comunității serviciilor de informații să desfășoare mai ușor activitățile de obținere de informații cu țintă precisă, mai degrabă decât colectarea în masă." Potrivit informațiilor publice, rezultatul acestui raport a fost că „nu există nicio alternativă bazată pe software care să ofere un înlocuitor complet pentru colectarea în masă în depistarea unor amenințări la adresa securității naționale." A se vedea Reforma legată de activitățile de colectare de informații pe baza semnalelor electromagnetice, raportul aniversar pentru anul 2015.

([72]) A se vedea nota de subsol 63.

([73]) Declarațiile ODNI (anexa VI). Aceasta răspunde în mod explicit îngrijorării exprimate de autoritățile naționale pentru protecția datelor în avizul referitor la proiectul de decizie privind caracterul adecvat. A se vedea Avizul 01/2016 referitor la proiectul de decizie privind caracterul adecvat al Scutului de confidențialitate UE-SUA, emis de Grupul de lucru „Articolul 29" (adoptat la 13 aprilie 2016), p. 38, cu n. 47.

([74]) A se vedea secțiunea 2 din PPD-28.

distrugere în masă, amenințările la adresa securității cibernetice, forțele armate sau personalul militar, precum și amenințările infracționale transnaționale legate de celelalte cinci scopuri și vor fi revizuite cel puțin o dată pe an. În conformitate cu declarațiile guvernului SUA, elementele comunității serviciilor de informații și-au consolidat practicile analitice și standardele pentru analizarea informațiilor colectate pe baza semnalelor electromagnetice neevaluate pentru a se conforma acestor cerințe; utilizarea unor întrebări cu țintă precisă „se asigură că numai acele elemente considerate a fi de o valoare potențială de informare sunt prezentate vreodată analiștilor pentru examinare” ([75]).

(75) Aceste limitări sunt deosebit de relevante pentru datele cu caracter personal transferate în temeiul Scutului de confidențialitate UE-SUA, în special în cazul în care colectarea datelor cu caracter personal ar avea loc în afara Statelor Unite, inclusiv în perioada tranzitului pe cablurile transatlantice din UE către Statele Unite. Astfel cum a fost confirmat de către autoritățile SUA în declarațiile ODNI, limitările și garanțiile prevăzute – inclusiv cele ale PPD-28 – se aplică în cazul unei astfel de colectări ([76]).

(76) Deși nu sunt formulate în termeni juridici, aceste principii reflectă esența principiilor necesității și proporționalității. Colectarea cu țintă precisă este clar prioritizată, în timp ce colectarea în masă se limitează la situații (excepționale) în care colectarea cu țintă precisă nu este posibilă din motive tehnice sau operaționale. Inclusiv în cazul în care *colectarea în masă* nu poate fi evitată, „utilizarea” ulterioară a acestor date prin intermediul accesului se *limitează strict* la scopuri specifice și legitime privind securitatea națională ([77]).

(77) Întrucât PPD-28 este o directivă emisă de președinte în calitate de șef al executivului, cerințele acesteia sunt obligatorii pentru întreaga comunitate a serviciilor de informații și au fost puse în aplicare în continuare prin intermediul normelor și procedurilor agenției care transpun principiile generale în instrucțiuni specifice pentru operațiunile zilnice. În plus, deși Congresul nu are obligații în temeiul PPD-28, trebuie să ia, de asemenea, măsuri pentru a se asigura că activitățile de colectare și accesarea datelor cu caracter personal în Statele Unite sunt mai degrabă cu țintă precisă decât efectuate „în mod generalizat”.

(78) Din informațiile disponibile, inclusiv declarațiile primite de la guvernul american conform cărora, odată ce datele au fost transferate către organizații situate în Statele Unite și autocertificate în temeiul Scutului de confidențialitate UE-SUA, serviciile de informații americane pot doar ([78]) să caute date cu caracter personal în cazul în care cererea lor este în conformitate cu Legea privind supravegherea activităților străine de spionaj (*Foreign Intelligence Surveillance Act* – FISA) sau este depusă de Biroul Federal de Investigații pe baza unei așa-numite „scrisori privind securitatea națională” (NSL) ([79]). Există mai multe temeiuri juridice în cadrul FISA care pot fi utilizate pentru

([75]) Declarațiile ODNI (anexa VI), p. 4. A se vedea, de asemenea, Directiva nr. 203 privind comunitatea serviciilor de informații.

([76]) Declarațiile ODNI (anexa VI), p. 2. De asemenea, se aplică limitările prevăzute în O.E. 12333 (de exemplu, necesitatea ca informațiile colectate să răspundă priorităților în materie de informații stabilite de către Președinte).

([77]) A se vedea Schrems, punctul 93.

([78]) În plus, colectarea de date de către FBI se poate baza, de asemenea, pe autorizațiile organismelor de aplicare a legii (a se vedea secțiunea 3.2 din prezenta decizie).

([79]) Pentru explicații suplimentare privind utilizarea NSL, a se vedea Declarațiile ODNI (anexa VI), p. 13-14, cu n. 38. Astfel cum se indică în acesta, FBI poate recurge la NSL pentru a solicita informații nelegate de conținut în cazul unei investigații de securitate naționale autorizată pentru a proteja împotriva terorismului internațional sau a activităților clandestine de spionaj. În ceea ce privește transferurile de date în temeiul Scutului de confidențialitate UE-SUA privind protecția vieții private, cele mai relevante autorizații legale par a fi Legea privind confidențialitatea comunicațiilor electronice (Electronic Communications Privacy Act) (18 U.S.C. § 2709), care prevede că orice cerere de informații referitoare la abonați sau evidențe comerciale utilizează un „termen care identifică în mod specific o persoană, o entitate, un număr de telefon sau un cont”.

a colecta (și prelucra ulterior) datele cu caracter personal ale persoanelor vizate din UE transferate în temeiul Scutului de confidențialitate UE-SUA. Pe lângă secțiunea 104 din FISA ([80]), care reglementează supravegherea electronică individualizată tradițională, și secțiunea 402 din FISA ([81]) privind instalarea dispozitivelor de interceptare a convorbirilor (pen registers) sau de capturare și trasabilitate (trap and traces), cele două instrumente principale sunt secțiunea 501 din FISA (fosta secțiune 215 din Legea PATRIOT a SUA) și secțiunea 702 din FISA ([82]).

(79) În această privință, Legea SUA privind libertatea (USA FREEDOM Act), care a fost adoptată la 2 iunie 2015, interzice colectarea în masă a înregistrărilor pe baza secțiunii 402 din FISA (competența de interceptare și de capturare și trasabilitate), secțiunea 501 din FISA (anterior, secțiunea 215 din Legea PATRIOT a SUA) ([83]) și prin utilizarea NSL și, în schimb, impune utilizarea unor „termeni de selecție" specifici ([84]).

(80) Deși FISA prevede competențe legale pentru a efectua activități naționale de colectare de informații, inclusiv pe bază de semnale electromagnetice, evaluarea Comisiei a arătat că, în măsura în care datele cu caracter personal sunt transferate în temeiul Scutului de confidențialitate UE și SUA, aceste competențe restricționează, de asemenea, ingerința autorităților publice în colectarea și accesul cu țintă precisă.

(81) Acest lucru este clar pentru supravegherea electronică individualizată tradițională în conformitate cu secțiunea 104 din FISA ([85]). În ceea ce privește secțiunea 702 din FISA, care constituie baza pentru două programe importante de informații conduse de agențiile de informații din SUA (PRISM, UPSTREAM), căutările se efectuează în mod specific, prin utilizarea de selectoare individuale care identifică mijloacele de comunicare specifice, cum ar fi adresa de e-mail sau numărul de telefon al persoanei vizate, dar nu cuvinte cheie sau chiar numele persoanelor vizate ([86]). Prin urmare, conform celor observate de Comitetul de supraveghere a vieții private și a libertăților

([80]) 50 U.S.C. § 1804. Deși această autoritate juridică prevede „o enunțare a faptelor și circumstanțelor invocate de reclamant pentru a a-și justifica convingerea sa că (A) obiectul supravegherii electronice este o putere străină sau un agent al unei puteri străine", aceasta din urmă poate include persoane care nu sunt cetățeni americani care se angajează în terorism internațional sau activități internaționale de proliferare a armelor de distrugere în masă (inclusiv actele pregătitoare) [50 U.S.C. § 1801 (b) (1)]. Cu toate acestea, există doar o legătură teoretică cu datele cu caracter personal transferate în temeiul Scutului de confidențialitate UE-SUA, dat fiind faptul că situația de fapt trebuie, de asemenea, să justifice convingerea că „fiecare dintre infrastructurile sau locurile vizate de supravegherea electronică este utilizat, sau este pe cale de a fi utilizat, de o putere străină sau un agent al unei puteri străine". În orice caz, utilizarea acestei autorități necesită recurgerea la FISC care va evalua, printre altele, dacă, pe baza faptelor prezentate, există o suspiciune rezonabilă să creadă că aceasta este într-adevăr situația.

([81]) 50 U.S.C. § 1842 cu § 1841(2) și secțiunea 3127 de la titlul 18. Această competență nu privește conținutul comunicațiilor, ci vizează informații cu privire la clientul sau abonatul care folosește un serviciu (cum ar fi numele, adresa, numărul de abonat, perioada/tipul de servicii primite, sursa/mecanismul de plată). Aceasta necesită o cerere de emitere a unui ordin de către FISC (sau un magistrat al SUA) și utilizarea unui anumit termen de selecție în sensul § 1841(4), și anume o clauză care identifică în mod specific o persoană, un cont etc. și care este utilizat pentru a limita, în măsura posibilului, domeniul de aplicare al informațiilor solicitate.

([82]) În timp ce secțiunea 501 din FISA (fosta secțiune 215 din Legea PATRIOT a SUA) autorizează FBI să solicite un ordin judecătoresc care vizează producerea de „elemente concrete" (în special metadate telefonice, dar și documente comerciale), în scopul colectării de date operative externe, secțiunea 702 din FISA permite elementelor comunității americane a serviciilor de informații să solicite accesul la informații, inclusiv conținutul comunicațiilor pe internet, din Statele Unite, dar care vizează anumite persoane care nu sunt cetățeni americani din afara Statelor Unite.

([83]) Pe baza acestei dispoziții, FBI poate solicita „elemente concrete" (de exemplu, înregistrări, documente) pe baza unei dovezi care să arate Curții de Supraveghere a Activităților Străine de Spionaj (*Foreign Intelligence Surveillance Court* – FISC) că există motive întemeiate să se considere că acestea sunt relevante pentru o anumită investigație efectuată de FBI. La efectuarea percheziției, FBI trebuie să utilizeze termeni de selecție aprobați de FISC pentru care există o „suspiciune rezonabilă, care poate fi formulată" că această mențiune este asociată cu una sau mai multe puteri străine sau agenții acestora implicați în terorism internațional sau activități în curs de pregătire în acest sens. A se vedea PCLOB, secțiunea 215 din Raport, p. 59; NSA CLPO, Raportul privind transparența: Punerea în aplicare a legii SUA cu privire la evidențele comerciale FISA, 15 ianuarie 2016, pp. 4-6.

([84]) Declarațiile ODNI (anexa VI), p. 13 (n. 38).

([85]) A se vedea nota de subsol 81.

([86]) PCLOB, secțiunea 702 din Raport, p. 32-33 cu trimiteri ulterioare. În conformitate cu biroul său pentru viață privată, NSA trebuie să verifice dacă există o legătură între țintă și selector, trebuie să documenteze informațiile operative străine preconizate a fi achiziționate, aceste informații trebuie să fie revizuite și aprobate de doi analiști superiori din NSA, iar procesul global va fi urmărit pentru analize de conformitate ulterioare de către ODNI și Departamentul de Justiție. A se vedea NSA CLPO, Punerea în aplicare de către NSA a secțiunii 702 din Legea privind activitățile de colectare de informații externe, 16 aprilie 2014.

civile (*Privacy and Civil Liberties Oversight Board* – PCLOB), supravegherea în temeiul secțiunii 702 „constă în întregime din vizarea unor persoane [care nu sunt cetățeni americani] cu privire la care s-a stabilit o hotărâre individuală" ([87]). Ca urmare a unei „clauze de caducitate", secțiunea 702 din FISA va trebui să fie revizuită în 2017, moment în care Comisia va trebui să reevalueze garanțiile de care dispun cetățenii UE.

(82) În plus, în declarațiile sale, guvernul american a oferit Comisiei Europene asigurări explicite că serviciile de informații americane „nu sunt implicate în activități de supraveghere arbitrară a niciunei persoane, inclusiv cetățenii europeni de rând" ([88]). În ceea ce privește datele cu caracter personal colectate în Statele Unite, această declarație este susținută de dovezi empirice, care arată că cererile de acces transmise prin intermediul NSL și în temeiul FISA, atât în mod individual, cât și împreună, se referă doar la un număr relativ mic de ținte în comparație cu totalul fluxului de date pe internet ([89]).

(83) În ceea ce privește accesul la datele colectate și securitatea datelor, PPD-28 prevede că accesul „este limitat la personalul autorizat care are nevoie să cunoască informațiile pentru îndeplinirea misiunii lor" și că datele cu caracter personal „trebuie să fie prelucrate și stocate în condiții care să ofere o protecție adecvată și să împiedice accesul persoanelor neautorizate, în conformitate cu garanțiile aplicabile pentru informațiile sensibile". Personalul serviciilor de informații beneficiază de formare potrivită și adecvată cu privire la principiile enunțate în PPD-28 ([90]).

(84) În sfârșit, în ceea ce privește stocarea și difuzarea ulterioară a datelor cu caracter personal ale persoanelor vizate, colectate de serviciile de informații americane, PPD-28 prevede că toate persoanele, (inclusiv persoanele care nu sunt cetățeni americani) ar trebui să fie tratate cu respect și demnitate, că toate persoanele au interese legitime în prelucrarea datelor cu caracter personal ale acestora și că, prin urmare, elementele comunității serviciilor de informații trebuie să elaboreze politici care oferă garanții adecvate pentru astfel de date „concepute în mod rezonabil pentru a reduce la minimum diseminarea și păstrarea [acestora] ([91])".

([87]) PLCOB, secțiunea 702 din Raport, p. 111. A se vedea, de asemenea, Declarațiile ODNI (anexa VI), p. 9 („Colectarea în temeiul secțiunii 702 din FISA] nu este «în masă și nediferențiată», ci este strict orientată asupra colectării de informații externe de la ținte legitime identificate individual") și pagina 13, n. 36 (cu trimitere la un aviz FISC din 2014); NSA CLPO, Punerea în aplicare de către NSA a secțiunii 702 din Legea privind activitățile de colectare de informații externe, 16 aprilie 2014. Chiar în cazul UPSTREAM, NSA poate solicita numai interceptarea comunicațiilor electronice către, dinspre sau cu privire la selectoarele cu sarcini specifice.

([88]) Declarațiile ODNI (anexa VI), p. 18. A se vedea, de asemenea, p. 6, unde se menționează că procedurile aplicabile „demonstrează un angajament clar de a împiedica colectarea arbitrară și nediscriminatorie a informațiilor pe baza semnalelor electromagnetice și de a pune în aplicare – de la cele mai înalte niveluri ale administrației – principiul rezonabilității."

([89]) A se vedea Raportul de transparență privind utilizarea statistică a autorităților naționale de securitate, 22 aprilie 2015. Pentru obiectivul global al fluxului de date pe internet, a se vedea, de exemplu, Agenția pentru Drepturi Fundamentale a Uniunii Europene, Supravegherea de către serviciile de informații: garanții privind drepturile fundamentale și căile de atac în UE (2015), pp. 15-16. În ceea ce privește programul UPSTREAM, în conformitate cu un aviz declasificat al FISC din 2011, peste 90 % din comunicațiile electronice obținute în temeiul secțiunii 702 din FISA provin din programul PRISM, în timp ce mai puțin de 10 % au provenit din UPSTREAM. A se vedea FISC, Avizul memorandum, 2011 WL 10945618 (FISA Ct., 3 octombrie 2011), n. 21 (disponibil la adresa: http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf).

([90]) A se vedea secțiunea 4(a)(ii) din PPD-28. A se vedea, de asemenea, ODNI, Protecția informațiilor cu caracter personal ale tuturor persoanelor: un raport de situație privind dezvoltarea și aplicarea procedurilor în temeiul Directivei nr. 28 privind politica prezidențială, iulie 2014, p. 5, potrivit căreia „politicile elementelor comunității serviciilor de informații ar trebui să consolideze practicile și standardele analitice existente, prin care analiștii trebuie să încerce să structureze întrebări sau alți termeni de căutare și tehnici pentru a identifica informațiile secrete relevante pentru o sarcină validă de informare sau de aplicare a legii; să concentreze întrebările despre persoane pe categorii de informații care răspund la o cerință de informații sau de aplicare a legii; și să reducă la minimum revizuirea informațiilor cu caracter personal care nu sunt pertinente pentru cerințele de informații sau de aplicare a legii." A se vedea, de exemplu Activitățile CIA de colectare de informații pe baza semnalelor electromagnetice, p. 5; Politici și proceduri ale FBI referitoare la Directiva nr. 28 privind politica prezidențială, p. 3. În conformitate cu raportul din 2016 privind progresele realizate cu privire la reforma colectării de informații pe baza semnalelor electromagnetice, elementele comunității serviciilor de informații (inclusiv FBI, CIA și NSA) au luat măsuri de sensibilizare a personalului lor la cerințele PPD-28 prin crearea de noi politici de formare sau modificarea celor existente.

([91]) Conform declarațiilor ODNI, aceste restricții se aplică indiferent dacă informațiile au fost colectate în masă sau cu o țintă precisă și indiferent de naționalitatea persoanei.

(85) Guvernul american a explicat că această cerință de rezonabilitate implică faptul că elementele comunității serviciilor de informații nu vor trebui să adopte „orice măsură teoretic posibilă", dar vor trebui să „își armonizeze eforturile de protejare a vieții private și a libertăților civile legitime cu necesitățile practice ale activităților de colectare de informații electromagnetice" ([92]). În acest sens, persoanele care nu sunt cetățeni americani vor fi tratate în același mod ca cetățenii americani, pe baza procedurilor aprobate de procurorul general ([93]).

(86) În conformitate cu aceste norme, păstrarea datelor este, în general, limitată la o perioadă maximă de cinci ani, cu excepția cazului în care există o dispoziție specifică în drept sau o dispoziție expresă emisă de directorul Serviciului național de informații după o evaluare atentă a preocupărilor privind viața privată – luând în considerare opiniile responsabilului ODNI pentru protecția libertăților civile, precum și ale funcționarilor agenției pentru protecția vieții private și a libertăților civile – conform căreia păstrarea în continuare este în interesul securității naționale ([94]). Activitatea de diseminare este limitată la cazurile în care informațiile sunt relevante pentru obiectivul care stă la baza colectării și, prin urmare, răspund unei cerințe de informații externe sau de aplicare a legii ([95]).

(87) Potrivit asigurărilor oferite de guvernul SUA, informațiile cu caracter personal nu pot fi difuzate numai pe baza faptului că persoana respectivă este o persoană care nu este cetățean american și „informațiile obținute pe baza semnalelor electromagnetice despre activitățile obișnuite ale unei persoane străine nu ar trebui considerate informații externe care ar putea fi diseminate sau păstrate în permanență prin acest simplu fapt, cu excepția cazului în care aceste informații răspund în alt mod unei cereri autorizate de informații externe" ([96]).

(88) Pe baza tuturor elementelor prezentate mai sus, Comisia concluzionează că există norme în vigoare în Statele Unite menite să limiteze orice imixtiune în scopul securității naționale cu drepturile fundamentale ale persoanelor ale căror date cu caracter personal sunt transferate din UE către Statele Unite în temeiul Scutului de confidențialitate UE-SUA la ceea ce este strict necesar pentru atingerea obiectivului legitim în cauză.

(89) După cum reiese din analiza de mai sus, legislația Statelor Unite asigură faptul că măsurile de supraveghere nu vor fi utilizate decât pentru obținerea de informații operative străine ([97]), ceea ce constituie un obiectiv legitim de

([92]) A se vedea Declarațiile ODNI (anexa VI).

([93]) A se vedea secțiunea 4(a)(i) din PPD-28 cu Sec 2.3 din O.E. 12333.

([94]) Secțiunea 4(a)(i) din PPD-28; Declarațiile ODNI (anexa VI), p. 7. De exemplu, pentru informațiile cu caracter personal colectate în temeiul secțiunii 702 din FISA, procedurile NSA de reducere la minimum aprobate de FISC prevăd, ca regulă generală, că metadatele și conținuturile neevaluate pentru PRISM se păstrează pentru o perioadă de cel mult cinci ani, în timp ce datele UPSTREAM sunt păstrate pentru maximum doi ani. NSA respectă aceste limite de stocare printr-un proces automatizat care elimină datele colectate la sfârșitul respectivelor perioade de păstrare a datelor. A se vedea NSA secțiunea 702 din FISA Procedurile de reducere la minimum, Secțiunea 7 cu Secțiunea 6(a)(1); NSA CLPO, Punerea în aplicare de către NSA a secțiunii 702 din Legea privind supravegherea activităților străine de spionaj, 16 aprilie 2014. De asemenea, păstrarea în conformitate cu Secțiunea 501 din FISA (fosta secțiune 215 din Legea PATRIOT a SUA) este limitată la cinci ani, cu excepția cazului în care datele cu caracter personal fac parte din activități autorizate în mod corespunzător de difuzare de informații operative străine sau dacă Departamentul de Justiție recomandă NSA în scris că înregistrările sunt supuse unei obligații de păstrare în litigii pendinte sau viitoare. A se vedea NSA, CLOP, Raportul privind transparența: Punerea în aplicare a legii SUA cu privire la evidențele comerciale FISA (*USA Freedom Act Business Records FISA Implementation*), 15 ianuarie 2016.

([95]) În special, în cazul secțiunii 501 din FISA (fosta secțiune 215 din Legea PATRIOT a SUA), diseminarea de informații cu caracter personal poate avea loc numai în scopul combaterii terorismului sau ca dovadă a unei infracțiuni; în cazul secțiunii 702 din FISA numai dacă există un scop valid legat de colectarea de informații externe sau de aplicarea legii. Cf., NSA, CLPO, Punerea în aplicare de către NSA a secțiunii 702 din Legea privind supravegherea activităților străine de spionaj, 16 aprilie 2014; Raportul privind transparența: Punerea în aplicare a legii SUA cu privire la evidențele comerciale FISA (*USA Freedom Act Business Records FISA Implementation*), 15 ianuarie 2016. A se vedea, de asemenea, Măsurile de protecție a libertăților civile și vieții private ale NSA pentru activitățile cu țintă precisă de colectare de informații SIGINT în temeiul Decretului 12333, 7 octombrie 2014.

([96]) Declarațiile ODNI (anexa VI), p. 7 (cu trimiteri la Directiva nr. 203 privind comunitatea serviciilor de informații (*Intelligence Community Directive* – ICD) (203).

([97]) Curtea de Justiție a clarificat faptul că securitatea națională constituie un obiectiv legitim de politică. A se vedea Schrems, punctul 88. A se vedea, de asemenea, *Digital Rights Ireland și alții,* punctele 42-44 și 51, în care Curtea de Justiție a considerat că lupta împotriva formelor grave de criminalitate, în special a criminalității organizate și a terorismului, poate depinde într-o mare măsură de utilizarea tehnicilor moderne de investigare. În plus, spre deosebire de anchetele penale, care vizează, în general, stabilirea retroactivă a răspunderii și a vinovăției pentru comportamente anterioare, activitățile serviciilor de informații se axează deseori pe prevenirea amenințărilor la adresa securității naționale înainte de producerea prejudiciilor. Prin urmare, astfel de anchete pot avea deseori să acopere o gamă mai largă de posibili actori („ținte"), precum și o zonă geografică mai vastă. A se vedea Curtea Europeană a Drepturilor Omului, hotărârea pronunțată în cauza *Weber and Saravia/Germania* din 29 iunie 2006, decizia nr. 54934/00, punctele 105-118 (cu privire la așa-numita „monitorizare strategică").

politică, și sunt adaptate cât mai mult posibil. În special, colectarea în masă de date este permisă numai în cazul în care colectarea cu țintă precisă prin utilizarea unor elemente discriminante nu este posibilă și va fi însoțită de garanții suplimentare pentru a reduce la minimum cantitatea de date colectate și accesul ulterior la acestea (care va trebui să aibă o țintă precisă și să fie permis numai în scopuri specifice).

(90) Conform evaluării Comisiei, aceste acțiuni sunt conforme cu standardul stabilit de Curtea de Justiție în cauza *Schrems*, conform căreia legislația care cuprinde o ingerință în drepturile fundamentale garantate la articolele 7 și 8 din cartă trebuie să impună „o serie de cerințe minime” ([98]) și „nu este limitată la strictul necesar o reglementare care autorizează în mod generalizat stocarea integralității datelor cu caracter personal ale tuturor persoanelor ale căror date au fost transferate din Uniune către Statele Unite, fără a se face vreo diferențiere, limitare sau excepție în funcție de obiectivul urmărit și fără a se prevedea un criteriu obiectiv care să permită delimitarea accesului autorităților publice la date și utilizarea lor ulterioară în scopuri precise, strict restrânse și susceptibile să justifice ingerința pe care o implică atât accesarea, cât și utilizarea acestor date” ([99]). Nu se intenționează nicio colectare și stocare nelimitată de date ale tuturor persoanelor, fără nicio limitare, și, de asemenea, niciun acces neîngrădit. În plus, declarațiile furnizate Comisiei, inclusiv în ceea ce privește asigurarea faptului că activitățile de colectare de informații secrete prin interceptarea de semnale desfășurate de Statele Unite ating numai o proporție scăzută a comunicațiilor care tranzitează internetul, exclud ipoteza că ar exista un acces „în mod generalizat” ([100]) la conținutul comunicărilor electronice.

3.1.2. Protecția juridică efectivă

(91) Comisia a evaluat atât mecanismele de supraveghere existente în Statele Unite cu privire la orice imixtiune a autorităților americane de informații cu datele cu caracter personal transferate către Statele Unite și modalitățile disponibile pentru persoanele vizate pentru o cale de atac individuală.

Supravegherea

(92) Comunitatea serviciilor de informații ale SUA face obiectul diverselor mecanisme de reexaminare și de supraveghere care depind de cele trei puteri ale statului. Printre acestea se numără organisme interne și externe din cadrul puterii executive, o serie de comitete al Congresului, precum și un control jurisdicțional, acesta din urmă vizând în mod expres activități desfășurate în temeiul Legii privind supravegherea activităților străine de spionaj.

(93) În primul rând, activitățile de spionaj ale autorităților americane fac obiectul supravegherii extinse din cadrul puterii executive.

(94) În conformitate cu secțiunea 4 litera (a) punctul (iv) din PPD-28, politicile și procedurile elementelor comunității serviciilor de informații „trebuie să includă măsuri adecvate pentru a facilita supravegherea punerii în aplicare a garanțiilor privind protecția datelor cu caracter personal”; aceste măsuri ar trebui să includă auditarea periodică ([101]).

([98]) A se vedea Schrems, punctul 91 cu trimiteri suplimentare.
([99]) *Schrems*, punctul 93.
([100]) Cf. *Schrems*, punctul 94.
([101]) ODNI, Protecția informațiilor cu caracter personal ale tuturor persoanelor: un raport de situație privind elaborarea și aplicarea procedurilor în temeiul Directivei nr. 28 privind politica prezidențială, p. 7. A se vedea, de exemplu Activitățile CIA de colectare de informații pe baza semnalelor electromagnetice, p. 6 (Conformitate); Politici și proceduri ale FBI referitoare la Directiva nr. 28 privind politica prezidențială, secțiunea III(A)(4), (B)(4); NSA, PPD-28 secțiunea 4 Proceduri, 12 ianuarie 2015, secțiunea 8.1, 8.6(c).

(95) Mai multe niveluri de supraveghere au fost instituite în acest sens, inclusiv responsabili pentru protecția libertăților civile și a vieții private, inspectori generali, Biroul pentru protecția vieții private și a libertăților civile al ODNI, PCLOB și Comitetul pentru supravegherea serviciilor de informații al Președintelui. Aceste funcții de control sunt sprijinite de personal cu sarcini legate de respectarea conformității din toate agențiile ([102]).

(96) Astfel cum a explicat guvernul SUA ([103]), în diferitele departamente cu responsabilități de colectare de informații și agenții de informații există responsabilii pentru protecția *libertăților civile sau a vieții private* cu responsabilități de supraveghere ([104]). Deși competențele specifice ale acestor agenții pot varia în funcție de statut, acestea cuprind, de regulă, proceduri de supraveghere care să asigure că departamentul/agenția ia în considerare în mod corespunzător aspectele legate de protecția vieții private și a libertăților civile și a instituit proceduri adecvate de soluționare a plângerilor din partea persoanelor care consideră că li s-a încălcat dreptul la viață privată sau libertățile civile (și, în unele cazuri, de exemplu ODNI, poate avea competența de a investiga plângerile ([105])). Șeful departamentului/agenției, la rândul său, trebuie să se asigure că responsabilul primește toate informațiile și are acces la toate materialele necesare pentru îndeplinirea funcțiilor sale. Responsabilii pentru protecția libertăților civile și a vieții private raportează periodic Congresului și PCLOB, inclusiv numărul și natura plângerilor primite de către departament/agenție și un rezumat al hotărârii privind astfel de plângeri, revizuiri și cercetări întreprinse și impactul activităților efectuate de responsabil ([106]). În conformitate cu evaluarea efectuată de autoritățile naționale pentru protecția datelor, controalele interne exercitate de responsabilii cu libertățile civile sau cu protecția confidențialității poate fi considerată ca fiind „relativ solide", deși, în opinia autorităților susmenționate, acestea nu îndeplinesc nivelul necesar de independență ([107]).

(97) În plus, fiecare element al comunității serviciilor de informații are propriul inspector general însărcinat, printre altele, să supravegheze activitățile străine de spionaj ([108]). Acesta include, în cadrul ODNI, un birou al inspectorului general cu competență generală asupra întregii comunități a serviciilor de informații și autorizat pentru a investiga plângeri sau informații privind acuzații de comportament ilicit sau abuz de autoritate în legătură cu ODNI și/sau programele și activitățile comunității serviciilor de informații ([109]). Inspectorii generali sunt unități independente ([110]) din punct de vedere statutar responsabile cu efectuarea de audituri și investigații privind programele și operațiunile efectuate de agenție pentru scopuri naționale de informații, inclusiv în caz de abuz sau încălcare a legii ([111]). Aceștia sunt autorizați să aibă acces la toate înregistrările, rapoartele, auditurile, analizele,

([102]) De exemplu, NSA are peste 300 de angajați în Direcția pentru respectarea conformității. A se vedea Observațiile ODNI (anexa VI), p. 7.

([103]) A se vedea mecanismul Ombudsmanului (anexa III), secțiunea 6(b) (i)-(iii).

([104]) A se vedea 42 U.S.C. § 2000ee-1. Acestea includ, de exemplu, Departamentul de Stat, Departamentul de Justiție (inclusiv FBI), Departamentul pentru Securitate Internă al SUA, Departamentul Apărării, NSA, CIA și ODNI.

([105]) În conformitate cu guvernul american, dacă Biroul pentru protecția vieții private și a libertăților civile al ODNI primește o plângere, acesta va coordona și cu alte elemente ale comunității serviciilor de informații cu privire la modul în care plângerea ar trebui să fie prelucrată ulterior în cadrul comunității serviciilor de informații. A se vedea mecanismul Ombudsmanului (anexa III), secțiunea 6(b) (ii).

([106]) A se vedea 42 U.S.C. § 2000ee-1 (f)(1),(2).

([107]) Avizul 01/2016 referitor la proiectul de decizie privind caracterul adecvat al Scutului de confidențialitate UE-SUA, emis de Grupul de lucru „Articolul 29" (adoptat la 13 aprilie 2016), p. 41.

([108]) Declarațiile ODNI (anexa VI), p. 7. A se vedea, de exemplu, NSA, PPD-28 secțiunea 4 Proceduri, 12 ianuarie 2015, secțiunea 8.1; Activitățile CIA de colectare de informații pe baza semnalelor electromagnetice, p. 7. (Responsabilități).

([109]) Acest inspector general (funcție creată în octombrie 2010) este desemnat de președinte, cu confirmarea Senatului, și poate fi îndepărtat numai de către președinte, nu de DNI.

([110]) Acești inspectori generali au o titularizare sigură și pot fi demiși doar de către președinte, care trebuie să comunice Congresului în scris motivele care justifică o astfel de măsură. Acest lucru nu înseamnă neapărat că aceștia nu primesc deloc instrucțiuni. În unele cazuri, șeful departamentului poate interzice inspectorului general să demareze, desfășoare sau finalizeze un audit sau anchetă, în cazul în care acest lucru este considerat necesar pentru a conserva interesele naționale importante (de securitate). Cu toate acestea, Congresul trebuie să fie informat cu privire la exercitarea acestei competențe și, pe această bază, să tragă la răspundere directorul respectiv. A se vedea, de exemplu, Legea privind inspectorul general din 1978,§ 8 (IG al Departamentului Apărării); § 8E (IG al Departamentului de Justiție), § 8G (d)(2)(A),(B) (IG al NSA); 50. U.S.C. § 403q (b) (IG pentru CIA); Legea privind autorizarea serviciilor de informații pentru anul fiscal 2010, secțiunea 405 (f) (IG pentru serviciile de informații). În conformitate cu evaluarea efectuată de autoritățile naționale de protecție a datelor, inspectorii generali *„ar putea îndeplini criteriul de independență organizațională, astfel cum este definit de Curtea de Justiție a Uniunii Europene și de Curtea Europeană a Drepturilor Omului (CEDO), cel puțin din momentul în care noul proces de numire li se aplică tuturor.*". A se vedea Avizul 01/2016 referitor la proiectul de decizie privind caracterul adecvat al Scutului de confidențialitate UE-SUA, emis de Grupul de lucru „Articolul 29" (adoptat la 13 aprilie 2016), p. 40.

([111]) A se vedea Observațiile ODNI (anexa VI), p. 7. A se vedea, de asemenea, Legea privind inspectorii generali din 1978, astfel cum a fost modificată, Pub. L. 113-126 din 7 iulie 2014.

documentele, dosarele, recomandările sau alte documente pertinente, dacă este necesar prin somații, și pot lua declarații ale martorilor ([112]). Deși inspectorii generali nu pot decât să emită recomandări neobligatorii privind măsuri corective, rapoartele lor, inclusiv cu privire la acțiunile de monitorizare (sau lipsa acestora) sunt făcute publice și transmise Congresului, care poate să își exercite, pe această bază, funcția de supraveghere ([113]).

(98) În plus, Comitetul de supraveghere a vieții private și a libertăților civile (*Privacy and Civil Liberties Oversight Board* – PCLOB), un organism independent ([114]) din cadrul executivului, format din cinci membri ([115]) care sunt numiți de Președinte cu aprobarea Senatului cu un mandat de 6 ani și care aparțin celor două mari partide politice, este însărcinat cu responsabilități în domeniul politicilor de combatere a terorismului și cu punerea în aplicare a acestora, în vederea protejării vieții private și a libertăților civile. În cadrul reexaminării efectuate cu privire la acțiunea comunității serviciilor de informații, acesta poate avea acces la toate înregistrările, rapoartele, auditurile, analizele, documentele, dosarele și recomandările agențiilor relevante, inclusiv informații clasificate, poate desfășura interviuri și audia martori. Comitetul primește rapoarte de la responsabilii pentru protecția libertățile civile și a vieții private din mai multe departamente/agenții federale ([116]), poate emite recomandări pentru acestea și prezintă rapoarte periodice către comisiile Congresului și către Președinte ([117]). De asemenea, PCLOB are sarcina, în limitele mandatului său, să pregătească un raport de evaluare a aplicării PPD-28.

(99) În cele din urmă, mecanismele de supraveghere menționate anterior sunt completate de *Comitetul pentru supravegherea serviciilor de informații* instituit în cadrul Consiliului consultativ de privind serviciile de informații al președintelui, care supraveghează respectarea Constituției și a tuturor normelor aplicabile de către serviciile de informații ale SUA.

(100) Pentru a facilita supravegherea, elementele comunității serviciilor de informații sunt încurajate să conceapă sisteme de informații care să permită monitorizarea, înregistrarea și examinarea întrebărilor sau a altor căutări de informații cu caracter personal ([118]). Organismele de supraveghere și de asigurare a conformității vor verifica periodic practicile elementelor comunității serviciilor de informații pentru protecția informațiilor personale conținute în informațiile colectate pe bază de semnale electromagnetice și conformitatea acestora cu procedurile respective ([119]).

(101) Aceste funcții de control sunt susținute, de asemenea, de cerințe de raportare cuprinzătoare cu privire la neconformitate. În special, procedurile agenției ar trebui să asigure că, în cazul în care apare o problemă de conformitate semnificativă care implică informații cu caracter personal ale oricărei persoane, indiferent de naționalitate, colectate prin intermediul informațiilor pe baza semnalelor electromagnetice, astfel de probleme trebuie raportate imediat șefului elementului comunității serviciilor de informații, care, la rândul său, va notifica directorul Serviciului național de informații care, în temeiul PPD-28, stabilește dacă sunt necesare măsuri corective ([120]). În plus, în conformitate cu O.E. 12333, toate elementele comunității serviciilor de informații au obligația de a informa Comitetul pentru supravegherea serviciilor de informații privind incidentele de neconformitate ([121]). Aceste mecanisme asigură că problema va fi abordată la cel mai înalt nivel în cadrul comunității

([112]) A se vedea Legea privind inspectorii generali din 1978, § 6.

([113]) A se vedea Observațiile ODNI (anexa VI), p. 7. A se vedea, de asemenea, Legea privind inspectorii generali din 1978, § § 4(5), 5. În conformitate cu secțiunea 405(b)(3),(4) din Legea privind autorizarea serviciilor de informații pentru exercițiul fiscal 2010, Pub. L. 111-259 din 7 octombrie 2010, IG pentru serviciile de informații va ține la curent DNI, precum și Congresul, cu privire la necesitatea și progresul acțiunilor corective.

([114]) În conformitate cu evaluarea efectuată de autoritățile naționale de protecție a datelor, PCLOB a demonstrat, în trecut, că „dispune de competențe independente". A se vedea Avizul 01/2016 referitor la proiectul de decizie privind caracterul adecvat al Scutului de confidențialitate UE-SUA, emis de Grupul de lucru „Articolul 29" (adoptat la 13 aprilie 2016), p. 42.

([115]) În plus, PCLOB angajează aproximativ 20 de persoane în cadrul personalului obișnuit. A se vedea https://www.pclob.gov/about-us/staff.html.

([116]) Acestea includ cel puțin Ministerul Justiției, Departamentul de Apărare, Departamentul pentru Securitate Internă al SUA, directorul Serviciului național de informații și Agenția Centrală de Informații, precum și orice alt departament, agenție sau element al executivului desemnate de PCLOB să fie adecvate pentru cerințele de acoperire.

([117]) A se vedea 42 U.S.C. § 2000ee. A se vedea, de asemenea, mecanismul Ombudsmanului (anexa III), secțiunea 6(b) (iv). Printre altele, PCLOB trebuie să prezinte un raport atunci când o agenție din cadrul executivului refuză să urmeze avizul său.

([118]) ODNI, Protecția informațiilor cu caracter personal ale tuturor persoanelor: raport de situație privind dezvoltarea și aplicarea procedurilor în temeiul Directivei nr. 28 privind politica prezidențială, p. 7-8.

([119]) Id. la p. 8. A se vedea, de asemenea, Declarațiile ODNI (anexa VI), p. 9.

([120]) ODNI, Protecția informațiilor cu caracter personal ale tuturor persoanelor: un raport de situație privind elaborarea și aplicarea procedurilor în temeiul Directivei nr. 28 privind politica prezidențială, p. 7. A se vedea, de exemplu, NSA, PPD-28 secțiunea 4 Proceduri, 12 ianuarie 2015, secțiunea 7.3, 8.7(c),(d); Politici și proceduri ale FBI referitoare la Directiva nr. 28 privind politica prezidențială, secțiunea III.(A)(4), (B)(4); Activitățile CIA de colectare de informații pe baza semnalelor electromagnetice, p. 6 (Conformitate) și p. 8 (Responsabilități).

([121]) A se vedea O.E. 12333, secțiunea 1.6(c).

serviciilor de informații. În cazul în care este vorba despre o persoană care nu este cetățean american, directorul Serviciului național de informații, în consultare cu Secretarul de Stat și șeful departamentului sau al agenției de notificare, trebuie să stabilească dacă ar trebui să se ia măsuri pentru a informa guvernele străine relevante, în conformitate cu normele de protecție a surselor și metodelor și a personalului din SUA ([122]).

(102) În al doilea rând, pe lângă aceste mecanisme de supraveghere din cadrul puterii executive, Congresul SUA, în special *comisiile pentru informații și pentru sistemul judiciar ale Camerei Reprezentanților și Senatului*, au responsabilități de supraveghere a activităților străine de spionaj ale SUA, inclusiv activitățile SUA de colectare de informații sub formă de semnale electromagnetice. În conformitate cu Legea privind securitatea națională, „[p]reședintele se asigură că comisiile pentru informații ale Congresului sunt ținute la curent pe deplin cu privire la activitățile de spionaj ale Statelor Unite, inclusiv orice activitate semnificativă anticipată de colectare de informații în conformitate cu cerințele acestui subcapitol" ([123]). De asemenea, „[p]reședintele se asigură că orice activitate ilegală de spionaj este raportată prompt comisiilor pentru informații ale Congresului, precum și orice măsuri corective care au fost luate sau sunt planificate în legătură cu o astfel de activitate ilegală" ([124]). Membrii acestor comisii au acces la informații clasificate, precum și la metode și programe de spionaj ([125]).

(103) Legile ulterioare au extins și au perfecționat cerințele de raportare în ceea ce privește atât elementele comunității serviciilor de informații, cât și inspectorii generali competenți și procurorul general. De exemplu, FISA solicită procurorului general să „informeze pe deplin" comisiile pentru informații și pentru sistemul judiciar ale Camerei Reprezentanților și Senatului cu privire la activitățile autorităților publice în temeiul anumitor secțiuni din FISA ([126]). De asemenea, FISA solicită autorităților publice să furnizeze comisiilor din cadrul Congresului copii după „toate deciziile, ordinele sau opiniile Curții Activităților de Spionaj Extern sau ale instanței de recurs a Curții de Supraveghere a Activităților de Spionaj Extern care includ o construcție sau interpretare semnificativă a dispozițiilor din FISA". În special în ceea ce privește supravegherea în temeiul secțiunii 702 din FISA, supravegherea este exercitată prin rapoarte prevăzute de lege către comisiile pentru informații și pentru sistemul judiciar, precum și informări și audieri frecvente. Printre acestea se numără un raport semestrial al procurorului general care descrie utilizarea secțiunii 702 din FISA, cu documente justificative, inclusiv, în special, rapoarte de conformitate ale Ministerului de Justiție și ODNI și o descriere a oricăror cazuri de neconformitate ([127]), precum și o evaluare semestrială separată efectuată de către procurorul general și DNI privind respectarea procedurilor de direcționare și reducere la minimum, inclusiv conformitatea cu procedurile menite să asigure că se colectează într-un scop valid legat de activități străine de spionaj ([128]). De asemenea, Congresul primește rapoarte elaborate de inspectorii generali care sunt autorizați să evalueze respectarea de către agenții a procedurilor de direcționare și de reducere la minimum și orientările procurorului general.

(104) În conformitate cu Legea SUA privind libertatea din 2015, guvernul american trebuie să comunice Congresului (și publicului larg) în fiecare an, printre altele, numărul de ordine și directive FISA solicitate și primite, precum și estimări ale numărului de persoane care sunt cetățeni americani și care nu sunt cetățeni americani vizate de supraveghere ([129]). Legea impune, de asemenea, o raportare publică suplimentară cu privire la numărul de NSL emise, de asemenea, atât în ceea ce privește atât cetățeni americani, cât și persoane care nu sunt cetățeni

([122]) PPD-28, secțiunea 4(a)(iv).
([123]) A se vedea secțiunea 501(a)(1) [50 U.S.C § 413(a)(1)]. Această dispoziție conține cerințele generale în ceea ce privește supravegherea Congresului în materie de securitate națională.
([124]) A se vedea secțiunea 501 (b) [50 U.S.C. § 413 (b)].
([125]) A se vedea secțiunea 501 (d) [50 U.S.C. § 413 litera (d)].
([126]) A se vedea 50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f.
([127]) A se vedea 50 U.S.C. § 1881f.
([128]) A se vedea 50 U.S.C. § 1881a(l)(1).
([129]) A se vedea USA FREEDOM Act din 2015, Pub. L. nr. 114-23, Sec. 602(a). În plus, în conformitate cu secțiunea 402, „directorul Serviciului național de informații, în consultare cu procurorul general, efectuează o analiză de declasificare a fiecărei decizii, ordin sau aviz emise de Curtea de Supraveghere a Activităților Străine de Spionaj sau de Curtea de revizuire privind Supravegherea Activităților Străine de Spionaj [astfel cum sunt definite în secțiunea 601(e)] care include o construcție sau interpretarea semnificativă a unei dispoziții de drept, inclusiv orice construcție sau interpretare semnificativă sau nouă a noțiunii «termen de selecție specific» și, în concordanță cu această revizuire, pune la dispoziția publicului, în măsura posibilului, fiecare astfel de decizii sau concluzii."

americani (permițând, în același timp, beneficiarilor de ordine și certificări FISA, precum și destinatarilor cererilor NSL, să prezinte rapoarte de transparență în anumite condiții) ([130]).

(105) În al treilea rând, activitățile de spionaj întreprinse de autoritățile publice americane pe baza FISA permit verificarea și, în unele cazuri, autorizarea prealabilă a măsurilor, de către Curtea FISA (FISC) ([131]), o instanță independentă ([132]) ale cărei decizii pot fi contestate în fața Curții de revizuire privind activitățile străine de spionaj (FISCR) ([133]) și, în cele din urmă, Curtea Supremă a Statelor Unite ([134]). În cazul unei autorizații prealabile, autoritățile solicitante (FBI, NSA, CIA etc.) vor trebui să transmită un proiect de cerere avocaților Departamentului pentru Securitate Națională din cadrul Departamentului de Justiție care îl va examina și, dacă este necesar, va solicita informații suplimentare ([135]). De îndată ce cererea a fost finalizată, aceasta va trebui să fie aprobată de către procurorul general, procurorul general adjunct sau procurorul general adjunct pentru securitatea națională ([136]). Departamentul de Justiție va transmite ulterior cererea către FISC, care o va examina și va lua o hotărâre preliminară cu privire la modul de a acționa ([137]). În cazul în care are loc o audiere, FISC are autoritatea de a audia martori, ceea ce poate include consultanță de specialitate ([138]).

(106) FISC beneficiază (la fel ca și FISCR) de sprjinul furnizat de un grup permanent de cinci persoane care au expertiză în domeniul securității naționale, precum și al libertăților civile ([139]). Din acest grup, instanța va desemna o persoană care să servească drept amicus curiae pentru a contribui la luarea în considerare a oricărei cereri pentru un ordin sau o revizuire care, în opinia instanței, prezintă o interpretare nouă sau semnificativă a legii, cu excepția cazului în care instanța constată că o astfel de numire nu este adecvată ([140]). Acest fapt asigură, în special, că aspectele legate de confidențialitate sunt reflectate în mod corespunzător în evaluarea Curții. De asemenea, instanța poate să numească o persoană sau organizație în calitate de *amicus curiae*, inclusiv furnizarea de expertiză tehnică, ori de câte ori consideră necesar acest lucru, sau, la depunerea unei moțiuni, acordă unei persoane sau organizații permisiunea de a prezenta observații cu titlu de *amicus curiae* ([141]).

([130]) Legea SUA privind libertatea, secțiunea 602(a), 603(a).

([131]) Pentru anumite tipuri de supraveghere, în mod alternativ, un judecător magistrat al SUA desemnat public de către președintele Curții Supreme a Statelor Unite poate avea competența de a judeca cereri și de a pronunța ordine.

([132]) FISC este alcătuită din unsprezece judecători numiți de către președintele Curții Supreme a Statelor Unite dintre judecătorii din cadrul instanțelor districtuale din SUA, care anterior au fost numiți de Președinte și confirmați de către Senat. Judecătorii, care au titularizare pe viață, pot fi demiși numai pentru motive temeinice și fac parte din FISC prin intermediul unor mandate eșalonate de șapte ani. FISA impune ca judecătorii să provină din cel puțin șapte circuite judiciare diferite din SUA. A se vedea Sec 103 din FISA [50 U.S.C. 1803 (a)]; PCLOB, secțiunea 215 din Raport, p. 174-187. Judecătorii sunt sprijiniți de funcționari cu experiență judiciară care constituie juriștii instanței respective și pregătesc o analiză juridică privind cererile de colectare. A se vedea PCLOB, secțiunea 215 din Raport, p. 178; Scrisoare din partea distinsului Reggie B. Walton, președintele completului de judecată, Curtea de Supraveghere a Activităților Străine de Spionaj a SUA, către distinsul Patrick J. Leahy, președinte al Comisiei pentru sistemul judiciar, Senatul SUA (29 iulie 2013) („Scrisoarea Walton"), p. 2-3.

([133]) FISCR este formată din trei judecători numiți de către președintele Curții Supreme a Statelor Unite și provin din instanțe districtuale sau curți de apel din SUA, care servesc un termen eșalonat de șapte ani. A se vedea secțiunea 103 FISA [50 U.S.C. § 1803 (b)].

([134]) A se vedea 50 U.S.C. §§ 1803 (b), 1861 a (f), 1881 a (h), 1881 a (i)(4).

([135]) De exemplu, mai multe detalii factuale cu privire la ținta supravegherii, informații tehnice referitoare la metodologia de supraveghere sau asigurări cu privire la modul în care informațiile obținute vor fi utilizate și diseminate. A se vedea PCLOB, secțiunea 215 din Raport, p. 177.

([136]) 50 U.S.C. §§ 1804 (a), 1801 (g).

([137]) FISC poate să aprobe cererea, să solicite informații suplimentare, să stabilească necesitatea unei audieri sau să indice un posibil refuz al cererii. Pe baza acestei determinări preliminare, autoritatea publică va face cerere finală. Aceasta din urmă poate include modificări substanțiale aduse la cererea inițială pe baza observațiilor preliminare ale judecătorului. Deși o mare parte dintre cererile finale sunt aprobate de către FISC, o parte substanțială din acestea conțin modificări substanțiale aduse la cererea inițială, de exemplu, 24 % din cererile aprobate pentru perioada iulie-septembrie 2013. A se vedea PCLOB, secțiunea 215 din Raport, p. 179; Scrisoarea Walton, p. 3.

([138]) PCLOB, secțiunea 215 din Raport, p. 179, n. 619.

([139]) 50 U.S.C. § 1803 (i)(1),(3)(A). Aceste noi texte legislative pun în aplicare recomandările PCLOB privind instituirea unui corp de experți în domeniul vieții private și a libertăților civile, care poate servi în calitate de amicus curiae, pentru a furniza instanței argumente juridice pentru promovare a vieții private și a libertăților civile. A se vedea PCLOB, secțiunea 215 din Raport, p. 183-187.

([140]) 50 U.S.C. § 1803 (i)(2)(A). Conform informațiilor prezentate de ODNI, astfel de numiri au avut deja loc. A se vedea Reforma legată de activitățile de colectare de informații pe baza semnalelor electromagnetice, raportul intermediar de activitate pentru anul 2016.

([141]) 50 U.S.C. § 1803 (i)(2)(B).

(107) În ceea ce privește cele două autorizații legale pentru supraveghere în temeiul FISA care sunt cele mai importante pentru transferurile de date în temeiul Scutului de confidențialitate UE-SUA, supravegherea efectuată de FISC diferă.

(108) Pe de o parte, în temeiul secțiunii 501 din FISA ([142]), care permite colectarea de „elemente concrete (inclusiv cărți, înregistrări, acte, documente și alte elemente)", cererea către FISC trebuie să conțină o expunere a faptelor din care să reiasă că există motive întemeiate să se considere că elementele concrete căutate sunt relevante pentru o investigație autorizată (alta decât o evaluare a amenințărilor) efectuată pentru a obține informații operative străine care nu privesc un cetățean american sau pentru a proteja împotriva terorismului internațional sau a activităților clandestine de spionaj. De asemenea, cererea trebuie să cuprindă o enumerare a procedurilor de reducere la minimum adoptate de procurorul general pentru păstrarea și difuzarea informațiilor colectate. ([143])

(109) Pe de altă parte, în conformitate cu secțiunea 702 din FISA ([144]), FISC nu autorizează măsuri individuale de supraveghere; dimpotrivă, aceasta autorizează programe de supraveghere, (precum PRISM, UPSTREAM) pe baza unor certificări anuale întocmite de procurorul general și directorul Serviciului național de informații. Secțiunea 702 din FISA permite vizarea unor persoane despre care se consideră, din motive întemeiate, că se află în afara Statelor Unite, pentru a dobândi informații operative străine ([145]). Această direcționare este efectuată de NSA în două etape: în primul rând, analiștii NSA vor identifica persoanele care nu sunt cetățeni americani aflate în străinătate a căror supraveghere va conduce, pe baza evaluării analiștilor, la informațiile externe relevante specificate în certificare. În al doilea rând, odată ce persoanele individualizate au fost identificate și vizarea lor a fost aprobată printr-un amplu mecanism de revizuire în cadrul NSA ([146]), se „vizează" (și anume, se elaborează și se aplică) selectoare care identifică mijloacele de comunicare (precum adresele de poștă electronică) utilizate de țințe ([147]). Astfel cum s-a arătat mai sus, certificările care trebuie să fie aprobate de către FISC nu conțin informații despre persoanele fizice care urmează să fie vizate, ci, mai degrabă, prezintă categoriile de informații operative străine ([148]). Deși FISC nu evaluează – în temeiul unei suspiciuni rezonabile sau a oricărui alt criteriu – dacă persoanele sunt vizate în mod corespunzător pentru a dobândi informații operative străine ([149]), controlul său se extinde la condiția că „un scop important al achiziției de date este de a obține informații operative străine" ([150]). Într-adevăr, în temeiul secțiunii 702 din FISA, NSA poate colecta comunicațiile persoanelor care nu sunt cetățeni americani din afara SUA doar în cazul în care se poate considera în mod rezonabil că un anumit mijloc de comunicare este utilizat pentru a comunica informații operative străine (de exemplu, cele legate de terorismul internațional, proliferarea nucleară sau activități cibernetice ostile). Constatările în acest sens sunt supuse controlului judiciar ([151]). De asemenea, certificatele trebuie să prevadă proceduri de direcționare și de reducere la minimum ([152]). Procurorul general și directorul Serviciului național de informații verifică respectarea, iar agențiile

([142]) 50 U.S.C. § 1861
([143]) 50 U.S.C. § 1861.
([144]) 50 U.S.C. § 1881.
([145]) 50 U.S.C. § 1881a (a).
([146]) PCLOB, secțiunea 702 din Raport, p. 46.
([147]) 50 U.S.C. § 1881a (h).
([148]) 50 U.S.C. § 1881a (g). Potrivit PCLOB, aceste categorii au vizat în principal terorismul internațional și subiecte precum achiziționarea de arme de distrugere în masă. A se vedea PCLOB, secțiunea 702 din Raport, p. 25;
([149]) PCLOB, secțiunea 702 din Raport, p. 27.
([150]) 50 U.S.C. § 1881a.
([151]) „Libertate și securitate într-o lume în schimbare", raportul și recomandările Grupului de analiză al președintelui privind serviciile de informații și tehnologia comunicațiilor, 12 decembrie 2013, p. 152.
([152]) 50 U.S.C.1881a (i).

au obligația de a raporta orice incidente de neconformitate către FISC ([153]) (precum și Congresului și Comitetului pentru supravegherea serviciilor de informații al Președintelui), care, pe această bază, poate modifica autorizația ([154]).

(110) În plus, pentru a spori eficiența supravegherii de către FISC, administrația SUA s-a angajat să pună în aplicare o recomandare a PCLOB de a furniza către FISC documentarea deciziilor de direcționare în temeiul secțiunii 702, inclusiv un eșantion aleatoriu de lucrări, astfel încât să permită FISC să evalueze modul în care cerința privind scopul informațiilor externe este respectată în practică ([155]). În același timp, administrația SUA a acceptat și a luat măsuri pentru a revizui procedurile de direcționare a intervențiilor NSA în scopul de a documenta mai bine motivele colectării de informații externe pentru deciziile de direcționare ([156]).

Măsuri reparatorii individuale

(111) Persoanele vizate din UE au la dispoziție o serie de căi de atac în temeiul legislației SUA în cazul în care au îndoieli legate de eventualitatea ca datele lor cu caracter personal să fi fost prelucrate (colectate, accesate etc.) de elemente ale comunității serviciilor de informații americane și, în caz afirmativ, dacă au fost respectate limitările aplicabile din legislația SUA. Acestea se referă în principal la trei domenii: imixtiune în temeiul FISA; accesul intenționat, ilegal la date cu caracter personal de către funcționari guvernamentali; și accesul la informații în conformitate cu Legea privind accesul liber la informații (*Freedom of Information Act* – FOIA) ([157]).

(112) În primul rând, Legea privind supravegherea activităților străine de spionaj prevede o serie de căi de atac, care sunt disponibile, de asemenea, persoanelor care sunt cetățeni americani, pentru a contesta supravegherea electronică ilegală ([158]). Aceasta include posibilitatea ca persoanele fizice să introducă o acțiune civilă pentru despăgubiri bănești împotriva Statelor Unite, atunci când informațiile despre acestea au fost folosite sau divulgate în mod ilegal și intenționat (18 U.S.C. § 2712) ([159]); să dea în judecată oficialii guvernului SUA în calitatea lor personală („în conformitate cu litera legii") pentru despăgubiri bănești ([160]); și să conteste legalitatea supravegherii (și să încerce să suprime informațiile) în cazul în care guvernul SUA intenționează să utilizeze sau să divulge orice informații obținute sau derivate din activitatea de supraveghere electronică împotriva persoanei în cadrul unei proceduri judiciare sau administrative în Statele Unite ale Americii ([161]).

(113) În al doilea rând, guvernul SUA a transmis Comisiei o serie de căi suplimentare pe care persoanele vizate din UE le-ar putea utiliza pentru a introduce o acțiune împotriva funcționarilor guvernamentali pentru accesul ilegal la

([153]) Norma 13 litera (b) din Regulamentul de procedură al FISC impune autorităților publice să depună o notificare scrisă în fața instanței de îndată ce descoperă că orice competență sau aprobare acordată de către Curte a fost pusă în aplicare într-un mod care nu este conform cu competența sau aprobarea sau cu legislația aplicabilă. De asemenea, aceasta impune autorităților publice să notifice în scris cu privire la faptele și circumstanțele relevante pentru o astfel de neconformitate. De regulă, guvernul va introduce o notificare finală în temeiul normei 13(a) atunci când faptele sunt cunoscute și orice operațiune de colectare neautorizată a fost eliminată. A se vedea Scrisoarea Walton, p. 10.

([154]) 50 U.S.C. § 1881 (l). A se vedea, de asemenea, PCLOB, secțiunea 702 din Raport, pp. 66-76; NSA CLPO, Punerea în aplicare de către NSA a secțiunii 702 din Legea privind supravegherea activităților străine de spionaj, 16 aprilie 2014. Colectarea datelor cu caracter personal în scopuri de spionaj, conform secțiunii 702 din FISA face obiectul supravegherii interne și externe în cadrul puterii executive. Printre altele, supravegherea internă include programe de conformitate interne pentru a evalua și supraveghea respectarea procedurilor de direcționare și de reducere la minimum; raportarea incidentelor de neconformitate, atât pe plan intern, cât și extern la ODNI, Departamentul de Justiție, Congres și FISC; și revizuiri anuale trimise către aceleași organisme. În ceea ce privește controlul extern, acesta constă în principal din revizuirile în materie de direcționare și reducere la minimum efectuate de ODNI, Departamentul de Justiție și inspectori generali, care, la rândul lor, raportează Congresului și FISC, inclusiv cu privire la incidente de neconformitate. Incidentele semnificative legate de conformare trebuie raportate către FISC imediat, altele într-un raport trimestrial. A se vedea PCLOB, secțiunea 702 din Raport, p. 66-77.

([155]) PCLOB, Raportul de evaluare a recomandărilor, 29 ianuarie 2015, p. 20.

([156]) PCLOB, Raportul de evaluare a recomandărilor, 29 ianuarie 2015, p. 16.

([157]) În plus, secțiunea 10 din Legea privind procedurile aplicabile informațiilor clasificate prevede că, în cadrul oricărei proceduri penale în care Statele Unite trebuie să demonstreze că un material constituie informații clasificate (de exemplu, deoarece necesită protecție împotriva divulgării neautorizate, din motive de securitate națională), Statele Unite informează pârâtul cu privire la părțile din material pe care acesta se așteaptă în mod rezonabil să se bazeze pentru a stabili elementul de informații clasificate al infracțiunii.

([158]) A se vedea următoarele Declarații ale ODNI (anexa VI), p. 16.

([159]) 18 U.S.C. § 2712.

([160]) 50 U.S.C. § 1810.

([161]) 50 U.S.C. § 1806.

datelor cu caracter personal sau utilizarea acestora, inclusiv în scopul securității naționale [și anume, Legea privind fraudele și abuzurile informatice (Computer Fraud and Abuse Act ([162])); Legea privind confidențialitatea comunicațiilor electronice (Electronic Communications Privacy Act ([163])) și Legea privind dreptul la confidențialitate financiară (Right to Financial Privacy Act ([164]))]. Toate aceste căi de atac privesc anumite date, ținte și/sau tipuri de acces (de exemplu, accesul la distanță la un calculator prin intermediul internetului) și sunt disponibile în anumite condiții (de exemplu, comportament intenționat în afara calității oficiale, prejudiciul suferit) ([165]). O cale de atac mai generală este oferită prin Legea privind procedura administrativă (*Administrative Procedure Act*, 5 U.S.C. § 702), potrivit căruia „orice persoană care este victima unui abuz juridic cauzat de acțiunea agenției sau este afectată ori lezată într-un alt mod de acțiunea agenției" are dreptul de a solicita controlul jurisdicțional. Acest lucru include posibilitatea de a solicita Curții „să declare ilegale sau să anuleze acțiunea, constatările și concluziile agenției în legătură cu care s-a constatat că sunt […] arbitrare, capricioase, un abuz de putere de apreciere sau neconforme cu legea din orice alt motiv" ([166]).

(114) În sfârșit, Guvernul SUA a indicat FOIA ca mijloc pentru persoanele care nu sunt cetățeni americani de a solicita accesul la înregistrările existente ale agențiilor federale, inclusiv în cazul în care acestea conțin date cu caracter personal ale persoanei în cauză ([167]). Dat fiind caracterul său, FOIA nu oferă o modalitate de recurs individual împotriva ingerințelor privind datele cu caracter personal ca atare, chiar dacă aceasta ar putea, în principiu, să permită persoanelor să aibă acces la informații pertinente deținute de către agențiile naționale de informații. Chiar și în acest sens, posibilitățile sunt limitate, întrucât agențiile pot refuza accesul la informații care se încadrează în anumite excepții enumerate, inclusiv accesul la informații clasificate legate de securitatea națională și informații privind anchetele autorităților de aplicare a legii ([168]). Având în vedere acestea, utilizarea unor astfel de derogări de către agențiile naționale de informații pot fi atacate de persoanele care pot solicita examinări administrative și judiciare.

(115) Deși persoanele fizice, inclusiv persoanele vizate din UE, au o serie de modalități de recurs în cazul în care au făcut obiectul supravegherii (electronice) ilegale în scopuri legate de securitatea națională, este la fel de clar că cel puțin anumite temeiuri juridice care pot fi utilizate de autoritățile americane de informații (de exemplu, O.E. 12333) nu sunt acoperite. În plus, inclusiv în cazul în care există, în principiu, căi de atac pentru persoanele care nu sunt cetățeni ai SUA, de exemplu pentru supravegherea în temeiul FISA, direcțiile de acțiune disponibile sunt limitate ([169]), iar cererile prezentate de persoane (inclusiv cetățeni americani), vor fi declarate inadmisibile atunci când acestea nu pot arăta că au „calitate procesuală" ([170]), ceea ce limitează accesul la instanțele ordinare ([171]).

(116) Pentru a oferi o cale de atac suplimentară accesibilă pentru toate persoanele vizate din UE, Gvernul SUA a decis să creeze un nou mecanism de tip Ombudsman, după cum este prezentat în scrisoarea adresată de Secretarul de stat al SUA Comisiei, care figurează în anexa III la prezenta decizie. Acest mecanism se bazează pe desemnarea, în temeiul PPD-28, a unui coordonator principal (la nivel de subsecretar) în cadrul Departamentului de stat ca punct de contact unde administrațiile străine pot să își exprime preocuparea privind activitățile de colectare de informații electromagnetice din SUA, dar depășește în mod semnificativ acest concept inițial.

([162]) 18 U.S.C. § 1030.
([163]) 18 U.S.C. §§ 2701-2712.
([164]) 12 U.S.C. § 3417.
([165]) Declarațiile ODNI (anexa VI), p. 17.
([166]) 5 U.S.C. § 706(2)(A).
([167]) 5 U.S.C. § 552. Există legi similare la nivel național.
([168]) În acest caz, persoana respectivă va primi în mod normal numai un răspuns standard prin care agenția refuză să confirme sau să infirme existența unor înregistrări. A se vedea *ACLU v. CIA*, 710 F.3d 422 (D.C. Cir. 2014).
([169]) A se vedea Observațiile ODNI (anexa VI), p. 16. Conform explicațiilor oferite, acțiunile disponibile fie necesită existența unui prejudiciu (18 USC § 2712; 50 USC § 1810), fie o dovadă că guvernul intenționează să utilizeze sau să divulge informații obținute sau derivate din supravegherea electronică a persoanei în cauză împotriva acestei persoane în cadrul unei proceduri judiciare sau administrative în Statele Unite ale Americii (50 U.S.C. § 1806). Cu toate acestea, astfel cum Curtea a subliniat în repetate rânduri, pentru a stabili existența unei ingerințe în dreptul fundamental la viață privată, nu contează dacă persoana în cauză a suferit consecințe negative din cauza acestei ingerințe. A se vedea *Schrems*, punctul 89 cu trimiteri suplimentare.
([170]) Acest criteriu de admisibilitate rezultă din cerința „cazului sau controverselor" din Constituția SUA, articolul III.
([171]) A se vedea Clapper/Amnesty Int'l USA, 133 S.Ct. 1138, 1144 (2013), În ceea ce privește utilizarea NSL, Legea SUA privind libertatea [secțiunea 502 (f) -503] prevede că cerințele de confidențialitate trebuie să fie revizuite periodic și că destinatarii scrisorilor privind securitatea națională trebuie notificați în cazul în care faptele nu mai pot justifica o cerință de confidențialitate [a se vedea Declarații ODNI (anexa VI), p. 13]. Cu toate acestea, acest lucru nu garantează faptul că persoana vizată din UE va fi informată că a făcut obiectul unei anchete.

(117) În special, în conformitate cu angajamentele asumate de Guvernul SUA, mecanismul Ombudsmanului pentru Scutul de confidențialitate va asigura faptul că plângerile individuale sunt investigate în mod adecvat și că persoanele primesc o confirmare independentă a faptului că legislația SUA a fost respectată sau, în caz de încălcare a acestei legislații, că neconformitatea a fost remediată ([172]). Mecanismul include „Ombudsmanul pentru Scutul de confidențialitate", și anume subsecretarul și alt personal, precum și alte organisme de supraveghere care au competența de a controla diferitele elemente ale comunității serviciilor de informații, a căror cooperare va sta la baza examinării plângerilor de către Ombudsmanul pentru Scutul de confidențialitate. În special, în cazul în care o cerere adresată de o persoană se referă la compatibilitatea supravegherii cu legislația SUA, Ombudsmanul pentru Scutul de confidențialitate se va putea baza pe organismele de supraveghere independente cu competențe de investigare (precum inspectorii generali sau PCLOB). În fiecare caz, Secretarul de Stat asigură faptul că Ombudsmanul va dispune de mijloacele necesare pentru a se asigura că răspunsul său la cererile individuale se bazează pe toate informațiile necesare.

(118) Prin această „structură compozită", mecanismul Ombudsmanului garantează supravegherea independentă și posibilitatea unui recurs individual. În plus, cooperarea cu alte organisme de supraveghere asigură accesul la expertiza necesară. În sfârșit, deoarece Ombudsmanul pentru Scutul de confidențialitate are obligația de a confirma respectarea sau măsurile de remediere a oricărei neconformități, mecanismul reflectă angajamentul Guvernului SUA în ansamblul său de a trata și a soluționa plângerile persoanelor din UE.

(119) În primul rând, în mod diferit față de un simplu mecanism interguvernamental, Ombudsmanul pentru Scutul de confidențialitate va primi și va răspunde la plângeri individuale. Aceste plângeri pot fi adresate autorităților de supraveghere ale statelor membre care au competențe în ceea ce privește controlul serviciilor de securitate națională și/sau prelucrarea datelor cu caracter personal, care le vor înainta unui organism centralizat la nivelul UE care le va transmite Ombudsmanului pentru Scutul de confidențialitate ([173]). De acest lucru vor beneficia, de fapt, persoanele din UE, care pot apela la o autoritate națională, mai aproape de locul de reședință și în propria lor limbă. Sarcina acestei autorități va fi să sprijine persoana în adresarea unei cereri individuale Ombudsmanului pentru Scutul de confidențialitate care conține informațiile de bază și, prin urmare, care poate fi considerată „completă". Persoana nu trebuie să demonstreze că datele sale cu caracter personal au fost accesate de guvernul SUA prin activitățile de colectare de informații pe bază de semnale electromagnetice.

(120) În al doilea rând, Guvernul SUA se angajează să asigure faptul că, în exercitarea funcțiilor sale, Ombudsmanul pentru Scutul de confidențialitate se va putea baza pe cooperarea mecanismelor de supraveghere și de control al conformității existente în temeiul legislației americane. Aceasta va presupune uneori implicarea autorităților naționale de informații, în special în cazul unei cereri care trebuie interpretată ca fiind una de acces la documente în temeiul Legii privind libertatea de informare. În alte cazuri, în special în situația în care cererile se referă la compatibilitatea cu legislația SUA de supraveghere, la această cooperare vor lua parte organe independente de supraveghere (de exemplu, Inspectorii Generali) cu responsabilitatea și competența de a efectua o anchetă detaliată (în special în ceea ce privește accesul la toate documentele relevante și puterea de a solicita informații și de a culege declarații) și de a trata cazurile de neconformitate ([174]). De asemenea, Ombudsmanul pentru Scutul de confidențialitate va putea transmite chestiunile către PCLOB spre examinare ([175]). În cazul unul din aceste organisme de supraveghere a constatat o neconformitate, elementul vizat din cadrul comunității serviciilor de informații (de exemplu, o agenție de informații) va trebui să remedieze neconformitatea, întrucât doar acest lucru îi va permite Ombudsmanului să ofere persoanei un „răspuns pozitiv" (și anume, că neconformitatea a fost

([172]) În cazul în care reclamantul urmărește să obțină acces la documentele deținute de autoritățile publice din SUA, se aplică normele și procedurile prevăzute în Legea privind libertatea de informare. Printre acestea se numără posibilitatea de a introduce o acțiune în justiție (mai degrabă decât supravegherea independentă), în cazul în care cererea este respinsă, în temeiul condițiilor prevăzute în FOIA.

([173]) În conformitate cu mecanismul Ombudsmanului (anexa III), secțiunea 4 (f), Ombudsmanul pentru Scutul de confidențialitate va comunica direct cu organismul de tratare a plângerilor individuale, care, la rândul său, vor fi responsabil pentru comunicarea cu persoana care a depus cererea. În cazul în care comunicările directe fac parte din „procesele subiacente" care ar putea oferi ajutorul solicitat (de exemplu, o cerere de acces în temeiul FOIA, a se vedea secțiunea 5), aceste comunicări se vor face în conformitate cu procedurile aplicabile.

([174]) A se vedea mecanismul Ombudsmanului (anexa III), secțiunea 2(a). A se vedea considerentele 0-0.

([175]) A se vedea mecanismul Ombudsmanului (anexa III), secțiunea 2(c). Potrivit explicațiilor furnizate de guvernul american, PCLOB urmărește să revizuiască permanent politicile și procedurile, precum și punerea lor în aplicare, ale autorităților americane responsabile de combaterea terorismului pentru a stabili dacă acțiunile lor „protejează în mod adecvat viața privată și libertățile civile și sunt în conformitate cu legislația aplicabilă, reglementările și politicile privind viața privată și libertățile civile." De asemenea, PCLOB „va primi și examina rapoarte și alte informații de la responsabilii pentru protecția vieții private și a libertăților civile și, după caz, va face recomandări în privința activităților lor."

remediată) pe care Guvernul SUA s-a angajat să-l ofere. De asemenea, în cadrul cooperării, Ombudsmanul pentru Scutul de confidențialitate va fi informat asupra rezultatului anchetei; Ombudsmanul va dispune de mijloacele necesare pentru a se asigura primește toate informațiile necesare pentru a-și pregăti răspunsul.

(121) În sfârșit, Ombudsmanul pentru Scutul de confidențialitate va fi independent și, prin urmare, nu primește instrucțiuni de la comunitatea serviciilor de informații din SUA ([176]). Acest lucru este deosebit de important, având în vedere faptul că Ombudsmanul va trebui să „confirme" că: (i) plângerea a fost investigată în mod corespunzător; și că (ii) s-a respectat legislația SUA relevantă – inclusiv, mai ales, limitările și garanțiile prezentate în anexa VI – sau, în caz de neconformitate, că o astfel de încălcare a fost remediată. Pentru a fi în măsură să ofere această confirmare independentă, Ombudsmanul pentru Scutul de confidențialitate va trebui să primească informațiile necesare cu privire la investigație pentru a evalua exactitatea răspunsului oferit plângerii. În plus, Secretarul de Stat s-a angajat să se asigure că subsecretarul va îndeplini funcția de Ombudsman pentru Scutul de confidențialitate în mod obiectiv și în condiții de independență față de orice influențe neadecvate care riscă să afecteze răspunsul care urmează să fie oferit.

(122) În general, acest mecanism asigură faptul că plângerile individuale vor fi examinate și rezolvate cu atenție și că, cel puțin în domeniul supravegherii, la acest proces vor lua parte organisme de supraveghere independente care dispun de expertiza și de competențele de investigare necesare și un Ombudsman care va fi în măsură să își îndeplinească funcțiile în condiții de independență față de orice influențe neadecvate, îndeosebi politice. În plus, persoanele vor putea să depună plângeri fără să fie obligate să demonstreze sau doar să ofere indicii că au făcut obiectul supravegherii ([177]). Având în vedere aceste elemente, Comisia consideră că există garanții adecvate și eficiente împotriva abuzurilor.

(123) Pe baza elementelor prezentate mai sus, Comisia concluzionează că Statele Unite garantează protecția juridică efectivă împotriva imixtiunilor din partea serviciilor de informații, cu respectarea drepturilor fundamentale ale persoanelor ale căror date sunt transferate din Uniunea Europeană către Statele Unite ale Americii în temeiul Scutului de confidențialitate UE-SUA.

(124) În această privință, Comisia ia act de hotărârea pronunțată de Curtea de Justiție în cauza *Schrems*, conform căreia „o reglementare care nu prevede nicio posibilitate pentru justițiabil de a exercita căi legale pentru a avea acces la date cu caracter personal care îl privesc sau pentru a obține rectificarea sau ștergerea unor astfel de date nu respectă nici substanța dreptului fundamental la o protecție jurisdicțională efectivă, astfel cum este consacrat la articolul 47 din cartă" ([178]). Evaluarea Comisiei a confirmat faptul că astfel de căi legale sunt prevăzute în Statele Unite, inclusiv prin intermediul mecanismului Ombudsmanului. Mecanismul Ombudsmanului prevede supravegherea independentă cu competențe de investigare. În cadrul monitorizării continue de către Comisie a Scutului de confidențialitate, inclusiv prin examinarea anuală comună, la care va lua parte și Ombudsmanul, eficacitatea acestui mecanism va fi reevaluată.

3.2. *Accesul și utilizarea de către autoritățile publice din SUA în scopul aplicării legii și în scopuri de interes public*

(125) În ceea ce privește imixtiunile privind datele cu caracter personal transferate în temeiul Scutului de confidențialitate UE-SUA în scopul aplicării legii, guvernul american (prin intermediul Departamentului de Justiție) a oferit asigurări privind limitările și garanțiile aplicabile în evaluarea Comisiei demonstrează un nivel de protecție adecvat.

([176]) A se vedea cauza *Roman Zakharov/Russia*, hotărârea din 4 decembrie 2015 (Marea Cameră), cererea nr. 47143/06, punctul 275 („cu toate că, în principiu, este de dorit să se încredințeze controlul unui judecător, supravegherea de către organisme care nu sunt de natură judiciară poate fi considerată compatibil cu convenția, cu condiția ca organismul de supraveghere să fie independent de autoritățile care efectuează supravegherea și să fie învestit cu competențe suficiente și eficiente de supraveghere").

([177]) A se vedea Kennedy/Regatul Unit, hotărârea din 18 mai 2010, cererea nr. 26839/05, punctul 167.

([178]) *Schrems*, punctul 95. Astfel cum rezultă din cuprinsul punctelor 91 și 96 din hotărâre, punctul 95 se referă la nivelul de protecție garantat în ordinea juridică a Uniunii, față de care nivelul de protecție din țara terță trebuie să fie „în esență echivalent". În conformitate cu punctele 73 și 74 din hotărâre, aceasta nu impune ca nivelul de protecție sau mijloacele utilizate de țara terță să fie identice, chiar dacă mijloacele care urmează a fi utilizate trebuie să se dovedească, în practică, eficace.

(126) Conform acestor informații, în conformitate cu cel de al patrulea amendament al Constituției Statelor Unite ale Americii ([179]), perchezițiile și punerile sub sechestru de către autoritățile de aplicare a legii necesită în principal ([180]) un mandat judecătoresc emis la prezentarea unei „suspiciuni rezonabile". În câteva cazuri excepționale și stabilite în mod specific în care cerința mandatului nu se aplică ([181]), aplicarea legii este supusă unui test privind „caracterul rezonabil" ([182]). Faptul dacă o percheziție sau un sechestru sunt rezonabile este „determinat prin evaluarea, pe de o parte, a măsurii în care aceste proceduri încalcă viața privată a persoanei și, pe de altă parte, măsura în care aceste proceduri necesare pentru promovarea intereselor publice legitime" ([183]). În termeni generali, al patrulea amendament garantează viața privată, demnitatea și protejează împotriva actelor arbitrare și invazive ale funcționarilor guvernamentali ([184]). Aceste concepte reflectă ideea necesității și proporționalității în legislația Uniunii. Odată ce autoritățile de aplicare a legii nu mai au nevoie de articolele confiscate cu titlu de probe, acestea trebuie returnate ([185]).

(127) Deși cel de-al patrulea amendament nu se aplică persoanelor care nu sunt cetățeni ai SUA și nu sunt rezidenți în SUA, acestea din urmă beneficiază totuși indirect de protecția oferită de acest amendament, dat fiind că datele cu caracter personal sunt deținute de societăți din SUA, ceea ce înseamnă că autoritățile de aplicare a legii trebuie să solicite, în orice caz, autorizarea judiciară (sau, cel puțin, să respecte cerința privind caracterul rezonabil) ([186]). Alte măsuri de protecție speciale sunt prevăzute de autoritățile de reglementare, precum și de orientările Departamentului de Justiție care limitează accesul autorităților de aplicare a legii la date din motive de necesitate și proporționalitate (de exemplu, prin solicitarea ca FBI să utilizeze cele mai puțin invazive metode de anchetă posibile, luând în considerare impactul asupra vieții private și a libertăților civile) ([187]). În conformitate cu observațiile prezentate de guvernul american, se aplică niveluri de protecție similare sau mai ridicate pentru anchetele în scopul aplicării legii la nivel statal (cu privire la investigațiile desfășurate în temeiul legilor în vigoare în statul în cauză) ([188]).

(128) Deși o autorizație judiciară prealabilă emisă de o instanță judecătorească sau de marele juriu (o componentă investigativă a instanței convocate de către un judecător sau magistrat) nu este necesară în toate cazurile ([189]), citațiile administrative sunt limitate la cazuri specifice și vor fi supuse unui control judiciar independent cel puțin în cazul în care guvernul urmărește executarea în instanță ([190]).

([179]) În conformitate cu cel de al patrulea amendament la Constituția Statelor Unite, „[n]u se va încălca dreptul cetățenilor de a fi siguri în ceea ce privește persoanele, locuințele, documentele și efectele, împotriva perchezițiilor și sechestrelor nerezonabile, și nu se vor emite mandate fără un motiv întemeiat, susținut de jurământ sau declarație solemnă, care include în special descrierea spațiului care urmează să fie percheziționat, persoanele care urmează să fie arestate sau obiectele care urmează să fie confiscate". Doar judecătorii (magistrații) pot emite astfel de mandate. Mandatele federale pentru copierea informațiilor stocate în format electronic sunt reglementate și prin norma 41 din Codului federal de procedură penală.

([180]) În repetate rânduri, Curtea Supremă a menționat perchezițiile efectuate fără mandat ca fiind „excepționale". A se vedea, de exemplu *Johnson/United States*, 333 U.S. 10, 14 (1948); *McDonald/United States*, 335 U.S. 451, 453 (1948); *Camara/Municipal Court*, 387 U.S. 523, 528-29 (1967); *G.M. Leasing Corp/United States*, 429 U.S. 338, 352-53, 355 (1977). În mod similar, Curtea Supremă subliniază în mod regulat că „regula constituțională cea mai elementară în acest domeniu este că perchezițiile desfășurate în afara procedurilor judiciare, fără aprobare prealabilă de către judecător sau magistrat, sunt, prin ele însele, nerezonabile în conformitate cu cel de-al patrulea amendament, sub rezerva câtorva excepții special prevăzute și bine delimitate." A se vedea, de exemplu *Coolidge/New Hampshire*, 403 U.S. 443, 454-55 (1971); *G.M. Leasing Corp/United States*, 429 U.S. 338, 352-53, 358 (1977).

([181]) *City of Ontario, Cal/Quon*, 130 S. Ct. 2619, 2630 (2010).

([182]) PCLOB, secțiunea 215 din Raport, p. 107, care face referire la Maryland/King, 133 S. Ct. 1958, 1970 (2013).

([183]) PCLOB, secțiunea 215 din Raport, p. 107, care face referire la Samson/California, 547 U.S. 843, 848 (2006).

([184]) *City of Ontario, Cal/Quon*, 130 S. Ct. 2619, 2630 (2010), 2627.

([185]) A se vedea, de ex. *United Sates/Wilson*, 540 F.2d 1100 (D.C. Cir. 1976).

([186]) A se vedea cauza *Roman Zakharov/Russia*, hotărârea din 4 decembrie 2015 (Marea Cameră), cererea nr. 47143/06, punctul 269, potrivit căreia „obligația de a prezenta o autorizare a interceptării comunicațiilor către prestatorul de servicii înainte de a obține accesul la comunicațiile unei persoane reprezintă una dintre măsurile importante de protecție împotriva abuzurilor comise de către autoritățile de aplicare a legii, asigurând faptul că se obține o autorizație adecvată în toate cazurile de interceptare."

([187]) Declarațiile Departamentului de Justiție (DOJ) (anexa VII), p. 4, cu trimiteri suplimentare.

([188]) Declarațiile Departamentului de Justiție (DOJ) (anexa VII), n. 2.

([189]) În conformitate cu informațiile primite de către Comisie și lăsând la o parte anumite domenii care nu sunt relevante pentru transferurile de date în temeiul Scutului de confidențialitate UE-SUA (de exemplu, investigațiile privind fraudele în domeniul sănătății, abuzurile asupra copiilor sau substanțe reglementate) se referă, în special, la anumite autorități în temeiul Legii privind confidențialitatea comunicațiilor electronice (*Electronic Communications Privacy Act* – ECPA), și anume cererile de informații de bază referitoare la abonați, sesiuni de conectare și facturare [18 U.S.C. § 2703 (c) (1), (2)], de ex. adresa, tipul/durata serviciului și pentru conținutul e-mailurilor mai vechi de 180 zile [18 U.S.C § 2703 (b)]. Însă, în al doilea caz, persoana în cauză trebuie să fie notificată și, astfel, are posibilitatea de a contesta cererea în instanță. A se vedea, de asemenea, rezumatul din documentul Ministerului Justiției intitulat *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Ch. 3: The Stored Communications Act, pp. 115138*.

([190]) Potrivit declarațiilor guvernului american, destinatarii unor citații administrative le pot contesta în instanță, pe motiv că acestea nu sunt rezonabile, și anume sunt excesiv de cuprinzătoare, abuzive sau împovărătoare. A se vedea Departamentul de Justiție (DOJ) (anexa VII), p. 2.

(129) Același lucru este valabil, de asemenea, pentru utilizarea unor citații administrative în scopuri de interes public. În plus, în conformitate cu observațiile din partea guvernului american, se aplică restricții esențiale similare în sensul că agențiile pot solicita accesul numai la datele care sunt relevante pentru domeniile care intră în sfera lor de competență și trebuie să respecte criteriul caracterului rezonabil.

(130) În plus, legislația SUA pune la dispoziția persoanelor fizice o serie de căi de atac judiciare împotriva unei autorități publice sau a unuia dintre funcționarii acesteia, în cazul în care aceste autorități prelucrează date cu caracter personal. Aceste căi, printre care figurează în special Legea privind procedura administrativă (APA), Legea privind accesul liber la informații (FOIA) și Legea privind confidențialitatea comunicațiilor electronice (ECPA) stau la dispoziția tuturor persoanelor, indiferent de cetățenia lor, sub rezerva condițiilor aplicabile.

(131) În general, în temeiul dispozițiilor referitoare la controlul jurisdicțional din Legea privind procedura administrativă (*Administrative Procedure Act*) ([191]), „orice persoană care este victima unui abuz juridic cauzat de acțiunea agenției sau este afectată ori lezată într-un alt mod de acțiunea agenției" are dreptul de a solicita controlul jurisdicțional ([192]). Acest lucru include posibilitatea de a solicita Curții „să declare ilegale sau să anuleze acțiunea, constatările și concluziile agenției în legătură cu care s-a constatat că sunt […] arbitrare, capricioase, un abuz de putere de apreciere sau neconforme cu legea din orice alt motiv" ([193]).

(132) Mai precis, titlul II din Legea privind confidențialitatea comunicațiilor electronice (ECPA) ([194]) prevede un sistem de drepturi legale în materie de viață privată și, prin urmare, reglementează accesul autorităților de aplicare a legii la conținutul comunicațiilor telefonice, orale sau electronice stocate de terți furnizori de servicii ([195]). Acesta penalizează accesul ilegal (și anume neautorizat de o instanță, dar, altfel, permis) la aceste comunicații și permite persoanelor afectate să intenteze o acțiune civilă într-o instanță federală americană pentru a solicita daune și interese, inclusiv punitive, precum și o reparație de tip *equity* sau o decizie declaratorie împotriva unui funcționar guvernamental care a săvârșit astfel de acte ilicite sau împotriva Statelor Unite ale Americii.

(133) De asemenea, în temeiul Legii privind accesul liber la informații (FOIA, 5 U.S.C. § 552), orice persoană are dreptul de a obține acces la înregistrările agențiilor federale și, la epuizarea căilor de atac administrative, de a cere executarea acestui drept în instanță, cu excepția cazului în care aceste înregistrări sunt protejate împotriva divulgării publice de către o derogare specială sau de o excepție de la aplicarea legii ([196]).

([191]) 5 U.S.C. § 702.

([192]) În general, doar acțiunea „finală" a agenției, mai degrabă decât „acțiunea preliminară, procedurală sau intermediară" a agenției, face obiectul unui control jurisdicțional. A se vedea 5 U.S.C. § 704.

([193]) 5 U.S.C. § 706(2)(A).

([194]) 18 U.S.C. §§ 2701-2712.

([195]) ECPA protejează comunicațiile deținute de două categorii distincte de furnizori de servicii de rețea, și anume furnizorii de: (i) servicii de comunicații electronice, de exemplu telefonie sau e-mail; (ii) servicii informatice la distanță, cum ar fi serviciile informatice de stocare sau de prelucrare.

([196]) Aceste excluderi sunt totuși încadrate. De exemplu, în conformitate cu punctul 5 U.S.C. § 552 (b) (7), drepturile prevăzute de FOIA sunt excluse în cazul „înregistrărilor sau informațiilor culese în scopul aplicării legii, însă numai în măsura în care prezentarea unor astfel de înregistrări sau informații referitoare la aplicarea legii: (A) ar risca în mod rezonabil să interfereze cu procedurile de executare; (B) ar priva o persoană de dreptul la un proces echitabil sau la o judecată imparțială; (C) ar putea constitui în mod rezonabil o încălcare nejustificată a vieții private; (D) ar putea în mod rezonabil să ducă la divulgarea identității unei surse confidențiale, inclusiv o agenție sau autoritate statală, locală sau străină sau orice instituție privată care furnizează informații în mod confidențial și, în cazul unei înregistrări sau al unor informații culese de autoritatea de aplicare a legii penale în cursul unei anchete penale sau de către o agenție care efectuează o anchetă de securitate națională, a informațiilor furnizate de o sursă confidențială, (E) ar dezvălui tehnici și proceduri referitoare la anchete sau urmăriri penale sau ar divulga orientările referitoare la anchete sau urmăriri penale în materie de aplicare a legii, în cazul în care o astfel de divulgare ar putea conduce în mod rezonabil la riscul eludării legii; sau (F) s-ar putea prevede în mod rezonabil că pune în pericol viața sau siguranța fizică a oricărei persoane. De asemenea, [o]ri de câte ori este prezentată o cerere care implică accesul la înregistrări [a căror prezentare ar putea duce în mod rezonabil la interferențe cu procedurile de aplicare a legii] și: (A) ancheta sau procedura implică o posibilă încălcare a dreptului penal; și (B), există motive să se creadă că: (i) persoana care face obiectul investigației sau al procedurii nu are cunoștință de desfășurarea acesteia; și (ii) divulgarea existenței înregistrărilor ar putea conduce în mod rezonabil la interferențe cu procedura de executare, Agenția poate, numai atât timp cât această împrejurare continuă, să trateze documentele ca nefăcând obiectul cerințelor prezentei secțiuni." [5 U.S.C. § 552 (c)(1)].

(134) În plus, mai multe alte statute acordă persoanelor fizice dreptul de a introduce acțiuni împotriva unei autorități sau a unui funcționar public din SUA cu privire la prelucrarea datelor lor cu caracter personal, precum *Wiretap Act* ([197]), *Computer Fraud and Abuse Act* ([198]), *Federal Torts Claim Act* ([199]), *Right to Financial Privacy Act* ([200]) și *Fair Credit Reporting Act* ([201])

(135) Prin urmare, Comisia concluzionează că există norme în vigoare în Statele Unite concepute să limiteze orice ingerință, în scopuri de aplicare a legii ([202]) sau în alte scopuri de interes public, în respectarea drepturilor fundamentale ale persoanelor ale căror date cu caracter personal sunt transferate din UE către Statele Unite în temeiul Scutului de confidențialitate UE-SUA la ceea ce este strict necesar pentru atingerea obiectivului legitim în cauză și să asigure protecție juridică împotriva unor astfel de intervenții.

4. UN NIVEL ADECVAT DE PROTECȚIE ÎN TEMEIUL SCUTULUI DE CONFIDENȚIALITATE UE-SUA

(136) Având în vedere aceste constatări, Comisia consideră că Statele Unite garantează un nivel adecvat de protecție a datelor cu caracter personal transferate din Uniune unor organizații autocertificate din Statele Unite în temeiul Scutului de confidențialitate UE-SUA.

(137) În special, Comisia consideră că principiile privind protecția vieții private publicate de Departamentul Comerțului al SUA, în ansamblul lor, asigură un nivel de protecție a datelor cu caracter personal care este, în esență, echivalent cu cel garantat de principiile de bază prevăzute în Directiva 95/46/CE.

(138) În plus, aplicarea efectivă a principiilor este garantată de obligații privind transparența și gestionarea Scutului de confidențialitate de către Departamentul Comerțului.

(139) De asemenea, Comisia consideră că, luate în ansamblu, supravegherea și mecanismele de recurs prevăzute de Scutul de confidențialitate permit identificarea și pedepsirea în practică a încălcărilor principiilor private de către organizațiile care aderă la Scutul de confidențialitate și oferă căi de atac persoanei vizate pentru a avea acces la datele cu caracter personal care o privesc și, în cele din urmă, pentru a obține rectificarea sau ștergerea datelor respective.

(140) În cele din urmă, pe baza informațiilor disponibile cu privire la ordinea juridică americană, inclusiv declarațiile și angajamentele din partea guvernului american, Comisia consideră că orice ingerință a autorităților publice americane în drepturile fundamentale ale persoanelor ale căror date sunt transferate din Uniunea Europeană către Statele Unite ale Americii în temeiul Scutului de confidențialitate pentru securitatea națională, aplicarea legii sau alte scopuri de interes public și, prin urmare, restricțiile rezultate impuse organizațiilor autocertificate în ceea ce privește aderarea la principiile privind protecția vieții private, vor fi limitate la ceea ce este strict necesar pentru atingerea obiectivului legitim în cauză și că există o protecție juridică efectivă împotriva unei astfel de ingerințe.

([197]) 18 U.S.C. §§ 2510 et seq. În temeiul Legii privind interceptarea convorbirilor telefonice (Wiretap Act – 18 U.S.C. § 2520) o persoană ale cărei comunicații telefonice, orale sau electronice sunt interceptate, divulgate sau utilizate în mod intenționat poate intenta o acțiune civilă pe motive de încălcare a acestei legi, inclusiv, în anumite circumstanțe, împotriva unei funcționar guvernamental sau a Statelor Unite ale Americii. Pentru colectarea de informații privind adresarea și a altor informații care nu sunt legate de conținut (de exemplu, adresa IP, emailurile trimise/primite), a se vedea, de asemenea, secțiunea consacrată dispozitivelor de interceptare a convorbirilor (pen registers) și de capturare și trasabilitate (trap and traces) de la titlul 18 (18 U.S.C. §§ 3121-3127 și, pentru acțiunile civile, § 2707)..

([198]) 18 U.S.C. § 1030. În conformitate cu Legea privind fraudele și abuzurile informatice, o persoană poate introduce o acțiune în justiție împotriva oricărei persoane în ceea ce privește accesul neautorizat intenționat (sau depășirea accesului autorizat) pentru obținerea de informații de la o instituție financiară, un sistem informatic al Guvernul Statelor Unite sau un alt computer, inclusiv, în anumite circumstanțe, împotriva unui funcționar.

([199]) 28 U.S.C. §§ 2671 et seq. În temeiul Legii federale privind acțiunile în răspundere civilă (Federal Tort Claims Act), o persoană poate introduce o acțiune, în anumite condiții, împotriva Statelor Unite ale Americii cu privire la „neglijența sau acțiunea greșită ori omisiunea oricărui angajat al guvernului care a acționat în domeniul de aplicare al mandatului sau al contractului său de muncă."

([200]) 12 U.S.C. § § 3401 și urm.). În conformitate cu Legea privind dreptul la confidențialitate financiară (*Right to Financial Privacy Act*), o persoană poate introduce o acțiune în justiție, în anumite condiții, împotriva Statelor Unite ale Americii cu privire la obținerea sau divulgarea, prin încălcarea legii, a evidențelor financiare protejate. Accesul guvernului la date financiare protejate este, în general, interzis, cu excepția cazului în care guvernul adresează cererea sub rezerva unei citații sau a unui mandat de percheziție sau, sub rezerva limitărilor, printr-o cerere oficială scrisă, cu condiția ca persoana ale cărei informații sunt solicitate să primească o notificare cu privire la această solicitare.

([201]) 15 U.S.C. §§ 1681-1681x. În temeiul Legii privind imparțialitatea rapoartelor privind solvabilitatea creditorilor (Fair Credit Reporting Act), o persoană poate introduce o acțiune împotriva oricărei persoane care nu respectă cerințele (în special necesitatea unei autorizații legale) în ceea ce privește colectarea, difuzarea și utilizarea rapoartelor privind creditul de consum sau, în anumite condiții, împotriva unei agenții guvernamentale.

([202]) Curtea de Justiție a recunoscut faptul că securitatea națională constituie un obiectiv legitim de politică. A se vedea cauzele conexate C-293/12 și C-594/12, *Digital Rights Ireland și alții*, EU:C:2014:238, punctul 42; A se vedea, de asemenea, articolul 8 alineatul (2) din CEDO și hotărârea pronunțată de CEDO în cauza *Weber și Saravia/Germania*, cererea nr. 54934/00, punctul 104.

(141) Comisia concluzionează că aceasta îndeplinește standardele prevăzute la articolul 25 din Directiva 95/46/CE, interpretată având în vedere Carta drepturilor fundamentale a Uniunii Europene, astfel cum a explicat Curtea de Justiție, în special în hotărârea Schrems.

5. ACȚIUNEA AUTORITĂȚILOR PENTRU PROTECȚIA DATELOR ȘI INFORMAȚIILE TRANSMISE COMISIEI

(142) În hotărârea Schrems, Curtea de Justiție a clarificat faptul că Comisia nu are competența de a limita competențele autorităților pentru protecția datelor care rezultă din articolul 28 din Directiva 95/46/CE (inclusiv competența de a suspenda transferurile de date), în cazul în care o persoană, prin introducerea unei cereri în temeiul dispoziției menționate, pune sub semnul întrebării compatibilitatea cu o decizie privind caracterul adecvat al nivelului de protecție a dreptului fundamental la viață privată și la protecția datelor ([203]).

(143) Pentru a monitoriza în mod eficient funcționarea Scutului de confidențialitate, Comisia ar trebui să fie informată de către statele membre în legătură cu acțiunile relevante întreprinse de către autoritățile pentru protecția datelor.

(144) Curtea de Justiție consideră că, în conformitate cu articolul 25 alineatul (6) al doilea paragraf din Directiva 95/46/CE, statele membre și organele acestora trebuie să ia măsurile necesare pentru a se conforma actelor instituțiilor Uniunii, acestea din urmă beneficiind în principiu de o prezumție de validitate și producând, așadar, efecte juridice atât timp cât nu au fost revocate, anulate în cadrul unei acțiuni în anulare sau declarate ca fiind lipsite de validitate în urma unei hotărâri preliminare sau a unei excepții de nelegalitate. În consecință, o decizie a Comisiei privind caracterul adecvat al nivelului de protecție, adoptată în temeiul articolului 25 alineatul (6) din Directiva 95/46/CE este obligatorie pentru toate organele statelor membre cărora li se adresează, inclusiv autoritățile de supraveghere independente ale acestora ([204]). În cazul în care o astfel de autoritate a primit o plângere care pune sub semnul întrebării conformitatea unei decizii a Comisiei privind caracterul adecvat al nivelului de protecție a dreptului fundamental la viață privată și la protecția datelor și consideră că obiecțiile invocate sunt întemeiate, legislația națională trebuie să prevadă o cale de atac pentru a prezenta obiecțiile respective în fața unei instanțe naționale, care, în caz de îndoieli, trebuie să suspende procedurile și să înainteze o cerere pentru o hotărâre preliminară a Curții de Justiție ([205]).

6. REVIZUIREA PERIODICĂ A CONSTATĂRII REFERITOARE LA CARACTERUL ADECVAT

(145) Având în vedere faptul că nivelul de protecție conferit de ordinea juridică americană poate suferi modificări, Comisia, în urma adoptării prezentei decizii, va verifica periodic dacă aceste constatări referitoare la caracterul adecvat al nivelului de protecție asigurat de Statele Unite în temeiul Scutului de confidențialitate UE-SUA este în continuare justificată din punct de vedere factual și juridic. O astfel de verificare este solicitată, în orice caz, atunci când Comisia obține orice informații care ridică o îndoială justificată în această privință ([206]).

(146) Prin urmare, Comisia va continua să monitorizeze cadrul general pentru transferul de date cu caracter personal creat de Scutul de confidențialitate UE-SUA, precum și respectarea de către autoritățile americane a declarațiilor și angajamentelor cuprinse în documentele anexate la prezenta decizie. Pentru a facilita acest proces, SUA s-a angajat să informeze Comisia cu privire la evoluțiile semnificative care au loc în legislația SUA în cazul în care sunt relevante pentru Scutul de confidențialitate în domeniul protecției datelor și al limitărilor și garanțiilor aplicabile accesului la date cu caracter personal de către autoritățile publice. În plus, prezenta decizie va face obiectul unei revizuiri comune anuale, care va cuprinde toate aspectele legate de funcționarea Scutului de confidențialitate, inclusiv punerea în aplicare a legii securității naționale și excepțiile de la principiile. În plus, deoarece constatarea privind caracterul adecvat poate fi, de asemenea, influențată de evoluțiile juridice din dreptul Uniunii, Comisia va evalua nivelul de protecție oferit de Scutul de confidențialitate după intrarea în vigoare a Regulamentului general privind protecția datelor.

(147) Pentru a efectua revizuirea comună anuală menționată la anexele I, II și VI, Comisia va participa la reuniuni cu Departamentul Comerțului și FTC, însoțite, dacă este cazul, de alte departamente și agenții implicate în punerea în aplicare a regimurilor Scutului de confidențialitate, precum și, pentru chestiuni care țin de securitatea națională, de reprezentanți ai ODNI, alte elemente ale comunității serviciilor de informații și Ombudsman. Participarea la această reuniune este deschisă reprezentanților autorităților UE pentru protecția datelor și ai Grupului de lucru „articolul 29”.

([203]) Schrems, punctele 40 și urm., 101-103.
([204]) *Schrems*, punctele 51, 52 și 62.
([205]) *Schrems*, punctul 65.
([206]) *Schrems*, punctul 76.

(148) În cadrul revizuirii comune anuale, Comisia va solicita ca Departamentul Comerțului să ofere informații detaliate cu privire la toate aspectele relevante legate de funcționarea Scutului de confidențialitate UE-SUA, inclusiv sesizări primite de Departamentul Comerțului de la autoritățile pentru protecția datelor și rezultatele evaluărilor de conformitate ex officio. De asemenea, Comisia va solicita explicații referitoare la orice întrebări sau probleme referitoare la Scutul de confidențialitate UESUA și funcționarea sa care rezultă din orice informații disponibile, inclusiv rapoartele de transparență permise în temeiul Legii SUA privind libertatea, rapoartele publice elaborate de către serviciile naționale de informații, autoritățile pentru protecția datelor, grupuri pentru promovarea vieții private, rapoarte din mass-media sau din orice altă sursă posibilă. În plus, pentru a facilita sarcina Comisiei în această privință, statele membre ar trebui să informeze Comisia în legătură cu cazurile în care acțiunile întreprinse de organismele însărcinate cu asigurarea respectării principiilor privind protecția vieții private în Statele Unite nu reușesc să asigure respectarea obligațiilor și în legătură cu orice indicii că acțiunile autorităților publice americane responsabile de securitatea națională sau de prevenirea, identificarea, investigarea, depistarea sau urmărirea penală a infracțiunilor nu asigură nivelul de protecție necesar.

(149) Pe baza revizuirii comune anuale, Comisia va pregăti un raport care va fi prezentat Parlamentului European și Consiliului.

7. SUSPENDAREA DECIZIEI PRIVIND CARACTERUL ADECVAT

(150) În cazul în care, pe baza controalelor sau a oricăror alte informații disponibile, Comisia a ajuns la concluzia că nivelul de protecție oferit de Scutul de confidențialitate nu mai poate fi considerat ca fiind, în esență, echivalent cu cel din Uniune sau în cazul în care există indicii clare că respectarea efectivă a principiilor în Statele Unite este posibil să nu mai fie garantată sau că acțiunile autorităților publice americane responsabile de securitatea națională sau de prevenirea, identificarea, investigarea, depistarea sau urmărirea penală a infracțiunilor nu asigură nivelul necesar de protecție, aceasta informează Departamentul Comerțului și solicită luarea de măsuri corespunzătoare pentru a soluționa rapid eventualele neconformități cu principiile, într-o perioadă de timp rezonabilă, specificată. În cazul în care, după expirarea termenului prevăzut, autoritățile americane nu au demonstrat în mod satisfăcător că Scutul de confidențialitate UE-SUA continuă să garanteze respectarea efectivă și un nivel adecvat de protecție, Comisia va iniția procedura care conduce la suspendarea parțială ori totală sau abrogarea acestei decizii ([207]). În caz contrar, Comisia poate propune modificarea prezentei decizii, de exemplu prin limitarea domeniului de aplicare a constatării referitoare la caracterul adecvat numai pentru transferurile de date sub rezerva unor condiții suplimentare.

(151) În special, Comisia va iniția procedura de suspendare sau de abrogare în cazul în care:

(a) există indicii că autoritățile americane nu respectă declarațiile și angajamentele cuprinse în documentele anexate la prezenta decizie, inclusiv în ceea ce privește condițiile și limitările pentru accesul de către autoritățile publice americane pentru aplicarea legii, securitatea națională și alte scopuri de interes public la date cu caracter personal transferate în temeiul Scutului de confidențialitate;

(b) plângerile persoanelor vizate din UE nu au fost abordate în mod eficient; în acest sens, Comisia va lua în considerare toate circumstanțele care au un impact asupra posibilității persoanelor vizate de a-și exercita drepturile, inclusiv, în special, angajamentul voluntar al companiilor americane autocertificate de a coopera cu autoritățile pentru protecția datelor și de a urma recomandările acestora; sau

(c) Ombudsmanul pentru Scutul de confidențialitate nu furnizează în timp util răspunsuri adecvate la cererile formulate de persoanele vizate din UE.

(152) Comisia va examina, de asemenea, posibilitatea de a iniția procedura de modificare, de suspendare sau de abrogare a prezentei decizii dacă, în contextul revizuirii comune anuale a funcționării Scutului de confidențialitate UE-SUA sau altfel, Departamentul Comerțului sau alte departamente ori agenții implicate în punerea în aplicare a Scutului de confidențialitate sau, pentru aspectele legate de securitatea națională, reprezentanții comunității serviciilor de informații din SUA sau Ombudsmanul nu furnizează informațiile sau clarificările necesare pentru evaluarea conformității cu principiile privind protecția vieții private, eficacitatea procedurilor de tratare

([207]) Începând cu data aplicării Regulamentului general privind protecția datelor, Comisia va face uz de prerogativele sale pentru a adopta, din motive imperioase de urgență justificate corespunzător, un act de punere în aplicare a suspendării prezentei decizii care se aplică imediat, fără prezentarea sa prealabilă comitetului de comitologie relevant și rămâne în vigoare pentru o perioadă care nu depășește șase luni.

a plângerilor sau orice scădere a nivelului necesar de protecție ca urmare a acțiunilor întreprinse de serviciile naționale de informații din SUA, în special ca urmare a colectării și/sau accesului la datele cu caracter personal care nu se limitează la ceea ce este strict necesar și proporțional. În acest sens, Comisia va lua în considerare măsura în care informațiile relevante pot fi obținute din alte surse, inclusiv prin rapoarte ale societăților de la companii americane autocertificate, posibilitate prevăzută de Legea SUA privind libertatea.

(153) Grupul de lucru pentru protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal instituit în temeiul articolului 29 din Directiva 95/46/CE și-a publicat avizul cu privire la nivelul de protecție oferit de Scutul de confidențialitate UE-SUA ([208]), iar acest aviz a fost luat în considerare la pregătirea prezentei decizii.

(154) Parlamentul European a adoptat o rezoluție referitoare la fluxurile de date transatlantice ([209]).

(155) Măsurile prevăzute de prezenta decizie sunt conforme cu avizul comitetului instituit în temeiul articolului 31 alineatul (1) din Directiva 95/46/CE,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

(1) În sensul articolului 25 alineatul (2) din Directiva 95/46/CE, Statele Unite garantează un nivel adecvat de protecție a datelor cu caracter personal transferate din Uniune către organizații din Statele Unite în temeiul Scutului de confidențialitate UE-SUA.

(2) Scutul de confidențialitate UE-SUA este constituit din principiile publicate de Departamentul Comerțului al SUA la 7 iulie 2016, prezentate în anexa II, precum și din declarațiile și angajamentele oficiale cuprinse în documentele enumerate în anexele I și IIIVII.

(3) În sensul alineatului (1), datele cu caracter personal sunt transferate în temeiul Scutului de confidențialitate UE-SUA în cazul în care acestea sunt transferate dinspre Uniune către organizații din Statele Unite ale Americii care fac parte din „lista Scutului de confidențialitate", menținută și pusă la dispoziția publicului de către Departamentul Comerțului al SUA, în conformitate cu secțiunile I și III din principiile prevăzute în anexa II.

Articolul 2

Prezenta decizie nu aduce atingere aplicării dispozițiilor Directivei 95/46/CE, cu excepția articolului 25 alineatul (1), care se referă la prelucrarea datelor cu caracter personal în statele membre, în special articolul 4.

Articolul 3

Ori de câte ori autoritățile competente din statele membre își exercită competențele în temeiul articolului 28 alineatul (3) din Directiva 95/46/CE determinând suspendarea sau interzicerea definitivă a fluxurilor de date către o organizație din Statele Unite ale Americii care este inclusă în lista Scutului de confidențialitate în conformitate cu secțiunile I și III din principiile prevăzute în anexa II, în vederea protejării persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal ale acestora, statul membru în cauză informează Comisia fără întârziere.

Articolul 4

(1) Comisia va monitoriza încontinuu funcționarea Scutului de confidențialitate UE-SUA, cu scopul de a evalua dacă Statele Unite continuă să asigure un nivel adecvat de protecție a datelor cu caracter personal transferate dinspre Uniune către organizații din Statele Unite.

([208]) Avizul 01/2016 referitor la Proiectul de decizie privind caracterul adecvat al Scutului de confidențialitate UE-SUA, publicat la 13 aprilie 2016.

([209]) Rezoluția Parlamentului European din 26 mai 2016 referitoare la fluxurile transatlantice de date [(2016/2727 (RSP)].

(2) Statele membre și Comisia se informează reciproc asupra cazurilor în care se pare că organismele guvernamentale din Statele Unite cu competențe legale pentru a asigura conformitatea cu principiile prevăzute în anexa II nu oferă mecanisme de depistare și supraveghere eficace care să permită identificarea și sancționarea în practică a încălcărilor principiilor.

(3) Statele membre și Comisia se informează reciproc cu privire la orice indicații că ingerințele autorităților publice responsabile pentru securitatea națională, aplicarea legii sau alte interese publice în exercitarea dreptului persoanelor fizice la protecția datelor lor cu caracter personal depășesc ceea ce este strict necesar și/sau că nu există o protecție juridică efectivă unor astfel de ingerințe.

(4) În termen de un an de la data notificării prezentei decizii către statele membre și, ulterior, anual, Comisia va evalua constatarea menționată la articolul 1 alineatul (1) pe baza tuturor informațiilor disponibile, inclusiv informațiile primite ca parte a revizuirii comune anuale menționate în anexele I, II și VI.

(5) Comisia va raporta toate constatările pertinente comitetului instituit în temeiul articolului 31 din Directiva 95/46/CE.

(6) Comisia va prezenta un proiect de măsuri în conformitate cu procedura prevăzută la articolul 31 alineatul (2) din Directiva 95/46/CE în vederea suspendării, a modificării sau a abrogării prezentei decizii sau în vederea limitării domeniului său de aplicare, printre altele, în cazul în care există indicii:

— că autoritățile publice americane nu respectă declarațiile și angajamentele cuprinse în documentele anexate la prezenta decizie, inclusiv în ceea ce privește condițiile și limitările pentru accesul de către autoritățile publice americane în scopuri de aplicare a legii, securitate națională și alte scopuri de interes public la datele cu caracter personal transferate în temeiul Scutului de confidențialitate UE-SUA;

— privind existența unei ineficiențe sistematice în abordarea plângerilor depuse de persoane vizate din UE; sau

— în repetate rânduri, Ombudsmanul pentru Scutul de confidențialitate nu furnizează în timp util răspunsuri adecvate la cererile formulate de persoanele vizate din UE, astfel cum se prevede la secțiunea 4 punctul (e) din anexa III.

Comisia va prezenta, de asemenea, un astfel de proiect de măsuri în cazul în care lipsa de cooperare a organismelor implicate în asigurarea funcționării Scutul de confidențialitate UESUA în Statele Unite nu îi permite să stabilească dacă a fost afectată constatarea stabilită la articolul 1 alineatul (1).

Articolul 5

Statele membre iau toate măsurile necesare pentru a se conforma prezentei decizii.

Articolul 6

Prezenta decizie se adresează statelor membre.

Adoptată la Bruxelles, 12 iulie 2016.

Pentru Comisie
Vra JOUROVÁ
Membru al Comisiei

ANEXA I

Scrisoarea Ministrului american al comerțului Penny Pritzker

7 iulie 2016

Doamna Věra JOUROVÁ
Comisar pentru justiție, consumatori și egalitate de gen
Comisia Europeană
Rue de la Loi/Westraat 200
1049 Bruxelles
Belgia

Stimată Doamnă Comisar Jourová,

În numele Statelor Unite, am plăcerea de a vă transmite în anexă un pachet de materiale referitoare la Scutul de confidențialitate UE-SUA, care este rezultatul a doi ani de discuții productive între echipele noastre. Acest pachet, împreună cu alte materiale aflate la dispoziția Comisiei și provenite din surse publice, oferă o bază foarte solidă pentru o nouă examinare a caracterului adecvat, efectuată de Comisia Europeană ([1]).

Ar trebui să fim cu toții mândri de îmbunătățirile aduse cadrului. Scutul de confidențialitate se bazează pe principii care se bucură de un puternic sprijin consensual pe ambele maluri ale Atlanticului, iar noi am consolidat funcționarea acestora. Prin intermediul colaborării noastre, avem posibilitatea concretă de a îmbunătăți protecția confidențialității în întreaga lume.

Pachetul privind Scutul de confidențialitate conține Principiile privind Scutul de confidențialitate, împreună cu o scrisoare, atașată ca anexa 1, din partea Administrației pentru comerț internațional (International Trade Administration – ITA) din cadrul Dpartamentului Comerțului, care gestionează programul, în care sunt descrise angajamentele asumate de departamentul nostru pentru a se asigura că Scutul de confidențialitate funcționează în mod eficient. De asemenea, pachetul include anexa 2, care cuprinde alte angajamente ale Departamentului Comerțului referitoare la noul model de arbitraj disponibil în cadrul Scutului de confidențialitate.

Mi-am îndemnat echipa să aloce toate resursele necesare pentru a pune în aplicare rapid și pe deplin cadrul privind Scutul de confidențialitate, precum și pentru a se asigura că angajamentele care figurează în anexa 1 și anexa 2 sunt îndeplinite în timp util.

Pachetul privind Scutul de confidențialitate cuprinde, de asemenea, o serie de documente din partea altor agenții din Statele Unite, și anume:

— o scrisoare din partea Comisiei Federale pentru Comerț (Federal Trade Commission – FTC) care descrie asigurarea respectării Scutului de confidențialitate la nivelul său;

— o scrisoare din partea Departamentului Transporturilor care descrie asigurarea respectării Scutului de confidențialitate la nivelul său;

— două scrisori pregătite de Biroul Directorului Serviciului Național de Informații (ODNI) cu privire la garanțiile și limitările aplicabile autorităților naționale americane în materie de securitate;

— o scrisoare din partea Departamentului de Stat și memorandumul de înțelegere care o însoțește, care descrie angajamentul Departamentului de Stat de a institui un nou Ombudsman pentru Scutul de confidențialitate în vederea depunerii solicitărilor de informații cu privire la practicile Statele Unite ale Americii de colectare de informații secrete prin interceptarea de semnale; și

— o scrisoare pregătită de Departamentul de Justiție cu privire la garanțiile și limitările privind accesul guvernului Statelor Unite în scopul aplicării legii și în scopuri de interes public.

Puteți fi sigur că SUA ia aceste angajamente în serios.

([1]) Pachetul privind Scutul de confidențialitate va acoperi atât Uniunea Europeană, cât și aceste trei țări, cu condiția ca Decizia Comisiei privind caracterul adecvat al protecției oferite de Scutul de confidențialitate UESUA să se aplice Islandei, Liechtensteinului și Norvegiei.

În termen de 30 de zile de la aprobarea finală a deciziei de conformitate, întregul pachet privind Scutul de confidențialitate va fi furnizat *Registrului federal* pentru publicare.

Așteptăm cu interes să colaborăm cu dumneavoastră pe parcursul punerii în aplicare a Scutului de confidențialitate și pe măsură ce ne angajăm în următoarea fază a acestui proces împreună.

Cu stimă,

Penny Pritzker

Anexa 1

Scrisoare din partea Subsecretarului de stat pentru comerț internațional Ken Hyatt

Onorabila Věra Jourová
Comisarul pentru justiție, consumatori și egalitate de gen
Comisia Europeană
Rue de la Loi/Westraat 200
1049 Bruxelles
Belgia

Stimată Doamnă Comisar Jourová,

În numele Administrației pentru comerțul internațional, am plăcerea de a descrie protecția sporită a datelor cu caracter personal pe care o oferă cadrul privind Scutul de confidențialitate UE-SUA (denumit în continuare „Scutul de confidențialitate" sau „cadrul") și angajamentele luate de Departamentul Comerțului („Departamentul") pentru a se asigura că Scutul de confidențialitate funcționează în mod eficient. Finalizarea acestui acord istoric este o realizare importantă pentru viața privată și întreprinderile de pe ambele maluri ale Atlanticului. Acesta oferă cetățenilor UE încrederea că datele lor vor fi protejate și că dispun de căile de atac legale pentru a soluționa eventualele probleme. Cadrul oferă certitudinea care va contribui la creșterea economiei transatlantice prin garantarea faptului că mii de întreprinderi europene și americane pot continua să investească și să facă afaceri dincolo de frontierele noastre. Scutul de confidențialitate este rezultatul a peste doi ani de eforturi deosebite și al colaborării cu dumneavoastră, colegii noștri din Comisia Europeană („Comisia"). Așteptăm cu nerăbdare să continuăm activitatea desfășurată în colaborare cu Comisia pentru a ne asigura că Scutul de confidențialitate funcționează astfel cum este prevăzut.

Am colaborat cu Comisia pentru a dezvolta Scutul de confidențialitate în scopul de a permite organizațiilor stabilite în Statele Unite să respecte cerințele de adecvare pentru protecția datelor în temeiul dreptului UE. Noul cadru va aduce o serie de beneficii importante atât pentru cetățeni, cât și pentru întreprinderi. În primul rând, acesta oferă un set important de măsuri de protecție a vieții private în ceea ce privește datele cetățenilor UE. Acesta presupune ca organizațiile americane participante să elaboreze o politică de confidențialitate, să își asume public angajamentul de a respecta principiile privind Scutul de confidențialitate, astfel încât angajamentul să devină executoriu în temeiul legislației SUA, să recertifice anual respectarea principiilor printr-o scrisoare adresată Departamentului, să ofere mecanisme independente gratuite de soluționare a litigiilor persoanelor din UE și să se afle sub autoritatea Comisiei Federale pentru Comerț din SUA („FTC"), a Departamentului Transporturilor („DOT") sau a altei agenții de punere în aplicare. În al doilea rând, Scutul de confidențialitate va permite ca mii de societăți din Statele Unite și filiale ale societăților europene în Statele Unite ale Americii să primească date cu caracter personal din Uniunea Europeană pentru a facilita fluxurile de date care sprijină comerțul transatlantic. Relația economică transatlantică este deja cea mai mare din lume, reprezentând jumătate din producția economică globală și aproape o mie de miliarde de dolari în comerțul cu bunuri și servicii, susținând milioane de locuri de muncă pe ambele maluri ale Atlanticului. Întreprinderile care se bazează pe fluxurile transatlantice de date provin din toate sectoarele industriei și includ societăți importante din clasamentul Fortune 500, precum și numeroase întreprinderi mici și mijlocii (IMM-uri). Fluxurile transatlantice de date permit organizațiilor din Statele Unite ale Americii să prelucreze datele necesare pentru a oferi bunuri, servicii și oportunități de ocupare a forței de muncă cetățenilor europeni. Scutul de confidențialitate sprijină principiile comune de confidențialitate, eliminând diferențele dintre abordările noastre juridice, promovând în același timp obiectivele economice și comerciale, atât din Europa, cât și din Statele Unite.

În timp ce decizia unei întreprinderi de a se autocertifica în acest nou cadru va fi voluntară, odată ce o întreprindere se angajează în mod public să respecte Scutul de confidențialitate, angajamentul său este executoriu în temeiul legislației SUA de către Comisia Federală pentru Comerț și Departamentul Transporturilor, în funcție de autoritatea care deține jurisdicția asupra organizației care aderă la Scutul de confidențialitate.

Modalități de ameliorare în temeiul principiilor privind Scutul de confidențialitate

Scutul de confidențialitate rezultat consolidează protecția vieții private prin:

— solicitarea de informații suplimentare care trebuie furnizate cetățenilor conform principiului notificării, inclusiv o declarație privind participarea organizației la Scutul de confidențialitate, o declarație privind dreptul cetățeanului de a accesa datele cu caracter personal, precum și identificarea unui organism independent competent de soluționare a litigiilor;

— consolidarea protecției datelor cu caracter personal care sunt transferate de la o organizație care aderă la Scutul de confidențialitate către un operator terț prin obligarea părților să încheie un contract care prevede că astfel de date pot fi prelucrate doar în scopuri specifice și limitate în conformitate cu acordul furnizat de fiecare cetățean și că destinatarul va asigura un nivel de protecție echivalent cu cel prevăzut de principii;

— consolidarea protecției datelor cu caracter personal care sunt transferate de la o organizație care aderă la Scutul de confidențialitate către un agent terț, inclusiv prin impunerea ca o organizație care aderă la Scutul de confidențialitate: să ia măsuri rezonabile și adecvate pentru a se asigura că agentul prelucrează în mod eficient informațiile cu caracter personal transferate într-un mod compatibil cu obligațiile organizației care îi revin în temeiul principiilor; în urma notificării, să ia măsuri rezonabile și adecvate pentru a opri și remedia prelucrarea neautorizată; și să ofere Departamentului, la cerere, un rezumat sau o copie a dispozițiilor relevante cu privire la protecția vieții private a contractului cu agentul respectiv;

— prevederea faptului că o organizație care aderă la Scutul de confidențialitate este responsabilă de prelucrarea datelor cu caracter personal pe care le primește în cadrul Scutului de confidențialitate și pe care ulterior le transferă către o parte terță care acționează ca agent în numele său și că organizația care aderă la Scutul de confidențialitate rămâne răspunzătoare, în temeiul principiilor, dacă agentul acesteia prelucrează astfel de informații cu caracter personal într-un mod incompatibil cu principiile, cu excepția cazului în care organizația dovedește că nu este responsabilă pentru fapta care a provocat prejudiciul;

— clarificarea faptului că organizațiile care aderă la Scutul de confidențialitate trebuie să limiteze informațiile cu caracter personal la informații care sunt relevante în scopul prelucrării;

— solicitarea ca o organizație să își certifice anual Departamentului angajamentul de a aplica principiile la informațiile primite în perioada în care a participat la Scutul de confidențialitate, în cazul în care părăsește Scutul de confidențialitate și decide să păstreze datele respective;

— solicitarea instituirii unor mecanisme independente de recurs fără ca persoana în cauză să suporte vreun cost;

— solicitarea ca organizațiile și mecanismele independente de recurs selectate de acestea să răspundă cu promptitudine la cererile de informații și la cererile Departamentului privind informații referitoare la Scutul de confidențialitate;

— solicitarea ca organizațiile să răspundă rapid la reclamații în ceea ce privește respectarea principiilor menționate de autoritățile statelor membre ale UE prin intermediul Departamentului; și

— solicitarea ca o organizație care aderă la Scutul de confidențialitate să publice toate secțiunile relevante cu privire la Scutul de confidențialitate sau orice raport de evaluare transmis către FTC în cazul în care face obiectul unei ordonanțe a FTC sau al unui ordin judecătoresc bazat pe nerespectarea principiilor.

Administrarea și supravegherea programului Scutului de confidențialitate de către Departamentul Comerțului

Departamentul își reiterează angajamentul de a menține și de a pune la dispoziția publicului o listă oficială a organizațiilor din SUA care s-au autocertificat la Departament și și-au luat angajamentul de a adera la principii (denumită în continuare „lista Scutului de confidențialitate”). Departamentul va actualiza lista Scutului de confidențialitate prin eliminarea organizațiilor în cazul în care se retrag în mod voluntar, nu finalizează recertificarea anuală în conformitate cu procedurile Departamentului sau dacă se constată că încalcă sistematic principiile. De asemenea, Departamentul va menține și va pune la dispoziția publicului un registru oficial al organizațiilor din SUA care s-au autocertificat la Departament, dar care au fost eliminate din lista Scutului de confidențialitate, inclusiv cele care au fost eliminate pentru încălcarea sistematică a principiilor. Departamentul va identifica motivul pentru care a fost eliminată fiecare organizație.

În plus, Departamentul își asumă angajamentul de a consolida gestionarea și supravegherea Scutului de confidențialitate. În special, Departamentul va asigura:

Furnizarea de informații suplimentare cu privire la site-ul internet al Scutului de confidențialitate

— va menține lista Scutului de confidențialitate, precum și un registru al organizațiilor care și-au autocertificat anterior aderarea la principii, dar care nu mai beneficiază de Scutul de confidențialitate;

— va include o explicație afișată foarte vizibil care să clarifice faptul că toate organizațiile eliminate de pe lista Scutului de confidențialitate nu mai beneficiază de avantajele Scutului de confidențialitate, dar trebuie totuși să continue să aplice principiile în ceea ce orivește informațiile cu caracter personal primite în perioada în care acestea au participat la Scutul de confidențialitate, atât timp cât păstrează informațiile respective; și

— va furniza un link către lista de cazuri FTC legate de Scutul de confidențialitate menținută pe site-ul internet al FTC.

Verificarea cerințelor de autocertificare

— înainte de finalizarea autocertificării (sau recertificării anuale) a unei organizații și de introducerea unei organizații înscrise pe lista Scutului de confidențialitate, acesta va verifica dacă organizația:

  — a furnizat informațiile de contact ale organizației solicitate;

  — a descris activitățile organizației cu privire la informațiile cu caracter personal primite din Uniunea Europeană;

  — a indicat datele cu caracter personal care sunt reglementate de autocertificare;

  — în cazul în care organizația dispune de un site internet public, a furnizat adresa de internet unde este publicată politica de confidențialitate, iar politica de confidențialitate este accesibilă la adresa de internet furnizată sau, în cazul în care o organizație nu dispune de un site internet public, a comunicat locul în care textul politicii de confidențialitate poate fi consultat de către public;

  — a inclus în politica de confidențialitate relevantă o declarație că aderă la principii, precum și, dacă politica de confidențialitate este disponibilă pe internet, un link către site-ul Scutului de confidențialitate al Departamentului;

  — a identificat denumirea organismului de reglementare specific având competențe de a trata plângerile depuse împotriva organizației privind posibile practici neloiale sau frauduloase și încălcări ale legilor sau reglementărilor privind protecția vieții private (și care este menționat în principii sau într-o anexă ulterioară la principii);

  — în cazul în care organizația decide să îndeplinească cerințele de la litera (a) punctele (i) și (iii) din principiul recursului, punerii în aplicare și responsabilității, luându-și angajamentul de a coopera cu autoritățile UE pentru protecția datelor („APD"), și-a exprimat intenția de a coopera cu autoritățile pentru protecția datelor la analizarea și soluționarea plângerilor înaintate în temeiul Scutului de confidențialitate, în special pentru a răspunde la cererile lor de informații atunci când persoanele vizate din UE și-au înaintat plângerile direct la autoritățile naționale pentru protecția datelor;

  — a identificat orice program privind protecția vieții private la care participă organizația;

  — a identificat metoda de verificare a asigurării respectării principiilor (de exemplu, internă sau printr-un terț);

  — a identificat, atât în declarația de autocertificare, cât și în politica sa de confidențialitate, instanța independentă de recurs care poate ancheta și soluționa plângerile;

  — a inclus în politica de confidențialitate relevantă, dacă aceasta este disponibilă pe internet, un link către site-ul internet sau formularul de depunere a plângerii al instanței independente de recurs care poate ancheta plângerile nesoluționate; și

  — în cazul în care organizația a indicat că intenționează să primească informații privind resursele umane transferate din UE în contextul unui raport de muncă, și-a declarat angajamentul de a coopera cu autoritățile pentru protecția datelor pentru a soluționa plângerile cu privire la activitățile sale în ceea ce privește astfel de date, a furnizat Departamentului o copie a politicii sale de confidențialitate în materie de resurse umane și a precizat unde poate fi consultat textul politicii de confidențialitate de către lucrătorii afectați;

— colaborează cu instanțele independente de recurs pentru a verifica dacă organizațiile s-au înregistrat, în fapt, la instanța relevantă indicată pe declarația de autocertificare, în cazul în care este necesară o astfel de înregistrare.

Extinderea eforturilor de a asigura urmărirea organizațiilor care au fost eliminate din lista Scutului de confidențialitate

— va notifica organizațiile care sunt eliminate din lista Scutului de confidențialitate pentru „nerespectare repetată" că nu au dreptul de a păstra informații colectate în temeiul Scutului de confidențialitate; și

— va trimite chestionare organizațiilor ale căror autocertificări expiră sau care s-au retras în mod voluntar din Scutul de confidențialitate pentru a verifica dacă organizația va returna, va șterge sau va continua să aplice principiile în ceea ce privește informațiile cu caracter personal primite în perioada în care au participat la Scutul de confidențialitate și în cazul în care datele cu caracter personal sunt păstrate, va verifica persoana din cadrul organizației care va servi drept punct de contact permanent pentru întrebările legate de Scutul de confidențialitate.

Identificarea și abordarea afirmațiilor false de participare

— va revizui politicile de confidențialitate ale organizațiilor care au participat anterior la programul Scutului de confidențialitate, dar care au fost eliminate din lista Scutului de confidențialitate, pentru a identifica orice declarație falsă de participare la Scutul de confidențialitate;

— în mod permanent, atunci când o organizație: (a) se retrage de la participarea la Scutul de confidențialitate; (b) nu își recertifică aderarea la principii; sau (c) este eliminată ca participant la Scutul de confidențialitate, în special pentru „nerespectare repetată a principiilor", acesta se angajează, din oficiu, să verifice dacă organizația a eliminat din orice trimiteri relevante la politica de confidențialitate publicată orice trimiteri la Scutul de confidențialitate care implică faptul că organizația continuă să participe activ la Scutul de confidențialitate și are dreptul la beneficiile acestuia. În cazul în care constată că astfel de trimiteri nu au fost eliminate, Departamentul va avertiza organizația că acesta va sesiza, după caz, problemele agenției relevante pentru posibile măsuri de asigurare a respectării dacă organizația continuă să pretindă certificarea Scutului de confidențialitate. În cazul în care organizația nu elimină trimiterile, nici nu autocertifică conformitatea acesteia cu Scutul de confidențialitate, Departamentul va sesiza problema, din oficiu, la FTC, Departamentul Transporturilor sau o altă agenție adecvată de asigurare a respectării sau, în anumite cazuri, va lua măsuri pentru a aplica marca de certificare a Scutului de confidențialitate;

— va depune alte eforturi pentru a identifica declarațiile false privind participarea la Scutul de confidențialitate și utilizarea necorespunzătoare a mărcii de certificare Scutul de confidențialitate, inclusiv prin efectuarea de căutări pe internet pentru a identifica unde sunt afișate imagini ale mărcii de certificare Scutul de confidențialitate și trimiteri la Scutul de confidențialitate în politicile de confidențialitate ale organizațiilor;

— va aborda fără întârziere orice probleme identificate în cadrul monitorizării *ex officio* a declarațiilor false de participare și utilizarea necorespunzătoare a mărcii de certificare, inclusiv avertizarea organizațiilor cu privire la declarațiile false privind participarea acestora la programul Scutului de confidențialitate în modul descris mai sus;

— va lua alte măsuri corective adecvate, inclusiv orice cale de atac pe care Departamentul este autorizat să o întreprindă și sesizarea FTC, a Departamentului Transporturilor sau a unei alte agenții adecvate de asigurare a respectării; și

— va revizui și va soluționa rapid plângerile primite cu privire la declarațiile false de participare.

Departamentul va revizui politicile de confidențialitate ale organizațiilor pentru a identifica și a aborda într-un mod mai eficient declarațiile false de participare la Scutul de confidențialitate. În special, Departamentul va revizui politicile de confidențialitate ale organizațiilor a căror autocertificare a expirat deoarece nu au recertificat aderarea la principii. Departamentul va efectua acest tip de control pentru a verifica dacă organizațiile au eliminat din orice politică de confidențialitate publicată orice trimiteri care indică faptul că organizațiile continuă să participe activ la Scutul de confidențialitate. Ca rezultat al acestor tipuri de analize, Departamentul va identifica organizațiile care nu au eliminat aceste trimiteri și va trimite acestor organizații o scrisoare de avertizare din partea biroului de consiliere generală al Departamentului cu privire la potențialele măsuri de asigurare a respectării în cazul în care trimiterile nu sunt eliminate. Departamentul va lua măsuri de monitorizare pentru a asigura că organizațiile fie elimină trimiterile necorespunzătoare, fie își recertifică aderarea la principii. În plus, Departamentul va depune eforturi pentru a identifica declarațiile false privind participarea la Scutul de confidențialitate a organizațiilor care nu au mai participat la programul Scutului de confidențialitate și va lua măsuri corective similare cu privire la astfel de organizații.

Efectuarea de evaluări periodice *ex officio* ale conformității și de evaluări ale programului

— va asigura o monitorizare permanentă a respectării efective, inclusiv prin trimiterea de chestionare detaliate organizațiilor participante, pentru a identifica aspectele care ar putea necesita acțiuni ulterioare suplimentare. În special, astfel de controale de conformitate au loc atunci când: (a) Departamentul a primit plângeri neabuzive specifice cu privire la respectarea principiilor de către organizație; (b) o organizație nu răspunde în mod satisfăcător la solicitările de informații din partea Departamentului referitoare la Scutul de confidențialitate; sau (c) există dovezi credibile că o organizație nu își îndeplinește angajamentele asumate în temeiul Scutului de confidențialitate. Serviciul trebuie, după caz, să consulte autoritățile competente de protecție a datelor cu privire la astfel de controale de conformitate; și

— va evalua periodic administrarea și supravegherea programului Scutului de confidențialitate, pentru a se asigura că eforturile de monitorizare sunt adecvate pentru abordarea noilor probleme pe măsură ce acestea apar.

Departamentul și-a sporit resursele care vor fi alocate pentru administrarea și supravegherea Scutului de confidențialitate, inclusiv prin dublarea numărului membrilor personalului responsabil de administrarea și supravegherea programului. Vom continua să alocăm resurse adecvate pentru astfel de eforturi în scopul de a asigura o monitorizare și administrare eficace a programului.

Adaptarea site-ului Scutului de confidențialitate la publicul vizat

Departamentul va adapta site-ul internet al Scutului de confidențialitate pentru a viza trei categorii de public: cetățeni UE, întreprinderi din UE și întreprinderi din SUA. Includerea materialelor care vizează direct cetățenii UE și întreprinderile din UE va facilita transparența în mai multe moduri. În ceea ce privește cetățenii UE, acesta va explica în mod clar: (1) drepturile pe care Scutul de confidențialitate le oferă cetățenilor UE; (2) mecanismele de recurs disponibile pentru cetățenii UE în momentul în care aceștia consideră că o organizație și-a încălcat angajamentul de a respecta principiile; și (3) modul în care se pot găsi informații referitoare la autocertificarea organizației în ceea ce privește Scutul de confidențialitate. În ceea ce privește întreprinderile din UE, acesta le va ajuta să verifice: (1) dacă o organizație este asigurată de beneficiile Scutului de confidențialitate; (2) tipul de informații care fac obiectul autocertificării unei organizații în ceea ce privește Scutul de confidențialitate; (3) politica de confidențialitate care se aplică informațiilor care intră sub incidența acesteia; și (4) metoda utilizată de organizație pentru a verifica respectarea principiilor de către aceasta.

Intensificarea cooperării cu autoritățile pentru protecția datelor

Pentru a spori posibilitățile de a coopera cu autoritățile pentru protecția datelor, Departamentul va stabili un punct de contact special în cadrul acestuia care să acționeze ca intermediar în relația cu autoritățile pentru protecția datelor. În cazul în care o autoritate pentru protecția datelor consideră că o organizație nu respectă principiile, inclusiv în urma unei plângeri din partea unei persoane din UE, APD poate lua legătura cu persoana de contact din cadrul Departamentului pentru a trimite organizația pentru revizuire ulterioară. De asemenea, persoana de contact va primi sesizări privind organizațiile care susțin în mod fals că participă la Scutul de confidențialitate, deși nu și-au autocertificat niciodată aderarea la principii. Persoana de contact va sprijini autoritățile pentru protecția datelor care caută informații referitoare la autocertificarea sau participarea anterioară a unei anumite organizații la program și va răspunde solicitărilor de informații ale autorității pentru protecția datelor cu privire la punerea în aplicare a anumitor cerințe ale Scutului de confidențialitate. În al doilea rând, Departamentul va oferi autorităților pentru protecția datelor materiale privind Scutul de confidențialitate pentru a fi incluse pe propriile site-uri internet în vederea sporirii transparenței pentru cetățenii UE și întreprinderile din UE. Creșterea gradului de conștientizare în ceea ce privește Scutul de confidențialitate și drepturile și responsabilitățile pe care le creează acesta ar trebui să faciliteze identificarea problemelor în momentul în care apar, astfel încât acestea să poată fi abordate în mod adecvat.

Facilitarea soluționării plângerilor referitoare la nerespectarea principiilor

Departamentul, prin persoana de contact, va primi plângerile trimise la Departament de o autoritate pentru protecția datelor cu privire la faptul că o organizație care aderă la Scutul de confidențialitate nu respectă principiile. Departamentul va depune toate eforturile pentru a facilita soluționarea plângerii împreună cu organizația care aderă la Scutul de confidențialitate. În termen de 90 de zile de la data primirii plângerii, Departamentul va furniza o actualizare autorității pentru protecția datelor. Pentru a facilita depunerea plângerilor, Departamentul va crea un formular standard pe care autoritățile pentru protecția datelor să îl transmită persoanei de contact a Departamentului. Persoana de contact va urmări toate sesizările de la autoritățile pentru protecția datelor primite de Departament, iar Departamentul va furniza în raportul anual de analiză descris mai jos o analiză agregată a plângerilor pe care le primește în fiecare an.

Adoptarea procedurilor de arbitraj și selectarea arbitrilor în consultare cu Comisia

Departamentul își va îndeplini angajamentele asumate în temeiul anexei I și va publica procedurile după ce s-a ajuns la un acord.

Mecanismul de revizuire comună a funcționării Scutului de confidențialitate

Departamentul Comerțului, FTC și celelalte agenții, după caz, vor organiza reuniuni anuale cu Comisia, autoritățile interesate pentru protecția datelor, precum și cu reprezentanți ai grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, în cursul cărora Departamentul va oferi informații actualizate cu privire la programul Scutului de confidențialitate. Reuniunile anuale vor include discuții cu privire la chestiuni d actualitate referitoare la funcționarea, punerea în aplicare, supravegherea și asigurarea respectării Scutului de confidențialitate, inclusiv sesizări primite de Departament de la autorități pentru protecția datelor, rezultatele evaluărilor de conformitate *ex officio* și poate include, de asemenea, discuții cu privire la modificări relevante de legislației. Prima reexaminare anuală și reexaminările ulterioare, după caz, vor include un dialog cu privire la alte teme, cum ar fi în domeniul procesului decizional automatizat, inclusiv în ceea ce privește asemănările și diferențele de abordare în UE și SUA.

Actualizarea legislației

Departamentul va depune eforturi rezonabile pentru a informa Comisia cu privire la evoluții semnificative în legislația Statelor Unite, în măsura în care acestea sunt relevante pentru Scutul de confidențialitate în ceea ce privește protecția datelor cu caracter personal și limitările și garanțiile aplicabile accesului la date cu caracter personal de către autoritățile SUA și utilizarea ulterioară a acestora.

Excepția pe motivul securității naționale

Cu privire la limitările referitoare la respectarea principiilor privind Scutul de confidențialitate în scopuri legate de securitatea națională, consilierul general al Biroului Directorului Serviciului Național de Informații, Robert Litt, a trimis, de asemenea, două scrisori adresate domnilor Justin Antonipillai și Ted Dean de la Departamentul Comerțului, care v-au fost transmise. Aceste scrisori abordează pe larg, printre altele, politicile, garanțiile și limitările care se aplică activităților de obținere de informații secrete prin interceptarea de semnale desfășurate de SUA. În plus, aceste scrisori descriu transparența asigurată de serviciile de informații cu privire la chestiunile respective. Pe măsură ce Comisia evaluează cadrul privind Scutul de confidențialitate, informațiile transmise prin aceste scrisori oferă asigurări pentru a concluziona că Scutul de confidențialitate va funcționa în mod corespunzător, în conformitate cu principiile exprimate în documentul respectiv. Înțelegem că, în viitor, puteți colecta informații care au fost comunicate în mod public de către comunitatea serviciilor de informații, împreună cu alte informații, pe care să se bazeze revizuirea anuală a cadrului privind Scutul de confidențialitate.

Pe baza principiilor privind Scutul de confidențialitate și a scrisorilor și materialelor însoțitoare, inclusiv a angajamentelor Departamentului în ceea ce privește administrarea și supravegherea cadrului privind Scutul de confidențialitate, ne așteptăm ca analiza Comisiei să stabilească faptul că acest cadru privind Scutul de confidențialitate UE-SUA oferă o protecție adecvată în sensul dreptului Uniunii și că transferurile de date din Uniunea Europeană vor continua pentru organizațiile care participă la Scutul de confidențialitate.

Cu stimă,

Ken Hyatt

Anexa 2

Model de arbitraj

ANEXA I

Prezenta anexă I prevede condițiile în care organizațiile care aderă la Scutul de confidențialitate sunt obligate să supună plângerile unei proceduri de arbitraj, în temeiul principiului recursului, punerii în aplicare și responsabilității. Opțiunea arbitrajului obligatoriu descrisă mai jos se aplică anumitor plângeri „rămase" privind datele aflate sub incidența Scutului de confidențialitate UE-SUA. Obiectivul acestei opțiuni este de a oferi un mecanism echitabil, independent și prompt, la alegerea persoanelor în cauză, pentru soluționarea presupuselor încălcări ale principiilor care nu au fost rezolvate prin alte mecanisme din cadrul Scutului de confidențialitate, în cazul în care există.

A. **Domeniu de aplicare**

Această opțiune a arbitrajului este pusă la dispoziția unei persoane pentru a determina, pentru plângerile rămase, dacă o organizație care aderă la Scutul de confidențialitate a încălcat obligațiile care îi revin în temeiul principiilor în ceea ce privește persoana în cauză și dacă orice astfel de încălcări nu sunt remediate în totalitate sau parțial. Această opțiune este disponibilă numai în aceste scopuri. Această opțiune nu este disponibilă, de exemplu, în ceea ce privește excepțiile de la principii ([1]) sau cu privire la o prezumție cu privire la caracterul adecvat al Scutului de confidențialitate.

B. **Căile de atac disponibile**

În cadrul acestei opțiuni de arbitraj, comitetul pentru Scutul de confidențialitate (format din unul sau din trei arbitri, astfel cum s-a convenit de către părți) are autoritatea de a impune măsuri echitabile, nemonetare, personalizate (precum accesul, rectificarea, ștergerea sau restituirea datelor persoanei în cauză) necesare pentru a remedia încălcarea principiilor numai cu privire la persoana în cauză. Acestea sunt singurele competențe ale comisiei de arbitraj referitoare la căile de atac. La examinarea căilor de atac, comisia de arbitraj este obligată să examineze alte căi de atac deja impuse prin alte mecanisme în temeiul Scutului de confidențialitate. Nu sunt disponibile măsuri pentru repararea prejudiciilor, taxe sau alte căi de atac. Fiecare parte suportă propriile onorarii plătite avocaților.

C. **Cerințe de îndeplinit înainte de arbitraj**

O persoană care decide să se prevaleze de această opțiune de arbitraj trebuie să ia următoarele măsuri înainte de inițierea unei solicitări de arbitraj: (1) să reclame presupusa încălcare direct la organizație și să ofere organizației posibilitatea de a soluționa problema în termenele prevăzute în secțiunea III.11 litera (d) punctul (i) din principii; (2) să utilizeze mecanismul independent de recurs în temeiul principiilor, fără ca persoana în cauză să suporte vreun cost; și (3) să ridice problema prin intermediul autorității pentru protecția datelor la Departamentul Comerțului și să ofere Departamentului Comerțului ocazia de a depune eforturi pentru a soluționa problema în termenele prevăzute în scrisoarea de la Administrația pentru comerțul internațional din cadrul Departamentului Comerțului, fără ca persoana în cauză să suporte vreun cost.

Această opțiune de arbitraj nu poate fi invocată în cazul în care aceeași acuzație de încălcare a principiilor a unei persoane (1) a făcut deja obiectul unui arbitraj obligatoriu; (2) a făcut obiectul unei hotărâri cu caracter definitiv într-o acțiune judiciară la care persoana a fost parte; sau (3) a fost soluționată de părți. În plus, această opțiune nu poate fi invocată în cazul în care o autoritate pentru protecția datelor din UE Autoritatea (1) are competență în temeiul secțiunilor III.5 sau III.9 din principii; sau (2) are competența de a soluționa presupusa încălcare în mod direct cu organizația. Competența unei APD de a soluționa aceeași plângere împotriva unui operator de date din UE nu se opune invocării opțiunii de arbitraj împotriva unei entități juridice diferite care nu intră sub jurisdicția autorității pentru protecția datelor.

D. **Caracterul obligatoriu al deciziilor**

Decizia unei persoane de a invoca opțiunea arbitrajului obligatoriu este exclusiv voluntară. Deciziile arbitrale sunt obligatorii pentru toate părțile la arbitraj. Odată invocată această opțiune, persoana în cauză renunță la posibilitatea de a solicita măsuri reparatorii pentru aceeași presupusă încălcare în alte forumuri, cu excepția cazului în care măsurile reparatorii echitabile nemonetare nu compensează pe deplin presupusa încălcarea, invocarea arbitrajului nu împiedică introducerea unei acțiuni în despăgubire care este disponibilă în alt mod în instanță.

([1]) Secțiunea I.5 din principii.

E. **Revizuirea și punerea în aplicare**

Persoanele și organizațiile care aderă la Scutul de confidențialitate vor putea să inițieze o procedură judiciară și să solicite aplicarea hotărârilor arbitrale în temeiul legislației SUA, în conformitate cu Legea federală privind arbitrajul ([1]). Orice astfel de cazuri trebuie introduse la instanța federală districtuală pe a cărei rază teritorială se află sediul principal al organizației care aderă la Scutul de confidențialitate.

Această opțiune de arbitraj vizează soluționarea litigiilor individuale, iar hotărârile arbitrale nu sunt destinate să funcționeze ca un precedent obligatoriu sau convingător în chestiuni care implică alte părți, inclusiv arbitraje viitoare sau în instanțe din UE sau din SUA sau într-o procedură judiciară a FTC.

F. **Comisia de arbitraj**

Părțile selectează arbitrii din lista arbitrilor discutată mai jos.

În conformitate cu legislația aplicabilă, Departamentul Comerțului din SUA și Comisia Europeană vor elabora o listă de cel puțin 20 de arbitri, selectați pe criterii de independență, integritate și expertiză. Următoarele dispoziții se aplică în ceea ce privește acest proces:

Arbitrii

1. vor rămâne pe listă pentru o perioadă de 3 ani, cu absențe în circumstanțe excepționale sau motivat, termen care poate fi reînnoit pentru o perioadă suplimentară de 3 ani;

2. nu se supun niciunei instrucțiuni din partea, nici nu au legătură cu una dintre părți, nici cu vreo organizație care aderă la Scutul de confidențialitate, nici cu SUA, UE sau orice stat membru al UE sau orice altă autoritate guvernamentală, autoritate publică sau autoritate de aplicare a legii; și

3. trebuie să fie autorizați să exercite o profesiune juridică în SUA și să fie experți în legislația SUA privind protecția vieții private, cu expertiză în legislația UE privind protecția datelor.

G. **Proceduri de arbitraj**

În conformitate cu legislația aplicabilă, în termen de 6 luni de la adoptarea deciziei privind caracterul adecvat, Departamentul Comerțului și Comisia Europeană sunt de acord să adopte o serie de proceduri de arbitraj ale SUA consacrate (cum ar fi AAA sau JAMS) care reglementează procedura în fața comitetului pentru Scutul de confidențialitate, sub rezerva fiecăreia dintre considerațiile următoare:

1. O persoană poate iniția un arbitraj obligatoriu, sub rezerva îndeplinirii dispoziției privind cerințele anterioare arbitrajului de mai sus, prin transmiterea unei „notificări" organizației. Notificarea trebuie să conțină un rezumat al măsurilor luate în conformitate cu punctul C pentru soluționarea cererii, o descriere a presupusei încălcări și, la alegerea persoanei, toate documentele și materialele justificative și/sau o discuție pe marginea legislației referitoare la presupusa încălcare.

([1]) Capitolul 2 din Federal Arbitration Act („FAA") prevede că „[u]n acord de arbitraj sau o hotărâre arbitrală care decurge dintr-o relație juridică, contractuală sau nu, care este considerată comercială, inclusiv o tranzacție, contract sau acord descrise în [secțiunea 2 din FAA], intră în sfera de aplicare a Convenției [privind recunoașterea și aplicarea hotărârilor arbitrale străine, din 10 iunie 1958, 21 U. S.T. 2519, T.I.A.S. nr. 6997 («Convenția de la New York»)." 9 U.S.C. § 202. De asemenea, FAA prevede că, „[u]n acord sau o hotărâre arbitrală care decurge dintr-o astfel de relație care este doar între cetățenii Statelor Unite se consideră că nu intră în domeniul de aplicare al Convenției [de la New York], cu excepția cazului în care această relație implică bunuri aflate în străinătate, prevede executarea sau aplicarea în străinătate sau are o altă relație cu unul sau mai multe state terțe." *Id.* În conformitate cu capitolul 2, „orice parte la arbitraj poate apela la orice instanță care are competență în temeiul prezentului capitol pentru o ordonanță prin care se confirmă hotărârea împotriva oricărei alte părți la arbitraj. Instanța confirmă hotărârea, cu excepția cazului în care constată că unul dintre motivele de refuz sau de amânare a recunoașterii sau a executării hotărârii este specificat în Convenția [de la New York] menționată." *Id.*, § 207 (g). Capitolul 2 prevede în continuare că „[i]nstanțele districtuale din Statele Unite. .. au jurisdicția inițială asupra. .. unei acțiuni sau proceduri [în temeiul Convenției de la New York], indiferent de suma în litigiu." *Id.* § 203.
Capitolul 2 prevede, de asemenea, că „dispozițiile capitolului 1 se aplică acțiunilor și procedurilor intentate în temeiul prezentului capitol, în măsura în care capitolul în cauză nu intră în conflict cu prezentul capitol sau cu Convenția [de la New York] astfel cum au fost ratificată de Statele Unite." *Id.* § 208. Capitolul 1, în schimb, prevede că „[o] dispoziție scrisă dintr-un... contract care demonstrează existența unei tranzacții care implică relații comerciale pentru a soluționa prin arbitraj o controversă, care decurge din acest contract sau tranzacție sau refuzul de a executa contractul în totalitate sau parțial sau un acord în scris de a supune arbitrajului o controversă existentă care decurge din acest contract, tranzacție sau refuz, este valabil, irevocabil și executoriu, cu excepția cazurilor în care există motive în drept sau în echitate în cazul revocării unui contract." *Id.* § 2. Capitolul 1 prevede, de asemenea, că „orice parte la procedura de arbitraj poate solicita instanței susmenționate o ordonanță care să confirme ulterior hotărârea, iar instanța trebuie să acorde o astfel de ordin, cu excepția cazului în care hotărârea este anulată, modificată sau rectificată, astfel cum se prevede în secțiunile 10 și 11 din [FAA]." *Id.* § 9.

2. Se vor elabora proceduri pentru a asigura că aceeași încălcare invocată de o persoană nu beneficiază de măsuri reparatorii sau proceduri duplicate.

3. Acțiunea FTC poate continua în paralel cu arbitrajul.

4. Niciun reprezentant al SUA, UE sau al oricărui stat membru al UE sau orice altă autoritate guvernamentală, autoritate publică sau autoritate de executare nu poate participa la aceste arbitraje, cu condiția ca, la cererea unei persoane din UE, autoritățile pentru protecția datelor din UE să poată oferi asistență doar în pregătirea notificării, fără ca APD din UE să aibă acces la materialele divulgate sau la orice alte materiale referitoare la aceste proceduri de arbitraj.

5. Locul arbitrajului este Statele Unite, iar persoana în cauză poate alege participarea telefonică sau video, servicii care vor fi furnizate gratuit. Nu va fi necesară participarea directă.

6. Limba procedurilor de arbitraj va fi limba engleză, cu excepția cazului în care părțile convin altfel. În urma unei cereri justificate și luând în considerare dacă persoana respectivă este reprezentată de un avocat, se oferă servicii de interpretare în cadrul ședinței de arbitraj, precum și traducerea materialelor de arbitraj fără ca persoana în cauză să suporte vreun cost, cu excepția cazului în care comitetul consideră că, în împrejurările specifice de arbitraj, aceasta ar putea conduce la costuri nejustificate sau disproporționate.

7. Materialele prezentate arbitrilor vor fi tratate confidențial și vor fi utilizate numai în legătură cu procedura de arbitraj.

8. Prezentarea dovezilor specifice persoanei în cauză poate fi permisă, dacă este necesar, iar dovezile vor fi tratate confidențial de către părți și vor fi utilizate numai în legătură cu procedura de arbitraj.

9. Arbitrajele trebuie finalizate în termen de 90 de zile de la transmiterea notificării către organizația în cauză, cu excepția cazului în care s-a convenit altfel de către părți.

H. **Costuri**

Arbitrii trebuie să ia măsurile necesare pentru a reduce la minimum costurile sau onorariile arbitrajelor.

Sub rezerva legislației aplicabile, Departamentul Comerțului va facilita instituirea unui fond la care organizațiile care aderă la Scutul de confidențialitate trebuie să plătească o cotizație anuală, bazată, parțial, pe dimensiunea organizației, care va acoperi costurile de arbitraj, inclusiv onorariile arbitrilor, până la sume maxime („plafoane”), în colaborare cu Comisia Europeană. Fondul va fi gestionat de un terț, care va raporta cu regularitate cu privire la activitățile Fondului. În cadrul revizuirii anuale, Departamentul Comerțului și Comisia Europeană vor revizui funcționarea fondului, inclusiv necesitatea de a ajusta valoarea cotizațiilor sau a plafoanelor, și va avea în vedere, printre altele, numărul de arbitri, costurile și calendarul arbitrajelor, cu înțelegerea că nu va exista o sarcină financiară excesivă impusă asupra organizațiilor care aderă la Scutul de confidențialitate. Onorariul avocatului nu este reglementat de prezenta dispoziție sau orice alt fond în temeiul acestei dispoziții.

ANEXA II

PRINCIPIILE CADRULUI PRIVIND SCUTUL DE CONFIDENȚIALITATE UE-SUA PUBLICATE DE DEPARTAMENTUL COMERȚULUI AL SUA

I. PREZENTARE GENERALĂ

1. Deși Statele Unite ale Americii și Uniunea Europeană au ca obiectiv comun asigurarea unei mai bune protecții a vieții private, Statele Unite ale Americii abordează în mod diferit acest domeniu față de Uniunea Europeană. Statele Unite ale Americii utilizează o abordare sectorială care se bazează pe un ansamblu de dispoziții legislative, regulamente și coduri de autoreglementare. Având în vedere aceste diferențe și pentru a furniza organizațiilor din Statele Unite ale Americii un mecanism fiabil pentru transferurile de date cu caracter personal către Statele Unite din Uniunea Europeană, asigurându-se, în același timp, că persoanele vizate din UE continuă să beneficieze de garanții eficiente și de protecție impuse de legislația europeană cu privire la prelucrarea datelor lor cu caracter personal, în cazul în care acestea au fost transferate către țări din afara UE, Departamentul Comerțului publică prezentele principii privind Scutul de confidențialitate, inclusiv principiile suplimentare (denumite în continuare, împreună, „principiile") în calitate de autoritate competentă cu scopul de a stimula, a promova și a dezvolta comerțul internațional (15 U.S.C. § 1512). Principiile au fost elaborate prin consultări cu Comisia Europeană, precum și cu industria și cu alte părți interesate, în vederea facilitării comerțului și a relațiilor de afaceri dintre Statele Unite ale Americii și Uniunea Europeană. Acestea sunt destinate exclusiv organizațiilor din Statele Unite ale Americii care primesc date cu caracter personal din Uniunea Europeană cu scopul de a se califica pentru Scutul de confidențialitate și, prin urmare, de a beneficia de decizia Comisiei Europene privind caracterul adecvat ([1]). Principiile nu afectează punerea în aplicare a dispozițiilor naționale de punere în aplicare a Directivei 95/46/CE (denumită în continuare „directiva"), care se aplică prelucrării datelor cu caracter personal în statele membre. Principiile nu limitează obligațiile de confidențialitate care se aplică în temeiul legislației SUA.

2. În scopul de a se prevala de Scutul de confidențialitate pentru a efectua transferuri de date cu caracter personal din UE, o organizație trebuie să prezinte autocertificarea aderării sale la prezentele principii Departamentului Comerțului (sau reprezentantul acestuia) (denumit în continuare „Departamentul"). Deși deciziile organizațiilor de a participa astfel la Scutul de confidențialitate sunt complet voluntare, conformitatea efectivă este obligatorie: organizațiile care prezintă Departamentului autocertificarea și se angajează public să adere la principii trebuie să respecte pe deplin principiile. Pentru a participa la Scutul de confidențialitate, o organizație trebuie: (a) să facă obiectul competențelor de investigare și de asigurare a respectării ale Comisiei Federale pentru Comerț (FTC), ale Departamentului Transporturilor sau ale altui organism oficial care asigură punerea în aplicare cu eficacitate a principiilor *(alte organisme oficiale din SUA recunoscute de UE pot fi incluse într-o anexă viitoare)*; (b) să își declare în mod public angajamentul de a respecta principiile; (c) să își facă publice politicile de confidențialitate în conformitate cu aceste principii; și (d) să le pună pe deplin în aplicare. Nerespectarea principiilor de către o organizație este executorie în temeiul secțiunii 5 din Legea privind Comisia Federală pentru Comerț, care interzice practicile neloiale sau frauduloase în domeniul comerțului sau care afectează comerțul [15 U.S.C § 45 (a)] sau în temeiul altor acte cu putere de lege care interzic astfel de acte.

3. Departamentul Comerțului va menține și va pune la dispoziția publicului o listă oficială a organizațiilor din Statele Unite ale Americii care au prezentat Departamentului autocertificarea și și-au declarat angajamentul de a adera la principii (denumită în continuare „lista Scutului de confidențialitate"). Beneficiile Scutului de confidențialitate sunt asigurate de la data la care Departamentul include organizația pe lista Scutului de confidențialitate. Departamentul va elimina o organizație de pe lista Scutului de confidențialitate în cazul în care aceasta se retrage în mod voluntar de la Scutul de confidențialitate sau în cazul în care nu își finalizează recertificarea anuală la Departament. Eliminarea organizației de pe lista Scutului de confidențialitate înseamnă că aceasta nu mai poate beneficia de decizia Comisiei Europene privind caracterul adecvat pentru a primi informații cu caracter personal din UE. Organizația trebuie să continue să aplice principiile în cazul informațiilor cu caracter personal primite în perioada în care aceasta a participat la Scutul de confidențialitate și își prezintă anual angajamentul față de Departament în acest sens, atât timp cât aceasta păstrează informațiile respective; în caz contrar, organizația trebuie să returneze sau să șteargă informațiile sau să ofere protecție „adecvată" pentru informații prin alte mijloace autorizate. De asemenea, Departamentul va elimina din lista Scutului de confidențialitate organizațiile care încalcă în mod sistematic principiile; aceste organizații nu se califică pentru beneficiile Scutului de confidențialitate și trebuie să returneze sau să șteargă datele cu caracter personal pe care le-au primit în cadrul Scutului de confidențialitate.

4. De asemenea, Departamentul va menține și va pune la dispoziția publicului un registru oficial al organizațiilor din SUA care și-au prezentat anterior Departamentului autocertificarea, dar care au fost eliminate din lista Scutului de confidențialitate. Departamentul va furniza un avertisment clar că aceste organizații nu participă la Scutul de

([1]) Cu condiția ca Decizia Comisiei privind caracterul adecvat al protecției oferite de Scutul de confidențialitate UE-SUA să se aplice Islandei, Liechtensteinului și Norvegiei, pachetul privind Scutul de confidențialitate va acoperi atât Uniunea Europeană, cât și aceste trei țări. În consecință, trimiterile la UE și statele sale membre vor fi interpretate ca incluzând Islanda, Liechtenstein și Norvegia.

confidențialitate; că eliminarea de pe lista Scutului de confidențialitate înseamnă că organizațiile nu pot pretinde că respectă Scutul de confidențialitate și trebuie să evite orice declarații sau practicile înșelătoare care ar sugera că acestea participă la Scutul de confidențialitate; și că organizațiile respective nu mai au dreptul de a beneficia de decizia Comisiei Europene privind caracterul adecvat, care le-ar permite acestora să primească date cu caracter personal din UE. O organizație care continuă să pretindă că participă la Scutul de confidențialitate sau face alte declarații false legate de Scutul de confidențialitate după ce aceasta a fost eliminată din lista Scutului de confidențialitate poate face obiectul unor măsuri de asigurare a respectării luate de către FTC, Departamentul Transporturilor sau alte autorități de aplicare a legii.

5. Aderarea la aceste principii poate fi limitată de: (a) cerințele privind securitatea națională, interesul public și respectarea legilor Statelor Unite ale Americii; (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; (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.

6. Organizațiile sunt obligate să aplice principiile pentru toate datele cu caracter personal transferate în legătură cu Scutul de confidențialitate ulterior aderării lor la Scutul de confidențialitate. Organizațiile care doresc să extindă avantajele Scutului de confidențialitate la informațiile cu caracter personal obținute din fișiere de tip „resurse umane" provenind din Uniunea Europeană pentru a le utiliza în cadrul unui raport de muncă trebuie să menționeze această intenție atunci când își autocertifică angajamentul la Departament și trebuie să se conformeze cerințelor stabilite în principiul suplimentar privind autocertificarea.

7. Se aplică legislația americană în ceea ce privește chestiunile de interpretare și respectare a principiilor și a politicilor de confidențialitate relevante puse în aplicare de organizațiile care aderă la Scutul de confidențialitate, cu excepția cazurilor în care organizațiile s-au angajat să coopereze cu autoritățile europene pentru protecția datelor (APD). Cu excepția cazului în care se prevede altfel, toate dispozițiile din principii se aplică în măsura în care acestea sunt relevante.

8. Definiții:

   a. „date cu caracter personal" și „informații cu caracter personal" înseamnă informațiile referitoare la o persoană fizică identificată sau identificabilă care intră în domeniul de aplicare a directivei, primite de o organizație din Statele Unite din Uniunea Europeană și înregistrate sub orice formă;

   b. „prelucrarea" datelor cu caracter personal înseamnă orice operațiune sau set de operațiuni care se efectuează asupra datelor cu caracter personal, indiferent dacă este efectuată sau nu prin mijloace automate, precum colectarea, înregistrarea, organizarea, stocarea, adaptarea sau modificarea, recuperarea, consultarea, utilizarea, divulgarea sau diseminarea, ștergerea sau distrugerea;

   c. „operator" înseamnă o persoană sau o organizație care, singur sau împreună cu alte persoane, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal.

9. Data intrării în vigoare a acestor principii este data aprobării finale a deciziei Comisiei Europene privind caracterul adecvat.

II. PRINCIPII

1. **Notificarea**

   a. O organizație trebuie să informeze persoanele cu privire la:

      i. participarea sa la Scutul de confidențialitate și să comunice un link sau adresa de internet pentru lista Scutului de confidențialitate,

      ii. tipurile de date cu caracter personal colectate și, dacă este cazul, entitățile sau filialele organizației care aderă, de asemenea, la principii,

iii. angajamentul său de a supune principiilor toate datele cu caracter personal primite din partea UE în legătură cu Scutul de confidențialitate,

iv. scopurile pentru care colectează sau utilizează informațiile cu caracter personal despre aceștia,

v. modul în care pot contacta organizația pentru orice întrebări sau plângeri, inclusiv la orice unitate din UE, care să poată răspunde la astfel de solicitări de informații și reclamații,

vi. tipul sau identitatea părților terțe cărora le comunică informații cu caracter personal și scopurile pentru care face acest lucru,

vii. dreptul persoanelor de a avea acces la datele lor personale,

viii. opțiunile și mijloacele pe care organizația le oferă persoanelor pentru limitarea utilizării și divulgării datelor lor cu caracter personal,

ix. organismul independent de soluționare a reclamațiilor desemnat pentru a soluționa plângeri și pentru a oferi persoanei respective căi de atac adecvate în mod gratuit, precum și dacă acesta este: (1) grupul special constituit de autoritățile pentru protecția datelor, (2) un sistem alternativ de soluționare a diferendelor furnizor cu sediul în UE sau (3) un sistem alternativ de soluționare a litigiilor cu sediul în Statele Unite,

x. că face obiectul competențelor de investigare și de asigurare a executării ale FTC, ale Departamentului Transporturilor sau ale oricărui alt organism de reglementare autorizat din Statele Unite ale Americii,

xi. posibilitatea, în anumite condiții, ca o persoană să invoce un arbitraj obligatoriu,

xii. cerința de a dezvălui informații cu caracter personal ca răspuns la solicitări legale formulate de către autorități publice, inclusiv pentru respectarea cerințelor privind securitatea națională sau respectarea legilor, și

xiii. răspunderea sa în cazuri de transferuri ulterioare către terți.

b. Notificarea trebuie formulată într-un limbaj clar și lizibil. Notificarea trebuie comunicată persoanelor în cauză atunci când acestea sunt invitate pentru prima dată să furnizeze informații cu caracter personal sau cât mai curând posibil după această invitație, dar, în orice caz, înainte ca datele să fie folosite într-un scop diferit de cel pentru care au fost inițial colectate sau prelucrate de organizația care a efectuat transferul sau înainte să fie comunicate pentru prima dată unui terț.

2. **Opțiunea**

a. Orice organizație trebuie să ofere persoanelor în cauză posibilitatea de a decide dacă (refuza ca) informațiile lor cu caracter personal (i) să poată fi divulgate unui terț sau (ii) să poată fi utilizate într-un scop incompatibil cu scopul sau scopurile pentru care au fost inițial colectate sau într-un scop aprobat ulterior de persoanele în cauză. Persoanele în cauză trebuie să dispună de mecanisme clare, vizibile și ușor accesibile pentru a-și exercita opțiunea.

b. Prin derogare de la punctul anterior, nu este necesar să se prevadă opțiuni atunci când informațiile sunt transmise către o parte terță care acționează ca agent pentru a îndeplini sarcina (sarcinile) în numele și pe baza instrucțiunilor organizației. Cu toate acestea, o organizație trebuie să încheie un contract cu agentul.

c. În ceea ce privește informațiile sensibile (de exemplu, datele privind dosarul medical sau starea de sănătate a unei persoane, originea rasială sau etnică, opiniile politice, credințele religioase sau convingerile filosofice, apartenența sindicală sau orientarea sexuală a persoanei respective), organizațiile trebuie să obțină consimțământul explicit (consimțământ) de la persoanele fizice dacă astfel de informații urmează să fie (i) divulgate unui terț sau (ii) utilizate într-un scop care diferă de obiectivul inițial pentru care au fost colectate sau într-un scop aprobat ulterior de persoana în cauză prin exercitarea dreptului de consimțământ. În plus, o organizație va considera drept informații sensibile orice informații cu caracter personal primite de la un terț în cazul în care terțul arată că aceste informații sunt sensibile și le tratează în consecință.

3. **Responsabilitatea pentru transferul ulterior**

a. Pentru a transfera date cu caracter personal către un terț care acționează în calitate de operator, organizațiile trebuie să respecte principiile notificării și opțiunii. Organizațiile trebuie să încheie un contract cu operatorul terț care prevede că astfel de date pot fi prelucrate doar în scopuri specifice și limitate în conformitate cu consimțământul acordat de către persoana în cauză și că beneficiarul va asigura același nivel de protecție ca principiile și va transmite o notificare organizației în cazul în care constată că nu mai poate îndeplini această obligație. Contractul stipulează că, în cazul în care concluzia unei astfel de analize se efectuează terț operator încetează prelucrarea sau ia alte măsuri adecvate și rezonabile pentru a remedia.

b. Pentru a transfera date cu caracter personal către un terț care acționează ca agent, organizațiile trebuie: (i) să transfere aceste date numai pentru scopuri specificate și limitate; (ii) să confirme faptul că agentul este obligat să asigure cel puțin același nivel de protecție a vieții private în conformitate cu principiile; (iii) să ia măsuri rezonabile și adecvate pentru a se asigura că agentul prelucrează în mod eficient informațiile cu caracter personal transferate într-un mod compatibil cu obligațiile organizației care îi revin în temeiul principiilor; (iv) să prevadă că agentul trebuie să transmită o notificare organizației în cazul în care constată că nu își mai poate îndeplini obligația de a furniza același nivel de protecție ca cel impus de principii; (v) în urma notificării, inclusiv în conformitate cu (iv), să ia măsuri rezonabile și adecvate pentru a opri și remedia prelucrarea neautorizată; și (vi) să furnizeze Departamentului, la cerere, un rezumat sau o copie reprezentativă a dispozițiilor de confidențialitate relevante ale contractului cu agentul respectiv.

4. **Securitate**

a. Organizațiile care creează, mențin, utilizează sau difuzează date cu caracter personal trebuie să ia măsuri rezonabile și adecvate pentru a preveni pierderea, utilizarea abuzivă, consultarea neautorizată, divulgarea, modificarea și distrugerea acestor date, ținând seama în mod corespunzător de riscurile pe care le presupune prelucrarea și natura datelor cu caracter personal.

5. **Integritatea datelor și limitarea scopului**

a. Ținând seama de aceste principii, informațiile cu caracter personal trebuie să se limiteze la informații care sunt relevante pentru scopul prelucrării ([1]). O organizație nu poate prelucra date cu caracter personal într-un mod incompatibil cu scopul pentru care acestea au fost colectate sau cu scopurile aprobate ulterior de persoana în cauză. În limita acestor obiective, orice organizație trebuie să ia măsurile necesare pentru a asigura fiabilitatea datelor în raport cu utilizarea prevăzută, precum și acuratețea, exhaustivitatea și actualitatea acestora. O organizație trebuie să adere la principii, atât timp cât aceasta păstrează informațiile respective.

b. Informațiile pot fi păstrate într-o formă care identifică sau permite identificarea persoanei ([2]) numai în măsura în care servește la atingerea obiectivului de prelucrare în sensul punctului 5a. Această obligație nu împiedică organizațiile să prelucreze informații cu caracter personal pe perioade mai lungi și în măsura în care o astfel de prelucrare servește în mod rezonabil la atingerea scopurilor de arhivare în interes public sau în scopuri legate de jurnalism, literatură și artă, știință sau cercetare istorică și de analiză statistică. În aceste cazuri, o astfel de prelucrare este supusă celorlalte principii și dispoziții ale cadrului. Organizațiile vor trebui să ia măsuri rezonabile și adecvate în ceea ce privește respectarea acestei dispoziții.

6. **Accesul**

a. Persoanele trebuie să aibă acces la informațiile cu caracter personal pe care o organizație le deține în legătură cu ele și să le poată corecta, modifica sau șterge atunci când sunt incorecte sau au fost prelucrate cu încălcarea principiilor, cu excepția cazurilor în care eforturile sau costurile ocazionate de acordarea dreptului de acces sunt disproporționate în raport cu riscurile pe care le creează pentru viața privată a persoanei în cauză sau a cazurilor în care ar fi încălcate drepturile altor persoane.

([1]) În funcție de circumstanțe, printre exemplele de scopuri de prelucrare compatibile sunt cele care pot servi, în mod rezonabil, la atingerea obiectivelor legate de relațiile cu clienții, respectarea reglementării și considerații de ordin juridic, de audit, de securitate și de prevenire a fraudei, de conservarea și apărarea a drepturilor juridice ale organizației sau a altor scopuri care sunt conforme cu așteptările unei persoane rezonabile, având în vedere contextul în care sunt colectate.

([2]) În acest context, în cazul în care, ținând seama de mijloacele de identificare care pot fi utilizate în mod rezonabil (luând în considerare, printre altele, costurile și intervalul de timp necesare pentru identificare și tehnologia disponibilă la momentul prelucrării) și forma sub care datele sunt păstrate, o persoană ar putea să fie identificată în mod rezonabil de organizație sau de un terț în cazul în care ar avea acces la date, se poate considera că persoana este „identificabilă”.

7. **Posibilitatea de recurs, aplicarea și responsabilitatea**

a. Pentru o protecție eficientă a vieții private, trebuie puse la punct mecanisme solide care să permită asigurarea respectării principiilor, posibilitatea de recurs pentru persoanele care au fost afectate de nerespectarea principiilor și de sancționare a organizațiilor care nu au respectat principiile. Aceste mecanisme trebuie să includă cel puțin:

i. mecanisme independente de recurs, ușor accesibile care să permită investigarea și soluționarea în mod rapid și gratuit a oricăror plângeri și litigii făcând trimitere la principii și acordarea de despăgubiri în cazurile prevăzute de legea aplicabilă sau de inițiativele din sectorul privat;

ii. proceduri de monitorizare pentru verificarea exactității informațiilor și indicațiilor pe care organizațiile le furnizează cu privire la practicile lor în ceea ce privește protecția vieții private și pentru verificarea punerii în aplicare a acestor practici în conformitate cu declarațiile acestora și, în special, cu privire la cazurile de nerespectare; și

iii. declarații care obligă organizațiile care subscriu la principii să soluționeze problemele care rezultă din nerespectarea principiilor și declarații care prevăd sancțiuni pentru contravenienți. Astfel de sancțiuni trebuie să fie suficient de severe pentru a garanta respectarea principiilor.

b. Organizațiile și mecanismele independente de recurs selectate răspund cu promptitudine la solicitările și cererile formulate de Departament pentru informații referitoare la Scutul de confidențialitate. Toate organizațiile trebuie să răspundă rapid plângerilor referitoare la respectarea principiilor menționate de autoritățile statelor membre ale UE prin intermediul Departamentului. Organizațiile care au ales să coopereze cu autoritățile pentru protecția datelor, inclusiv organizațiile care prelucrează datele privind resursele umane, trebuie să răspundă în mod direct acestor autorități în ceea ce privește investigarea și soluționarea plângerilor.

c. Organizațiile sunt obligate să supună plângerile arbitrajului și să respecte condițiile stabilite în anexa I, cu condiția ca persoana în cauză să fi invocat arbitrajul obligatoriu prin notificarea organizației în cauză și în conformitate cu procedurile și în condițiile prevăzute în anexa I.

d. În contextul unui transfer ulterior, o organizație care aderă la Scutul de confidențialitate este responsabilă pentru prelucrarea datelor cu caracter personal pe care le primește în temeiul Scutului de confidențialitate și pe care le transferă ulterior către un terț care acționează ca agent în numele său. Organizația care aderă la Scutul de confidențialitate rămâne răspunzătoare în conformitate cu principiile în cazul în care agentul prelucrează astfel de informații cu caracter personal într-un mod incompatibil cu principiile, cu excepția cazului în care organizația dovedește că nu este responsabilă pentru fapta care a provocat prejudiciul.

e. În cazul în care o organizație face obiectul unui ordin FTC sau al unei hotărâri judecătorești pe baza neconformității, organizația pune la dispoziția publicului orice secțiuni relevante cu privire la Scutul de confidențialitate din orice raport de conformitate sau de evaluare transmis către FTC, în măsura în care respectă cerințele de confidențialitate. Departamentul a instituit un punct de contact pentru autoritățile pentru protecția datelor pentru orice încălcări ale conformității de către organizații care aderă la Scutul de confidențialitate. FTC va acorda prioritate cazurilor de nerespectare a principiilor primite de la Departament și autoritățile statelor membre ale UE și va face schimb de informații cu privire la sesizări cu autoritățile de stat de trimitere în timp util, sub rezerva restricțiilor de confidențialitate existente.

III. PRINCIPII SUPLIMENTARE

1. **Date sensibile**

a. O organizație nu este obligată să obțină consimțământul explicit (acordul) cu privire la datele sensibile atunci când prelucrarea:

i. este în interesul vital al persoanei vizate sau al unei alte persoane;

ii. este necesară pentru stabilirea unui drept sau a unei apărări în justiție;

iii. este necesară în vederea acordării îngrijirii medicale sau a stabilirii unui diagnostic;

iv. este efectuată în cadrul activităților legitime de către o fundație, o asociație sau orice alt organism cu scop nelucrativ și cu un obiectiv politic, filosofic, religios sau sindical și cu condiția ca prelucrarea să privească exclusiv membrii acestui organism sau persoanele care au contacte frecvente cu acesta în legătură cu scopurile sale, iar datele să nu fie comunicate unor terți fără consimțământul persoanelor în cauză;

v. este necesară pentru respectarea obligațiilor organizației în domeniul dreptului muncii; sau

vi. are legătură cu date care sunt în mod clar făcute publice de către persoana în cauză.

2. **Excepțiile jurnalistice**

a. Ținând seama de garanțiile pe care le oferă Constituția Statelor Unite ale Americii în ceea ce privește libertatea presei și derogările din directivă cu privire la informațiile utilizate de jurnaliști, atunci când drepturile presei menționate la primul amendament al Constituției Statelor Unite ale Americii nu sunt compatibile cu protecția vieții private, primul amendament trebuie să reglementeze activitățile cetățenilor americani sau ale organizațiilor din Statele Unite ale Americii.

b. Informațiile cu caracter personal care sunt colectate în vederea publicării, difuzării sau comunicării publice prin alte forme, indiferent dacă sunt sau nu utilizate, precum și informațiile care au fost publicate anterior și apoi arhivate nu sunt supuse principiilor Scutului de confidențialitate.

3. **Responsabilitatea secundară**

a. Furnizorii de servicii de internet (FSI), societățile de telecomunicații și alte organizații nu sunt răspunzătoare în conformitate cu principiile Scutului de confidențialitate în numele altei organizații atunci când acestea se limitează la transmiterea, direcționarea, înlocuirea sau mascarea informațiilor. La fel ca în cazul directivei, Scutul de confidențialitate nu creează o responsabilitate secundară. În măsura în care un organism funcționează doar ca vector pentru datele transmise de terți și nu stabilește nici obiectivele și nici mijloacele de prelucrare a acestor date cu caracter personal, responsabilitatea sa nu este angajată.

4. **Efectuarea unor verificări prealabile și desfășurarea de audituri**

a. Activitățile auditorilor și ale băncilor de investiții pot presupune prelucrarea de date cu caracter personal fără consimțământul sau cunoștința persoanei. Acest lucru este permis de principiile notificării, opțiunii și accesului în circumstanțele descrise mai jos.

b. Societățile publice pe acțiuni și societățile cu număr redus de acționari, inclusiv organizațiile care aderă la Scutul de confidențialitate, fac în mod regulat obiectul unor audituri. Astfel de audituri, în special cele privind posibile nereguli, pot fi puse în pericol în cazul în care sunt dezvăluite prematur. În mod similar, o organizație care aderă la Scutul de confidențialitate implicată într-o potențială fuziune sau preluare va trebui să efectueze sau să facă obiectul unei revizuiri de verificare prealabilă. Adesea, acest lucru presupune colectarea și prelucrarea de date cu caracter personal, cum ar fi informațiile cu privire la cadrele superioare și la alți membri importanți ai personalului. Divulgarea prematură ar putea împiedica tranzacția sau chiar încălca reglementările aplicabile în cazul valorilor mobiliare. Băncile de investiții și avocații implicați în efectuarea unei verificări prealabile sau auditorii care efectuează un audit pot prelucra informații fără cunoștința persoanei în cauză numai în măsura și pe perioada necesară îndeplinirii dispozițiilor de reglementare sau a cerințelor legate de interesul general, precum și în alte circumstanțe în care aplicarea acestor principii ar aduce atingere intereselor legitime ale organizației. Aceste interese legitime includ supravegherea respectării de către societățile comerciale a obligațiilor lor legale, a activităților lor contabile legitime și a confidențialității care trebuie să fie asigurată în contextul eventualelor achiziții, fuziuni, asociații în participațiune sau al altor tranzacții similare efectuate de băncile de investiții sau de auditori.

5. **Rolul autorităților însărcinate cu protecția datelor**

a. Organizațiile vor pune în aplicare angajamentul de a coopera cu autoritățile însărcinate cu protecția datelor din Uniunea Europeană („APD"), după cum se descrie mai jos. În temeiul Scutului de confidențialitate, organizațiile din Statele Unite ale Americii care primesc date cu caracter personal din Uniunea Europeană trebuie să își ia angajamentul de a utiliza mecanisme eficiente pentru a garanta respectarea principiilor Scutului de confidențialitate. Mai exact, astfel cum prevede principiul recursului, punerii în aplicare și responsabilității, organizațiile participante trebuie să prevadă: (a)(i) căi de recurs pentru persoanele la care se referă datele; (a)(ii) proceduri de urmărire pentru verificarea veridicității afirmațiilor și declarațiilor pe care le fac organizațiile cu privire la respectarea vieții private; și (a)(iii) dispoziții privind condițiile în care organizațiile trebuie să remedieze problemele care decurg din nerespectarea principiilor, precum și asumarea consecințelor care rezultă din aceasta. O organizație trebuie să îndeplinească punctele (a)(i) și (a)(iii) din principiul recursului, punerii în aplicare și responsabilității în cazul în care aderă la cerințele stabilite aici pentru cooperarea cu autoritățile pentru protecția datelor.

b. O organizație își ia angajamentul de a coopera cu autoritățile pentru protecția datelor declarând în autocertificarea sa de aderare la Scutul de confidențialitate adresată Departamentului Comerțului (a se vedea principiul suplimentar privind autocertificarea) că organizația:

i. decide să îndeplinească cerințele de la punctele (a)(i) și (a)(iii) din principiul Scutului de confidențialitate privind recursul, punerea în aplicare și responsabilitatea, luându-și angajamentul de a coopera cu APD;

ii. va coopera cu APD la analizarea și soluționarea plângerilor înaintate în temeiul Scutului de confidențialitate; și

iii. va respecta orice aviz emis de APD conform căruia organizația trebuie să adopte măsuri specifice în vederea respectării principiilor Scutului de confidențialitate, inclusiv măsuri de despăgubire sau reparație în beneficiul persoanelor afectate de nerespectarea principiilor, și va informa APD în scris cu privire la măsurile adoptate în acest sens.

c. Funcționarea comitetelor APD

i. Cooperarea autorităților pentru protecția datelor se traduce prin informații și avize acordate după cum urmează:

1. APD vor fi consultate prin intermediul unui comitet neoficial al APD înființat la nivel european care, *inter alia*, va contribui la elaborarea unei abordări armonizate și coerente;

2. comitetul va oferi consiliere organizațiilor din Statele Unite ale Americii cu privire la plângerile nesoluționate din partea unor persoane privind prelucrarea informațiilor cu caracter personal care au fost transferate din Uniunea Europeană în temeiul Scutului de confidențialitate. Consilierea are ca obiectiv asigurarea unei aplicări corecte a principiilor Scutului de confidențialitate și privește, de asemenea, mecanismele de reglementare a litigiilor pe care APD le consideră corespunzătoare pentru persoana (persoanele) în cauză;

3. comitetul își va da avizul ca răspuns la sesizările organizațiilor în cauză și/sau la plângerile introduse direct de persoane fizice împotriva organizațiilor care și-au luat angajamentul de a coopera cu APD în sensul respectării principiilor Scutului de confidențialitate, încurajând și sprijinind, după caz, aceste persoane fizice să utilizeze mai întâi mecanismele interne de tratare a plângerilor pe care le oferă organizația;

4. avizul va fi emis numai după ce ambele părți au avut posibilitatea de a-și prezenta observațiile și, după caz, de a aduce toate dovezile pe care doresc să le prezinte. Comitetul va urmări să emită avizul cât mai repede posibil, respectând totodată principiile procesului echitabil. În principiu, comitetul se va pronunța în termen de cel mult 60 de zile de la primirea plângerii sau a sesizării și mai repede, atunci când este posibil;

5. în cazul în care consideră necesar, comitetul va face publice rezultatele analizelor plângerilor care îi sunt înaintate;

6. avizul comitetului nu creează obligații pentru comitet sau pentru oricare dintre APD.

ii. Astfel cum s-a menționat mai sus, organizațiile care optează pentru acest mod de soluționare a litigiilor trebuie să-și ia angajamentul de a se conforma avizului emis de APD. În cazul în care o organizație nu se conformează în termen de 25 de zile de la notificarea avizului și nu oferă o explicație satisfăcătoare, comitetul ar putea decide să înainteze cazul către Comisia Federală pentru Comerț, Departamentul Transporturilor sau un alt organism de reglementare de stat sau federal din Statele Unite ale Americii cu competențe statutare să ia măsuri de asigurare a respectării în cazuri de înșelăciune sau declarații false sau să constate că angajamentul de cooperare a fost grav încălcat și, prin urmare, trebuie considerat nul și neavenit. În acest ultim caz, comitetul informează Departamentul Comerțului, astfel încât lista participanților la Scutul de confidențialitate să poată fi modificată în consecință. Orice încălcare a angajamentului de cooperare cu comitetul, precum și orice nerespectare a principiilor Scutului de confidențialitate se consideră elemente constitutive ale unui act fraudulos în temeiul articolului 5 din Federal Trade Commission Act sau în temeiul unui text legislativ similar.

d. O organizație care dorește ca beneficiile Scutului de confidențialitate să acopere date privind resursele umane transferate din UE în contextul unui raport de muncă trebuie să își asume angajamentul de a coopera cu APD în ceea ce privește astfel de date (a se vedea principiul suplimentar privind date referitoare la resursele umane).

e. Organizațiile care optează pentru această formulă trebuie să plătească o cotizație anuală care să acopere costurile de gestionare ale comitetului și, după caz, vor fi invitate să participe la costurile pentru traducerile pe care le presupune analizarea de către comitet a acțiunilor și plângerilor depuse împotriva lor. Cotizația anuală nu poate depăși 500 USD, iar în cazul societăților comerciale mai mici se acordă o reducere.

6. **Autocertificarea**

a. Beneficiile Scutului de confidențialitate sunt asigurate de la data la care Departamentul a introdus declarația de autocertificare a organizației pe lista Scutului de confidențialitate, după ce a hotărât că aceasta este completă.

b. Pentru autocertificarea aderării la Scutul de confidențialitate, o organizație trebuie să prezinte Departamentului o declarație de autocertificare, semnată de un funcționar al organizației care aderă la Scutul de confidențialitate, care trebuie să conțină cel puțin următoarele informații:

i. numele organizației, adresa poștală, adresa electronică, numerele de telefon și de fax ale acesteia;

ii. descrierea activităților organizației cu privire la informațiile cu caracter personal primite din Uniunea Europeană; și

iii. descrierea politicii de confidențialitate a organizației cu privire la informațiile cu caracter personal menționate anterior, precizând:

1. în cazul în care organizația dispune de un site internet public, adresa web la care este disponibilă politica de confidențialitate sau, în cazul în care organizația nu dispune de un site internet public, locul în care textul acestor dispoziții poate fi consultat de către public;

2. data punerii în aplicare a acestor dispoziții;

3. serviciul care poate fi contactat pentru soluționarea plângerilor, pentru cererile de acces sau pentru orice altă problemă legată de Scutul de confidențialitate;

4. denumirea instanței de reglementare specifice care este însărcinată să hotărască în privința plângerilor depuse, după caz, împotriva organizației pentru practici neloiale sau frauduloase și pentru încălcări ale legilor sau reglementărilor privind protecția vieții private (și care este menționată în principii sau într-o viitoare anexă la principii);

5. numele oricărui program privind protecția vieții private la care participă organizația;

6. metoda de verificare (de exemplu, internă sau printr-un terț) (a se vedea principiul suplimentar de verificare); și

7. instanța independentă de recurs care poate ancheta plângerile nesoluționate.

c. În cazul în care o organizație dorește să extindă avantajele Scutului de confidențialitate la informații de tip „resurse umane” transferate din UE pentru a fi utilizate în cadrul raporturilor de muncă, aceasta poate face acest lucru atunci când una dintre instanțele de reglementare menționate în principii sau într-o viitoare anexă la principii are competența de a ancheta plângerile depuse împotriva organizației care rezultă din prelucrarea informațiilor privind resursele umane. Pe lângă aceasta, organizația trebuie să indice în scrisoarea sa de autocertificare că dorește acest lucru și că se angajează să coopereze cu autoritățile competente ale Uniunii Europene în conformitate cu principiile suplimentare cu privire la datele privind resursele umane și rolul autorităților de protecție a datelor și că se conformează sfaturilor date de aceste autorități. De asemenea, organizația trebuie să furnizeze Departamentului o copie a politicii sale de confidențialitate în materie de resurse umane și să precizeze unde poate fi consultat textul politicii de confidențialitate de către lucrătorii afectați.

d. Departamentul va păstra lista organizațiilor care aderă la Scutul de confidențialitate care prezintă scrisori de autocertificare complete, garantând astfel disponibilitatea avantajelor Scutului de confidențialitate, și va actualiza această listă pe baza scrisorilor de autocertificare și a notificărilor anuale primite în temeiul principiului suplimentar privind soluționarea litigiilor și punerea în aplicare a deciziilor. Aceste scrisori de autocertificare trebuie trimise cel puțin o dată pe an; în caz contrar, organizația va fi ștearsă de pe lista Scutului de confidențialitate și nu se vor mai asigura avantajele Scutului de confidențialitate. Atât lista Scutului de confidențialitate, cât și scrisorile de autocertificare prezentate de organizații vor fi făcute publice. Toate organizațiile care sunt incluse de departament în lista Scutului de confidențialitate trebuie, de asemenea, să indice în declarațiile lor publice referitoare la politica de confidențialitate faptul că aderă la principiile Scutului de confidențialitate. În cazul în

care este disponibilă online, politica de confidențialitate a unei organizații trebuie să includă un link către site-ul Scutului de confidențialitate al Departamentului, precum și un link către site-ul internet sau formularul de depunere a plângerii către instanța independentă de recurs care poate ancheta plângerile nesoluționate.

e. Principiile privind protecția vieții private se aplică imediat după certificare. Recunoscând faptul că principiile vor afecta relațiile comerciale cu terți, organizațiile care își certifică aderarea la cadrul privind Scutul de confidențialitate în primele două luni după data intrării în vigoare a cadrului aduc relațiile comerciale existente cu terții în conformitate cu principiul responsabilității pentru transferul ulterior cât mai curând posibil și, în orice caz, nu mai târziu de nouă luni de la data la care acestea aderă la Scutul de confidențialitate. În cursul acestei perioade intermediare, în cazul în care organizațiile transferă date către un terț, acestea (i) aplică principiile notificării și opțiunii și (ii) în cazul în care datele cu caracter personal sunt transferate către un terț care acționează ca agent, confirmă faptul că agentul este obligat să asigure cel puțin același nivel de protecție în conformitate cu principiile.

f. O organizație trebuie să aplice principiile Scutului de confidențialitate tuturor datelor cu caracter personal primite din UE în temeiul Scutului de confidențialitate. Angajamentul de aderare la principiile Scutului de confidențialitate nu este limitat în timp în ceea ce privește datele cu caracter personal primite în perioada în care organizația beneficiază de avantajele Scutului de confidențialitate. Angajamentul luat de o organizație înseamnă că aceasta va continua să aplice principiile în ceea ce privește datele respective pe toată perioada în care organizația le păstrează, le utilizează sau le divulgă, chiar dacă aceasta părăsește ulterior, dintr-un motiv sau altul, Scutul de confidențialitate. O organizație care își retrage angajamentul la Scutul de confidențialitate, dar dorește să păstreze astfel de date, trebuie să își afirme anual în fața Departamentului angajamentul de a continua să aplice principiile sau să furnizeze un nivel „adecvat" de protecție pentru informații prin alte mijloace autorizate (de exemplu, folosind un contract care reflectă pe deplin cerințele clauzelor contractuale standard relevante adoptate de către Comisia Europeană); în caz contrar, organizația trebuie să returneze sau să șteargă informațiile respective. O organizație care își retrage angajamentul la Scutul de confidențialitate trebuie să elimine din orice politică de confidențialitate relevantă orice trimiteri la Scutul de confidențialitate, care implică faptul că organizația continuă să participe activ la Scutul de confidențialitate și are dreptul să beneficieze de avantajele acestuia.

g. Atunci când o organizație încetează să existe ca persoană juridică distinctă, ca urmare a unei fuziuni sau absorbții, trebuie să notifice în prealabil acest lucru Departamentului. Notificarea trebuie, de asemenea, să indice dacă entitatea care o absoarbe sau entitatea care rezultă în urma fuziunii (i) rămâne supusă în continuare principiilor Scutului de confidențialitate în virtutea dispozițiilor juridice care reglementează absorbția sau fuziunea sau (ii) decide să-și autocertifice aderarea la principiile Scutului de confidențialitate sau oferă alte garanții, ca de exemplu un acord scris privind aderarea sa la aceste principii. În cazul în care nu este pusă în aplicare niciuna dintre soluțiile menționate la punctele (i) și (ii), orice date cu caracter personal care au fost obținute în cadrul Scutului de confidențialitate trebuie șterse fără întârziere.

h. Atunci când o organizație părăsește Scutul de confidențialitate, indiferent de motiv, aceasta trebuie să elimine toate declarațiile care implică faptul că organizația participă în continuare la Scutul de confidențialitate sau are dreptul la avantajele Scutului de confidențialitate. Dacă se utilizează marca de certificare a Scutului de confidențialitate, aceasta trebuie să fie eliminată de asemenea. Orice declarație falsă adresată publicului general cu privire la aderarea unei organizații la principiile Scutului de confidențialitate poate da naștere unei acțiuni intentate la Comisia Federală pentru Comerț sau altă instanță administrativă competentă. Orice declarație falsă adresată Departamentului poate da naștere unei acțiuni intentate în temeiul legii privind declarațiile false (18 U.S.C § 1001).

7. **Verificarea**

a. Organizațiile trebuie să prevadă proceduri de urmărire pentru a verifica dacă atestările și declarațiile întreprinderilor cu privire la practicile lor în ceea ce privește protecția vieții private în cadrul Scutului de confidențialitate sunt adevărate și dacă aceste practici au fost puse în aplicare în conformitate cu declarațiile acestora și cu principiile Scutului de confidențialitate.

b. Pentru a răspunde cerințelor de verificare a principiului recursului, punerii în aplicare și responsabilității, o organizație trebuie să verifice astfel de atestări și declarații prin organizarea unei autoevaluări sau a unui control extern al conformității.

c. În cadrul autoevaluării, verificarea trebuie să indice faptul că politica de confidențialitate a unei organizații în ceea ce privește informațiile cu caracter personal primite de la Uniunea Europeană, care este făcută publică de organizație, este exactă, completă, prezentată în mod vizibil, pusă în aplicare în totalitate și accesibilă. De asemenea, aceasta trebuie să arate că politica sa de confidențialitate este conformă cu principiile Scutului de confidențialitate; că persoanele sunt informate de existența mecanismelor interne de rezolvare a plângerilor și a mecanismelor independente prin intermediul cărora pot depune plângeri, că organizația dispune de proceduri de formare a angajaților în acest scop și de sancționare a acestora în cazul în care nu le respectă, și că există proceduri interne privind controlul obiectiv și periodic al respectării acestei politici. O declarație care verifică

autoevaluarea trebuie semnată cel puțin o dată pe an, de către un funcționar al organizației sau de un alt reprezentant autorizat al acesteia și trebuie pusă la dispoziția persoanelor în cauză la cerere sau în cadrul unei anchete ori al unei plângeri pentru neconformitate.

d. În cazul în care organizația optează pentru controlul extern al conformității, acest control trebuie să demonstreze că politica de confidențialitate cu privire la informațiile primite de la Uniunea Europeană respectă principiile Scutului de confidențialitate, că această politică este respectată și că persoanele sunt informate cu privire la mecanismele prin care își pot depune plângerile. Metodele de control pot include (listă neexhaustivă) un audit, o verificare aleatorie, utilizarea de „momeli" sau alte instrumente tehnologice, după caz. O declarație care confirmă că a fost efectuat un control extern al conformității trebuie semnată, cel puțin o dată pe an, de către cel care a efectuat controlul, de către responsabilul organizației sau de către orice alt reprezentat al acesteia și trebuie transmisă, la cerere, persoanelor în cauză sau în cadrul unei anchete ori al unei reclamații pentru neconformitate.

e. Organizațiile trebuie să păstreze arhive privind punerea în aplicare a practicilor lor cu privire la protecția vieții private în cadrul Scutului de confidențialitate și să le pună la dispoziție, la cerere, organismului independent însărcinat cu analizarea reclamațiilor sau agenției cu competență în materie de practici neloiale și frauduloase, în cadrul unei anchete sau al unei plângeri pentru neconformitate. De asemenea, organizațiile trebuie să răspundă prompt la solicitările de informații și la alte cereri din partea Departamentului legate de aderarea organizației la principii.

8. **Accesul**

a. Principiul accesului în practică

i. În conformitate cu principiile Scutului de confidențialitate, dreptul de acces este fundamental pentru protecția vieții private. Acesta permite fiecărei persoane să verifice acuratețea informațiilor care o privesc. Principiul accesului înseamnă că orice persoană are dreptul:

1. de a obține confirmarea din partea unei organizații dacă organizația prelucrează sau nu date cu caracter personal care le privesc ([1]);

2. de a li se comunica aceste date, astfel încât să poată verifica exactitatea acestora și legalitatea prelucrării; și

3. de a corecta, a modifica sau a șterge datele, în cazul în care acestea sunt inexacte sau sunt prelucrate cu încălcarea acestor principii.

ii. Nimeni nu este obligat să justifice o cerere de acces cu privire la propriile date. Atunci când răspund cererilor de acces ale persoanelor, organizațiile trebuie, înainte de toate, să fie ghidate de motivul (motivele) solicitării. De exemplu, în cazul în care o cerere de acces este vagă sau extrem de amplă, organizația poate iniția un dialog cu solicitantul pentru a înțelege mai bine motivele acestui demers și pentru a găsi informațiile pertinente. Organizația poate încerca să stabilească cu care din serviciile organizației a avut contacte persoana în cauză și/sau care este natura sau utilizarea informațiilor care fac obiectul cererii de acces.

iii. Întrucât dreptul la acces este un element fundamental al protecției vieții private, organizațiile trebuie să facă întotdeauna eforturi de bună credință pentru a furniza accesul. De exemplu, în cazul în care anumite informații trebuie protejate și pot fi separate cu ușurință de alte informații cu caracter personal care fac obiectul unei cereri de acces, organizația trebuie să separe datele confidențiale și să pună la dispoziție celelalte informații. În cazul în care organizația decide să refuze accesul într-un anumit caz, aceasta trebuie să își motiveze decizia și să comunice datele unei persoane de contact pentru informații suplimentare.

b. Eforturile sau costurile ocazionate de acordarea dreptului de acces

i. Dreptul de acces la datele cu caracter personal poate fi limitat în împrejurări excepționale în care ar fi încălcate drepturile legitime ale persoanelor, altele decât cele vizate, sau în cazul în care eforturile sau costurile ocazionate de acordarea dreptului de acces ar fi disproporționate în raport cu riscurile la adresa vieții private a persoanei în cauză. Costurile și dificultatea sunt factori importanți care trebuie luați în considerare, dar care nu au un rol decisiv în stabilirea caracterului rezonabil al accesului.

([1]) Organizația ar trebui să răspundă solicitărilor din partea unei persoane fizice în ceea ce privește scopurile prelucrării, categoriile de date cu caracter personal vizate și destinatarii sau categoriile de destinatari cărora le sunt divulgate datele cu caracter personal.

ii. De exemplu, în cazul în care informațiile cu caracter personal sunt utilizate în scopul luării unor decizii care vor avea consecințe importante asupra persoanei în cauză (de exemplu, refuzarea sau acordarea unor avantaje importante precum o asigurare, o ipotecă sau un loc de muncă), în concordanță cu celelalte dispoziții ale acestor principii suplimentare, organizația trebuie să comunice aceste informații, chiar dacă acest lucru este destul de dificil sau presupune costuri ridicate. În cazul în care datele cu caracter personal solicitate nu sunt sensibile sau nu sunt utilizate pentru decizii care vor afecta în mod semnificativ persoana în cauză, dar sunt ușor accesibile și nu presupun costuri ridicate, o organizație ar trebui să ofere acces la aceste informații.

c. Informații comerciale confidențiale

i. Informațiile comerciale confidențiale sunt informații cu privire la care o organizație a luat măsuri să nu fie divulgate deoarece ar favoriza concurenții săi de pe piață. Organizațiile pot refuza sau limita accesul în cazul în care acordarea acestuia ar conduce la divulgarea propriilor sale informații comerciale confidențiale, cum ar fi concluziile sau clasificările comerciale stabilite de organizație, sau a informațiilor comerciale confidențiale aparținând altor organizații, în cazul în care aceste informații fac obiectul unei obligații contractuale de confidențialitate.

ii. În cazul în care informațiile comerciale confidențiale pot fi separate ușor de informațiile cu caracter personal care fac obiectul unei cereri de acces, organizația ar trebui să separe datele comerciale confidențiale și să pună la dispoziție informațiile neconfidențiale.

d. Organizarea bazelor de date

i. Accesul poate fi furnizat sub forma unui transfer de informații cu caracter personal relevante efectuat de organizație către persoana în cauză și nu implică obligatoriu consultarea bazei de date a organizației.

ii. Accesul trebuie furnizat numai în măsura în care organizația stochează informațiile cu caracter personal. Principiul accesului în sine nu creează nicio obligație de conservare, gestionare, reorganizare sau restructurare a fișierelor care cuprind informații cu caracter personal.

e. Cazul în care accesul poate fi restricționat

i. Întrucât organizațiile trebuie să depună întotdeauna eforturi de bună credință pentru a acorda acces persoanelor la datele lor cu caracter personal, circumstanțele în care organizațiile pot restricționa accesul sunt limitate, iar motivele pentru restricționarea accesului trebuie să fie specifice. În temeiul directivei, organizația poate refuza accesul la anumite informații în măsura în care difuzarea acestora riscă să aducă atingere unor importante interese publice, cum ar fi siguranța națională, apărarea sau siguranța publică. În plus, atunci când informațiile cu caracter personal sunt prelucrate exclusiv în scopuri statistice sau de cercetare, accesul poate fi refuzat. Alte motive pentru refuzarea sau restricționarea accesului:

1. o barieră în calea executării sau a aplicării legii, inclusiv în calea prevenirii criminalității, a detectării și anchetării infracțiunilor și delictelor sau a dreptului la un proces echitabil;

2. divulgarea informațiilor în cazul în care ar fi încălcate drepturile legitime sau interesele importante ale terților;

3. încălcarea unui privilegiu sau a unei obligații legale sau profesionale;

4. o barieră în calea anchetelor privind la securitatea angajaților și a procedurilor de arbitraj sau în legătură cu organizarea înlocuirilor și a restructurărilor; sau

5. compromiterea confidențialității necesare în legătură cu funcțiile de control, de inspecție sau de reglementare în raport cu o bună gestiune sau în cadrul negocierilor viitoare sau în curs în care este implicată organizația.

ii. Organizația care invocă o excepție trebuie să demonstreze necesitatea acesteia și motivele pentru restricționarea accesului și solicitanților trebuie să li se indice un punct de contact pentru întrebări suplimentare.

f. Dreptul de a obține confirmarea și perceperea unei taxe pentru acoperirea costurilor pentru asigurarea accesului

i. O persoană are dreptul de a obține confirmarea dacă o organizație deține date cu caracter personal care o privesc. De asemenea, o persoană are dreptul de a-i fi comunicate datele cu caracter personal care o privesc. O organizație poate solicita o taxă care nu este excesivă.

ii. Perceperea unei taxe poate fi justificată, de exemplu, în cazul în care cererile de acces sunt în mod vădit excesive, în special din cauza caracterului lor repetitiv.

iii. Accesul nu poate fi refuzat pentru motive legate de costuri în cazul în care persoana în cauză se oferă să plătească cheltuielile.

g. Cereri de acces repetate sau vexatorii

O organizație poate stabili o limită acceptabilă a numărului de cereri de acces depuse de o anumită persoană într-o perioadă de timp dată, la care va răspunde. Atunci când stabilește astfel de limite, organizația trebuie să ia în considerare factori precum frecvența actualizării informațiilor, scopul în care sunt utilizate datele și natura informațiilor.

h. Cererile de acces frauduloase

Organizația nu este obligată să ofere accesul în cazul în care nu primește informații suficiente pentru a confirma identitatea solicitantului.

i. Termenul pentru furnizarea răspunsurilor

Organizațiile trebuie să răspundă la solicitările de acces într-o perioadă de timp rezonabilă, într-un mod rezonabil și într-o formă ușor de înțeles pentru persoana în cauză. O organizație care furnizează cu regularitate informații persoanelor în cauză poate răspunde la o cerere de acces individuală prin divulgare periodică, în cazul în care aceasta nu ar produce o întârziere excesivă.

9. **Datele privind resursele umane**

a. Acoperirea furnizată de Scutul de confidențialitate

i. În cazul în care o organizație din Uniunea Europeană transferă informații cu caracter personal despre (foștii sau actualii săi) angajați care au fost colectate în cadrul unui raport de muncă către o societate-mamă, afiliată sau neafiliată, care prestează servicii în Statele Unite ale Americii și care aderă la principiile Scutului de confidențialitate, acest transfer beneficiază de avantajele Scutului de confidențialitate. În acest caz, colectarea de informații precum și prelucrarea lor înainte de transfer sunt supuse legilor naționale ale statului membru al Uniunii Europene în care are loc colectarea și toate condițiile sau restricțiile stabilite în domeniu de acesta trebuie să fie respectate.

ii. Principiile Scutului de confidențialitate sunt relevante numai în caz de transfer sau de acces la dosare identificate individual. Declarația statistică bazată pe date globale cu privire la ocuparea forței de muncă și care nu conține date cu caracter personal sau utilizarea datelor anonime sau pseudoanonime nu prezintă riscuri pentru viața privată.

b. Aplicarea principiilor notificării și opțiunii

i. O organizație din Statele Unite ale Americii care a primit din Uniunea Europeană informații despre angajați în temeiul Scutului de confidențialitate le poate comunica unor terți sau le poate utiliza în alte scopuri numai în cazul în care principiile notificării și opțiunii sunt respectate. De exemplu, în cazul în care o organizație intenționează să utilizeze informațiile cu caracter personal colectate în cadrul unui raport de muncă într-un scop care nu are legătură cu acest raport de muncă – cum ar fi trimiterea de mesaje de marketing –, organizația trebuie în prealabil să ofere persoanelor în cauză posibilitatea necesară de opțiune, exceptând cazurile în care acestea și-au dat deja acceptul pentru utilizarea acestor informații în astfel de scopuri. O astfel de utilizare nu trebuie să fie incompatibilă cu scopurile în care informațiile cu caracter personal au fost culese sau autorizate ulterior de persoana în cauză. Pe lângă aceasta, angajatorul nu poate utiliza opțiunile exprimate pentru a împiedica dezvoltarea carierei profesionale a angajaților săi sau pentru a aplica sancțiuni împotriva lor.

ii. Trebuie remarcat că anumite condiții cu aplicabilitate generală cu privire la transferul din unele state membre UE pot exclude alte utilizări ale acestor informații inclusiv după transferul lor în afara Uniunii Europene, iar aceste condiții trebuie respectate.

iii. De asemenea, angajatorii ar trebui să depună toate eforturile posibile pentru a ține seama de preferințele angajatului cu privire la protecția vieții sale private. Aceasta poate include restricționarea accesului la datele cu caracter personal, transformarea anumitor date în anonime sau atribuirea de coduri sau pseudonime atunci când numele reale nu sunt necesare în scopuri administrative.

iv. În măsura și pe durata necesară, fără a aduce atingere capacității organizației de a lua decizii de promovare, numire sau alte decizii similare privind ocuparea forței de muncă, o organizație nu este obligată să ofere notificare și opțiune.

c. Aplicarea principiului accesului

Principiul suplimentar privind accesul oferă indicații cu privire la motivele care pot justifica refuzarea sau limitarea accesului solicitat în contextul resurselor umane. Desigur, angajatorii din Uniunea Europeană trebuie să se conformeze regulamentelor locale și să se asigure că salariații din Uniunea Europeană au acces la aceste informații în conformitate cu legile din țările lor, indiferent de locul în care datele sunt prelucrate și păstrate. Scutul de confidențialitate prevede că o organizație care prelucrează astfel de date în Statele Unite ale Americii trebuie să coopereze la furnizarea accesului, fie direct, fie prin intermediul angajatorului din UE.

d. Asigurarea respectării

i. În măsura în care informațiile cu caracter personal sunt utilizate numai în cadrul unui raport de muncă, responsabilitatea principală pentru date față de angajat revine organizației din UE. Din acest motiv, în cazul în care un angajat european depune o plângere cu privire la încălcarea dreptului său la protecția datelor și nu este mulțumit de rezultatele procedurilor interne de evaluare, de reclamație și de apel (sau orice procedură de arbitraj aplicabilă în temeiul unui contract încheiat cu un sindicat), acesta trebuie direcționat spre autoritățile naționale responsabile de problemele de muncă sau de protecția datelor în jurisdicția în care muncește angajatul. Aceasta include, de asemenea, cazurile în care pretinsa utilizare necorespunzătoare a informațiilor cu caracter personal este responsabilitatea organizației din Statele Unite ale Americii care a primit informațiile de la angajator și, prin urmare, implică o presupusă încălcare a principiilor Scutului de confidențialitate. Acesta este modul cel mai eficient de soluționare a suprapunerilor care există adesea între drepturile și obligațiile stabilite de legislația muncii și de convențiile colective de muncă locale, precum și de legislația privind protecția datelor.

ii. O organizație din Statele Unite ale Americii care aderă la principiile Scutului de confidențialitate și care utilizează date din Uniunea Europeană privind resursele umane transferate din Uniunea Europeană în cadrul unui raport de muncă și care dorește ca aceste transferuri să fie reglementate de Scutul de confidențialitate trebuie să își ia angajamentul în acest sens de a coopera la anchetele autorităților competente din Uniunea Europeană și de a respecta avizele acestora.

e. Aplicarea principiului responsabilității pentru transferurile ulterioare

Pentru necesitățile operaționale legate de forța de muncă ocazională ale organizației care aderă la Scutul de confidențialitate în ceea ce privește datele cu caracter personal transferate în temeiul Scutului de confidențialitate, cum ar fi rezervarea unui bilet de avion, a unei camere de hotel sau asigurare, se pot transfera către operatori date cu caracter personal ale unui număr mic de angajați, fără aplicarea principiului accesului sau fără încheierea unui contract cu operatorul terț, astfel cum prevede principiul responsabilității pentru transferurile ulterioare, cu condiția ca organizația care aderă la Scutul de confidențialitate să fi respectat principiile notificării și opțiunii.

10. **Contracte obligatorii pentru transferurile ulterioare**

a. Contractele de prelucrare a datelor

i. Transferul de date cu caracter personal din Uniunea Europeană în Statele Unite ale Americii efectuat doar în scopul prelucrării necesită un contract independent de participarea responsabilului cu prelucrarea datelor la Scutul de confidențialitate.

ii. Operatorii de date din Uniunea Europeană au întotdeauna obligația de a încheia un contract atunci când are loc un transfer pentru prelucrare de date, indiferent dacă această operațiune este efectuată în Uniunea Europeană sau în afara acesteia și indiferent dacă responsabilul cu prelucrarea datelor participă sau nu la Scutul de confidențialitate. Scopul contractului este de a asigura că responsabilul cu prelucrarea datelor:

1. acționează numai la instrucțiunile operatorului;

2. prevede măsuri tehnice și organizatorice adecvate pentru a proteja datele cu caracter personal împotriva distrugerii accidentale sau ilegale sau a pierderii accidentale, a modificării, a divulgării sau a accesului neautorizat și are cunoștință dacă transferul ulterior este permis; și

3. ținând seama de natura prelucrării, oferă asistență operatorului în ceea ce privește răspunsurile oferite persoanelor care își exercită drepturile în conformitate cu principiile.

iii. Întrucât participanții la Scutul de confidențialitate asigură o protecție adecvată a datelor, contractele de prelucrare încheiate cu aceștia nu necesită o autorizație prealabilă (sau această autorizație este acordată automat de statele membre ale UE), spre deosebire de contractele ai căror beneficiari nu participă la Scutul de confidențialitate sau nu asigură o protecție adecvată.

b. Transferurile în cadrul unui grup controlat de societăți sau entități

În cazul în care informațiile cu caracter personal sunt transferate între doi operatori în cadrul unui grup controlat de societăți sau entități, nu este întotdeauna necesar un contract în conformitate cu principiul responsabilității pentru transferul ulterior. Operatorii de date din cadrul unui grup controlat de societăți sau entități pot stabili astfel de transferuri pe baza altor instrumente precum regulile corporatiste obligatorii la nivelul UE sau a altor instrumente din cadrul grupului (de exemplu, programe de conformitate și control), care asigură continuitatea programelor de protecție a informațiilor cu caracter personal în temeiul principiilor. În cazul unor astfel de transferuri, organizația care aderă la Scutul de confidențialitate rămâne responsabilă pentru respectarea principiilor.

c. Transferurile între operatori

În cazul transferurilor între operatori, operatorul care primește datele nu este obligatoriu să fie o organizație care aderă la Scutul de confidențialitate sau să dispună de un mecanism independent de recurs. Organizația care aderă la Scutul de confidențialitate trebuie să încheie un contract cu un operator terț care primește datele, care oferă același nivel de protecție oferit de Scutul de confidențialitate, fără a include cerința ca operatorul terț să fie o organizație care aderă la Scutul de confidențialitate sau să dispună de un mecanism independent de recurs, cu condiția de a pune la dispoziție un mecanism echivalent.

11. **Soluționarea litigiilor și punerea în aplicare**

a. Principiul recursului, punerii în aplicare și responsabilității stabilește cerințele pentru punerea în aplicare a Scutului de confidențialitate. Modul în care sunt îndeplinite cerințele de la punctul (a)(ii) din principiu este prezentat în principiul suplimentar privind verificarea. Acest principiu suplimentar vizează punctele (a)(i) și (a)(ii), ambele necesitând mecanisme independente de recurs. Astfel de mecanisme pot lua forme diferite, dar trebuie să îndeplinească cerințele principiului recursului, punerii în aplicare și responsabilității. Organizațiile satisfac aceste cerințe în următoarele moduri: (i) participând la programele organizate de sectorul privat cu privire la protecția vieții private care integrează principiile Scutului de confidențialitate în normele lor și care includ mecanisme de punere în aplicare eficiente de tipul celor descrise în principiul recursului, punerii în aplicare și responsabilității; (ii) conformându-se instrucțiunilor organelor de supraveghere sau de reglementare legale care asigură prelucrarea plângerilor persoanelor și soluționarea litigiilor; sau (iii) luându-și angajamentul de a coopera cu autoritățile însărcinate cu protecția datelor în cadrul Uniunii Europene sau cu reprezentanții autorizați ai acestora.

b. Prezenta listă are valoare ilustrativă și nu este restrictivă. Sectorul privat poate elabora mecanisme suplimentare de asigurare a respectării, cu condiția ca acestea să întrunească cerințele principiului recursului, punerii în aplicare și responsabilității și ale principiilor suplimentare. Trebuie remarcat faptul că cerințele principiului

recursului, punerii în aplicare și responsabilității vin în completarea cerinței conform căreia inițiativele de autoreglementare trebuie să fie aplicate în conformitate cu articolul 5 din Federal Trade Commission Act, care interzice practicile neloiale sau frauduloase, sau în conformitate cu altă lege sau act normativ care interzice astfel de practici.

c. Pentru a asigura respectarea angajamentelor asumate în temeiul Scutului de confidențialitate și pentru a sprijini gestionarea programului, organizațiile, precum și mecanismele independente de recurs ale acestora trebuie să furnizeze informații cu privire la Scutul de confidențialitate atunci când acestea sunt solicitate de către Departament. În plus, organizațiile trebuie să răspundă rapid plângerilor privind respectarea principiilor, transmise prin intermediul Departamentului de către APD. Răspunsul ar trebui să stabilească dacă plângerea este justificată și, în caz afirmativ, modul în care organizația va remedia problema. Departamentul va proteja confidențialitatea informațiilor pe care le primește în conformitate cu legislația SUA.

d. Instanțe de recurs

i. Consumatorii ar trebui să fie încurajați să adreseze eventualele plângeri organizației în cauză, înainte de a face apel la instanțe independente de recurs. Organizațiile trebuie să răspundă unui consumator în termen de 45 de zile de la primirea plângerii. Independența unei instanțe de recurs este o chestiune de fapt care poate fi demonstrată, în special, prin imparțialitate, transparența componenței sale și a finanțării și un bilanț pozitiv în domeniul său de activitate. În conformitate cu principiul recursului, punerii în aplicare și responsabilității, recursul disponibil persoanelor particulare trebuie să fie ușor disponibil și gratuit pentru persoanele fizice. Organismele de instrumentare a litigiilor trebuie să analizeze fiecare plângere primită de la persoane particulare, exceptând cazurile în care acestea sunt în mod evident nefondate sau abuzive. Această condiție nu împiedică stabilirea condițiilor de eligibilitate de către organizația care gestionează mecanismul de recurs, însă astfel de cerințe ar trebui să fie transparente și justificate (de exemplu, excluderea plângerilor care nu intră în domeniul de aplicare a programului sau care sunt de competența altei instanțe) și nu trebuie să aibă ca rezultat compromiterea angajamentului de a analiza plângerile legitime. Pe lângă aceasta, instanțele de recurs trebuie să ofere persoanelor particulare informații complete și ușor accesibile cu privire la modul în care funcționează procedura de soluționare a litigiilor când acestea depun o plângere. Aceste informații trebuie să includă o descriere a practicilor instanței în materie de protecție a vieții private, în conformitate cu principiile Scutului de confidențialitate. De asemenea, instanțele trebuie să coopereze pentru a pune la punct instrumente, cum ar fi formularele tip pentru plângeri, pentru a facilita procedura de soluționare a litigiilor.

ii. Mecanismele independente de recurs trebuie să includă pe site-urile lor publice informații cu privire la principiile Scutului de confidențialitate și serviciile pe care acestea le furnizează în temeiul Scutului de confidențialitate. Informațiile în cauză trebuie să includă: (1) informații despre sau un link către cerințele principiilor Scutului de confidențialitate referitoare la mecanisme independente de recurs; (2) un link către site-ul Scutului de confidențialitate al Departamentului; (3) o explicație că serviciile de soluționare a litigiilor în temeiul Scutului de confidențialitate al Departamentului sunt gratuite pentru persoanele fizice; (4) o descriere a modului în care se poate depune o plângere legată de Scutul de confidențialitate; (5) termenul în care sunt prelucrate plângerile legate de Scutul de confidențialitate; și (6) o descriere a seriei de soluții posibile.

iii. Instanțele de recurs independente trebuie să publice un raport anual care furnizează statistici agregate privind serviciile lor de soluționare a litigiilor. Raportul anual trebuie să conțină: (1) numărul total de plângeri legate de Scutul de confidențialitate primite în cursul anului de raportare; (2) tipurile de plângeri primite de soluționare a litigiilor; (3) măsurile de asigurare a calității, cum ar fi perioada de timp pentru prelucrarea reclamațiilor; și (4) rezultatele plângerilor primite, în special numărul și tipul de măsuri corective sau sancțiuni impuse.

iv. Astfel cum se prevede în anexa I, o opțiune de arbitraj este pusă la dispoziția unei persoane pentru a determina, pentru plângerile rămase, dacă o organizație care aderă la Scutul de confidențialitate și-a încălcat obligațiile care îi revin în temeiul principiilor cu privire la persoana în cauză și dacă orice astfel de încălcări nu sunt remediate în totalitate sau parțial. Această opțiune este disponibilă numai în aceste scopuri. Această opțiune nu este disponibilă, de exemplu, în ceea ce privește excepțiile de la principii ([1]) sau cu privire la o prezumție cu privire la caracterul adecvat al Scutului de confidențialitate. În cadrul acestei opțiuni de arbitraj, comitetul pentru Scutul de confidențialitate (format din unul sau din trei arbitri, astfel cum s-a convenit de către părți) are autoritatea de a impune măsuri echitabile, nemonetare, personalizate (precum accesul, rectificarea, ștergerea sau restituirea datelor persoanei în cauză) necesare pentru a remedia încălcarea principiilor numai cu privire la persoana în cauză. Persoanele și organizațiile care aderă la Scutul de confidențialitate vor putea să inițieze o procedură judiciară și să solicite aplicarea hotărârilor arbitrale în temeiul legislației SUA, în conformitate cu Legea federală privind arbitrajul.

([1]) Secțiunea I.5 din principii.

e. Recursuri și sancțiuni

Orice recurs la organismul de instrumentare a litigiilor ar trebui să conducă la anularea sau corectarea, în măsura în care este posibil, a efectelor nerespectării principiilor de către organizație, la respectarea principiilor în timpul prelucrărilor viitoare de către aceeași organizație și, după caz, la încetarea prelucrării datelor cu caracter personal ale persoanei care a depus plângerea. Sancțiunile trebuie să fie suficient de severe pentru a garanta respectarea principiilor de către organizație. O serie de sancțiuni cu grade diferite de severitate va permite instanțelor de soluționare a litigiilor să răspundă în mod corespunzător diferitelor niveluri de nerespectare a principiilor. Sancțiunile trebuie să includă atât publicarea constatărilor de nerespectare, cât și obligația de a șterge datele în anumite circumstanțe ([1]). Alte sancțiuni pot include suspendarea sau anularea mărcii de conformitate, despăgubirea persoanelor pentru pierderile suferite ca urmare a nerespectării principiilor, precum și acțiuni în încetare. Organismele de soluționare a litigiilor și de autoreglementare a sectorului privat trebuie să semnaleze tribunalelor sau organului administrativ competent, după caz, organizațiile care aderă la Scutul de confidențialitate și care nu respectă deciziile acestora și să informeze Departamentul.

f. Acțiunea FTC

FTC s-a angajat să acorde prioritate analizării sesizărilor referitoare la nerespectarea principiilor, prezentate de: (i) organizații de autoreglementare în vederea protejării vieții private și de alte organisme independente de soluționare a litigiilor; (ii) state membre ale UE; și (iii) Departament, pentru a stabili dacă a fost încălcat punctul 5 din Federal Trade Commission Act, care interzice actele sau practicile neloiale sau frauduloase în comerț. În cazul în care stabilește că există motiv pentru a considera că articolul 5 a fost încălcat, FTC poate soluționa această problemă obținând un ordin administrativ de încetare care interzice practicile contestate sau depunând o plângere la un tribunal districtual federal, care, în cazul în care plângerea este soluționată favorabil, poate emite o ordonanță care produce același efect. Aceasta include declarații false privind aderarea la principiile Scutului de confidențialitate sau privind participarea la Scutul de confidențialitate a organizațiilor care fie nu se mai află pe lista Scutului de confidențialitate, fie nu s-au autocertificat la Departament. FTC poate cere sancțiuni de drept civil pentru încălcarea unui ordin administrativ de încetare și poate urmări contravenientul pentru ultraj într-un tribunal civil sau penal în cazul încălcării ordinului unui tribunal federal. FTC informează Departamentul cu privire la orice acțiune de acest tip întreprinsă. Departamentul încurajează celelalte organisme administrative să îi comunice toate cazurile similare sau alte decizii care determină aderarea la principiile Scutului de confidențialitate.

g. Încălcarea sistematică a principiilor

i. În cazul în care o organizație încalcă sistematic principiile, aceasta nu mai are dreptul să beneficieze de avantajele Scutului de confidențialitate. Organizațiile care au încălcat în mod sistematic principiile vor fi eliminate de pe lista Scutului de confidențialitate de către Departament și trebuie să returneze sau să șteargă datele cu caracter personal pe care le primesc în temeiul Scutului de confidențialitate.

ii. Principiile sunt încălcate sistematic atunci când o organizație care și-a transmis Departamentului autocertificarea refuză să se conformeze unei decizii definitive luate de un organism de autoreglementare în vederea protejării vieții private, o instanță independentă de soluționare a litigiilor sau un organism public sau atunci când un asemenea organism constată că aceasta încalcă frecvent principiile, astfel încât declarația sa de aderare nu mai este credibilă. În aceste cazuri, organizația trebuie să notifice neîntârziat Departamentul cu privire la aceste fapte. În caz contrar, aceasta este pasibilă de sancțiuni în temeiul legii privind declarațiile false (18 U.S.C § 1001). Retragerea unei organizații dintr-un program de autoreglementare în vederea protejării vieții private organizat de sectorul privat sau dintr-un mecanism independent de soluționare a litigiilor nu o exonerează de obligația de a respecta principiile și ar putea constitui o încălcare sistematică a obligațiilor.

iii. Departamentul va elimina o organizație de pe lista Scutului de confidențialitate ca răspuns la orice notificare de încălcare sistematică pe care o primește, indiferent dacă aceasta provine de la organizația însăși, de la un organism de autoreglementare în vederea protejării vieții private, de la un alt organism independent de soluționare a litigiilor sau de la un organism public, însă numai după ce a acordat organizației în cauză un

([1]) Organismele de soluționare a litigiilor dispun de o marjă de apreciere cu privire la circumstanțele în care utilizează aceste sancțiuni. Caracterul sensibil al datelor în cauză este un element care trebuie luat în considerare pentru a stabili dacă ar trebui să se impună ștergerea datelor, precum și dacă o organizație a colectat, a utilizat sau a divulgat informații cu încălcarea flagrantă a principiilor Scutului de confidențialitate.

preaviz de 30 de zile și posibilitatea de a răspunde. În consecință, lista Scutului de confidențialitate gestionată de Departament va preciza care organizații beneficiază de avantajele Scutului de confidențialitate și care organizații nu mai beneficiază de acestea.

iv. Orice organizație care solicită să fie supusă autorității unui organism de autoreglementare pentru a putea beneficia din nou de avantajele Scutului de confidențialitate trebuie să furnizeze acestui organism informații complete cu privire la aderarea ei anterioară la Scutul de confidențialitate.

12. **Opțiune – Când poate fi exercitat dreptul de refuz**

a. În general, obiectivul principiului opțiunii este de a asigura că informațiile cu caracter personal sunt utilizate și comunicate în conformitate cu așteptările și opțiunile persoanelor în cauză. În consecință, atunci când informații cu caracter personal sunt utilizate în cadrul unei acțiuni de marketing direct, orice persoană ar trebui să poată să își exercite opțiunea de a refuza în orice moment, în anumite limite definite de organizație, de exemplu timpul necesar pentru a permite organizației punerea în aplicare a refuzului. De asemenea, organizația poate solicita un anumit număr de informații pentru a confirma identitatea persoanei care și-a exprimat refuzul. În Statele Unite ale Americii, acest drept poate fi exercitat prin intermediul unui program central de refuz, cum ar fi „Mail Preference Service" al Direct Marketing Association. Organizațiile care participă la „Mail Preference Service" al Direct Marketing Association ar trebui să promoveze disponibilitatea aceste opțiuni în rândul consumatorilor care nu doresc să primească informații comerciale. În orice caz, exercitarea acestei opțiuni trebuie să fie ușor accesibilă și puțin costisitoare.

b. În mod similar, o organizație poate utiliza informații în anumite scopuri de marketing direct atunci când condițiile nu permit exprimarea opțiunii persoanelor în cauză înainte de utilizarea informațiilor, cu condiția ca organizația să ofere ulterior cu promptitudine (și, la cerere, în orice moment) posibilitatea persoanelor în cauză de a refuza (fără a plăti vreo taxă) să primească orice alte informații de marketing direct, precum și să se conformeze dorințelor acestor persoane.

13. **Informații cu privire la călătorii**

a. Informațiile cu privire la pasagerii din transporturile aeriene furnizate în special în momentul rezervărilor și alte informații privind călătoriile, cum ar fi cele privind clienții frecvenți sau rezervările la hotel, precum și cererile speciale, de exemplu mese care sunt în conformitate cu anumite principii religioase sau asistență fizică pot fi comunicate organizațiilor situate în afara Uniunii Europene în diferite circumstanțe. În conformitate cu articolul 26 din directivă, datele cu caracter personal pot fi transferate spre o țară terță care nu asigură un nivel adecvat de protecție în sensul articolului 25 alineatul (2) cu condiția ca (i) transferul să fie necesar pentru prestarea serviciilor solicitate de client sau pentru executarea unui contract, cum este acordul „client frecvent al zborurilor aeriene"; sau (ii) pasagerul să își fi dat acordul în mod neechivoc. Organizațiile din Statele Unite ale Americii care aderă la Scutul de confidențialitate oferă o protecție adecvată a datelor cu caracter personal și, în consecință, pot primi astfel de date din Uniunea Europeană fără a îndeplini aceste condiții și nici alte condiții menționate la articolul 26 din directivă. Întrucât Scutul de confidențialitate cuprinde reguli specifice cu privire la informațiile sensibile, acest tip de informații (care pot privi, de exemplu, necesitatea clientului de a beneficia de asistență fizică) poate fi inclus în datele transferate organizațiilor care aderă la principiile Scutului de confidențialitate. Cu toate acestea, în toate cazurile, organizația care transferă informațiile trebuie să aplice legislația națională a statului membru al Uniunii Europene în care operează, care poate impune, *inter alia*, condiții speciale pentru prelucrarea datelor sensibile.

14. **Produse farmaceutice și medicale**

a. Aplicarea legislațiilor statelor membre ale UE sau a principiilor Scutului de confidențialitate

Legislația statelor membre ale UE se aplică colectării de date cu caracter personal și oricărei prelucrări care are loc înainte de transferul către Statele Unite ale Americii. Principiile Scutului de confidențialitate se aplică datelor atunci când au fost transferate către Statele Unite ale Americii. Datele utilizate pentru cercetarea farmaceutică și în alte scopuri trebuie transmise, după caz, anonime.

b. Cercetarea științifică viitoare

i. Datele cu caracter personal elaborate în cadrul studiilor medicale sau farmaceutice joacă de multe ori un rol important în cercetarea științifică. Atunci când datele cu caracter personal colectate pentru un studiu sunt transferate unei organizații din Statele Unite ale Americii care a aderat la Scutul de confidențialitate, organizația poate să utilizeze datele pentru o nouă activitate de cercetare științifică în cazul în care au fost prevăzute de la început o notificare și o opțiune corespunzătoare. Notificarea trebuie să ofere informații cu privire la orice utilizare specifică viitoare a datelor, cum ar fi controlul periodic, studiile asociate sau comercializarea.

ii. Este de la sine înțeles că nu pot fi precizate toate utilizările viitoare ale datelor, întrucât o nouă examinare a datelor, noi descoperiri și progrese medicale, precum și evoluția în domeniul sănătății publice și al reglementării ar putea determina noi utilizări ale datelor. Prin urmare, notificarea ar trebui să includă, după caz, o mențiune că datele cu caracter personal pot fi utilizate pentru activități medicale și farmaceutice de cercetare viitoare neanticipate. În cazul în care această utilizare a datelor nu este conformă cu scopurile de cercetare generale pentru care datele au fost colectate inițial sau pentru care persoana în cauză a consimțit, trebuie obținut un nou consimțământ al persoanei vizate.

c. Retragerea dintr-un studiu clinic

Participanții pot decide sau pot fi invitați să se retragă dintr-un studiu clinic în orice moment. Cu toate acestea, datele colectate înaintea retragerii pot fi prelucrate în continuare împreună cu celelalte date colectate în cadrul studiului clinic, cu condiția ca acest fapt să fi fost comunicat participantului în notificare în momentul în care și-a dat acordul.

d. Transferurile în scopuri de reglementare și de supraveghere

Societățile producătoare de aparate farmaceutice și medicale au dreptul de a furniza date cu caracter personal extrase din testele clinice efectuate în Uniunea Europeană către autoritățile din Statele Unite ale Americii în scopul reglementării și al controlului. Acest tip de transferuri este permis și altor părți, cum ar fi întreprinderi și alți cercetători, în conformitate cu principiile notificării și opțiunii.

e. „Teste mascate”

i. Pentru a asigura obiectivitatea testelor clinice, accesul la informațiile privind tratamentul de care beneficiază fiecare pacient este interzis participanților, precum și, deseori, chiar cercetătorilor. Accesul la aceste informații ar periclita validitatea testului și a rezultatelor. Participanții la asemenea teste clinice (denumite „teste mascate”) nu vor avea acces la datele privind tratamentul lor pe parcursul testului în cazul în care această restricție le-a fost explicată la începutul testului și dacă publicarea acestor informații ar periclita integritatea eforturilor de cercetare.

ii. Acordul de a participa la test în aceste condiții presupune renunțarea la dreptul de acces. La încheierea testului și după analizarea rezultatelor, participanții ar trebui să aibă acces la datele lor, dacă doresc acest lucru. Aceștia ar trebui să ceară datele în primul rând medicului sau altui prestator de servicii de sănătate de la care au primit tratamentul în cadrul testului clinic sau, în al doilea rând, organizației care a sponsorizat programul.

f. Controlul securității și eficacității produsului

O societate producătoare de aparate farmaceutice sau medicale nu trebuie să aplice în activitățile sale de control al securității și eficacității produsului principiile Scutului de confidențialitate privind notificarea, opțiunea, răspunderea pentru transferul ulterior și accesul, inclusiv semnalarea incidentelor și urmărirea pacienților/subiecților care folosesc anumite medicamente sau aparate medicale, în măsura în care respectarea acestor principii contravine cerințelor de reglementare. Acest lucru este valabil în ceea ce privește, de exemplu,

rapoartele prezentate atât de prestatorii de servicii de sănătate către societățile comerciale producătoare de aparate farmaceutice și medicale, cât și cele prezentate de aceste din urmă societăți comerciale către agenții guvernamentale precum Food and Drug Administration (autoritatea pentru supravegherea alimentelor și medicamentelor).

g. Date codificate la sursă

Datele referitoare la cercetare sunt codificate, de regulă, la sursă de către cercetătorul principal pentru a nu fi dezvăluită identitatea persoanelor vizate. Societățile comerciale farmaceutice care sponsorizează aceste cercetări nu primesc codul de acces. Codul de acces unic este deținut numai de către cercetător, astfel încât acesta să poată identifica persoana în cauză în circumstanțe speciale (de exemplu, în cazul în care este necesară monitorizarea medicală). Transferul din Uniunea Europeană către Statele Unite ale Americii de date codificate în acest fel reprezintă un transfer de date cu caracter personal supus principiilor Scutului de confidențialitate.

15. **Informații din registre publice și informații accesibile publicului**

a. O organizație trebuie să aplice principiile Scutului de confidențialitate privind securitatea, integritatea datelor și limitarea scopului și privind recursul, punerea în aplicare și răspunderea față de datele cu caracter personal, din surse aflate la dispoziția publicului. Aceste principii se aplică, de asemenea, datelor cu caracter personal colectate din registrele publice, și anume registrele păstrate de autorități guvernamentale sau de alte administrații publice la orice nivel și care pot fi consultate de publicul larg.

b. Nu este necesar să se aplice principiul notificării, opțiunii și răspunderii pentru transferul ulterior informațiilor din registrele publice în cazul în care acestea din urmă nu sunt asociate cu informații care nu sunt accesibile publicului și dacă sunt respectate toate condițiile de consultare stabilite de instanța competentă. De asemenea, nu este necesară aplicarea principiilor notificării, opțiunii și răspunderii pentru transferul ulterior în cazul informațiilor accesibile publicului decât în cazul în care entitatea europeană care efectuează transferul indică faptul că aceste informații fac obiectul restricțiilor care necesită aplicarea respectivelor principii de către organizație în timpul utilizării lor. Organizația nu are nicio responsabilitate cu privire la modul în care sunt utilizate astfel de informații de către cei care le obțin din materiale publicate.

c. În cazul în care se constată că o organizație a făcut publice în mod intenționat informații cu caracter personal încălcând principiile astfel încât ea însăși sau alte părți terțe să poată beneficia de aceste excepții, aceasta va fi exclusă din Scutul de confidențialitate.

d. Nu este necesar să se aplice principiul accesului în cazul informațiilor extrase din registrele publice atât timp cât acestea nu sunt asociate cu alte date cu caracter personal (cu excepția unor loturi mici utilizate pentru indexarea sau organizarea registrelor publice); cu toate acestea, trebuie respectate toate condițiile privind consultarea stabilite de instanțele competente. În schimb, atunci când informațiile din registre publice sunt asociate cu alte date care nu au caracter public (altele decât cele menționate mai sus), organizația trebuie să permită accesul la toate aceste informații, în cazul în care acestea nu fac obiectul altor derogări.

e. La fel ca în cazul informațiilor extrase din registrele publice, nu este necesar să se acorde accesul la informații care sunt deja disponibile publicului, atât timp cât acestea nu sunt asociate cu alte date care nu sunt disponibile publicului. Organizațiile specializate în vânzarea de informații accesibile publicului pot solicita taxa practicată în mod obișnuit de organizație ca răspuns la cererile de acces. De asemenea, fiecare persoană poate obține informațiile care o privesc adresându-se direct primei organizații care a adunat inițial datele.

16. **Cererile de acces formulate de autorități publice**

a. Pentru a asigura transparența în ceea ce privește solicitările legale formulate de autorități publice pentru a avea acces la informații cu caracter personal, organizațiile care aderă la Scutul de confidențialitate pot emite voluntar rapoarte periodice privind transparența cu privire la numărul de cereri de informații cu caracter personal pe care le primesc, formulate de autorități publice pentru rațiuni de securitate națională sau de aplicare a legii, în măsura în care divulgările sunt admisibile în conformitate cu legislația aplicabilă.

b. Informațiile furnizate de organizațiile care aderă la Scutul de confidențialitate în aceste rapoarte, împreună cu informațiile care i-au fost comunicate de către serviciile de informații, împreună cu alte informații, pot fi utilizate ca fundament pentru examinarea anuală comună cu privire la funcționarea Scutului de confidențialitate în conformitate cu principiile.

c. Absența notificării în conformitate cu litera (a) punctul (xii) din principiul notificării nu împiedică, nici nu compromite capacitatea unei organizații de a răspunde la orice solicitări legale.

Anexa I

Model de arbitraj

Prezenta anexă I prevede condițiile în care organizațiile care aderă la Scutul de confidențialitate sunt obligate să supună plângerile unei proceduri de arbitraj, în temeiul principiului recursului, punerii în aplicare și responsabilității. Opțiunea arbitrajului obligatoriu descrisă mai jos se aplică anumitor plângeri „rămase" privind datele aflate sub incidența Scutului de confidențialitate UE-SUA. Obiectivul acestei opțiuni este de a oferi un mecanism echitabil, independent și prompt, la alegerea persoanelor în cauză, pentru soluționarea presupuselor încălcări ale principiilor care nu au fost rezolvate prin alte mecanisme din cadrul Scutului de confidențialitate, în cazul în care există.

A. **Domeniu de aplicare**

Această opțiune a arbitrajului este pusă la dispoziția unei persoane pentru a determina, pentru plângerile rămase, dacă o organizație care aderă la Scutul de confidențialitate a încălcat obligațiile care îi revin în temeiul principiilor în ceea ce privește persoana în cauză și dacă orice astfel de încălcări nu sunt remediate în totalitate sau parțial. Această opțiune este disponibilă numai în aceste scopuri. Această opțiune nu este disponibilă, de exemplu, în ceea ce privește excepțiile de la principii ([1]) sau cu privire la o prezumție cu privire la caracterul adecvat al Scutului de confidențialitate.

B. **Căile de atac disponibile**

În cadrul acestei opțiuni de arbitraj, comitetul pentru Scutul de confidențialitate (format din unul sau din trei arbitri, astfel cum s-a convenit de către părți) are autoritatea de a impune măsuri echitabile, nemonetare, personalizate (precum accesul, rectificarea, ștergerea sau restituirea datelor persoanei în cauză) necesare pentru a remedia încălcarea principiilor numai cu privire la persoana în cauză. Acestea sunt singurele competențe ale comisiei de arbitraj referitoare la căile de atac. La examinarea căilor de atac, comisia de arbitraj este obligată să examineze alte căi de atac deja impuse prin alte mecanisme în temeiul Scutului de confidențialitate. Nu sunt disponibile măsuri pentru repararea prejudiciilor, taxe sau alte căi de atac. Fiecare parte suportă propriile onorarii plătite avocaților.

C. **Cerințe de îndeplinit înainte de arbitraj**

O persoană care decide să se prevaleze de această opțiune de arbitraj trebuie să ia următoarele măsuri înainte de inițierea unei solicitări de arbitraj: (1) să reclame presupusa încălcare direct la organizație și să ofere organizației posibilitatea de a soluționa problema în termenele prevăzute în secțiunea III.11 litera (d) punctul (i) din principii; (2) să utilizeze mecanismul independent de recurs în temeiul principiilor, fără ca persoana în cauză să suporte vreun cost; și (3) să ridice problema prin intermediul autorității pentru protecția datelor la Departamentul Comerțului și să ofere Departamentului Comerțului ocazia de a depune eforturi pentru a soluționa problema în termenele prevăzute în scrisoarea de la Administrația pentru comerțul internațional din cadrul Departamentului Comerțului, fără ca persoana în cauză să suporte vreun cost.

Această opțiune de arbitraj nu poate fi invocată în cazul în care aceeași acuzație de încălcare a principiilor a unei persoane (1) a făcut deja obiectul unui arbitraj obligatoriu; (2) a făcut obiectul unei hotărâri cu caracter definitiv într-o acțiune judiciară la care persoana a fost parte; sau (3) a fost soluționată de părți. În plus, această opțiune nu poate fi invocată în cazul în care o autoritate pentru protecția datelor din UE (1) are competență în temeiul secțiunilor III.5 sau III.9 din principii; sau (2) are competența de a soluționa presupusa încălcare în mod direct cu organizația. Competența unei APD de a soluționa aceeași plângere împotriva unui operator de date din UE nu se opune invocării opțiunii de arbitraj împotriva unei entități juridice diferite care nu intră sub jurisdicția autorității pentru protecția datelor.

D. **Caracterul obligatoriu al deciziilor**

Decizia unei persoane de a invoca opțiunea arbitrajului obligatoriu este exclusiv voluntară. Deciziile arbitrale sunt obligatorii pentru toate părțile la arbitraj. Odată invocată această opțiune, persoana în cauză renunță la posibilitatea de a solicita măsuri reparatorii pentru aceeași presupusă încălcare în alte forumuri, cu excepția cazului în care măsurile reparatorii echitabile nemonetare nu compensează pe deplin presupusa încălcarea, invocarea arbitrajului nu împiedică introducerea unei acțiuni în despăgubire care este disponibilă în alt mod în instanță.

([1]) Secțiunea I.5 din principii.

E. **Revizuirea și punerea în aplicare**

Persoanele și organizațiile care aderă la Scutul de confidențialitate vor putea să inițieze o procedură judiciară și să solicite aplicarea hotărârilor arbitrale în temeiul legislației SUA, în conformitate cu Legea federală privind arbitrajul ([1]). Orice astfel de cazuri trebuie introduse la instanța federală districtuală pe a cărei rază teritorială se află sediul principal al organizației care aderă la Scutul de confidențialitate.

Această opțiune de arbitraj vizează soluționarea litigiilor individuale, iar hotărârile arbitrale nu sunt destinate să funcționeze ca un precedent obligatoriu sau convingător în chestiuni care implică alte părți, inclusiv arbitraje viitoare sau în instanțe din UE sau din SUA sau într-o procedură judiciară a FTC.

F. **Comisia de arbitraj**

Părțile selectează arbitrii din lista arbitrilor discutată mai jos.

În conformitate cu legislația aplicabilă, Departamentul Comerțului din SUA și Comisia Europeană vor elabora o listă de cel puțin 20 de arbitri, selectați pe criterii de independență, integritate și expertiză. Următoarele dispoziții se aplică în ceea ce privește acest proces:

Arbitrii

(1) vor rămâne pe listă pentru o perioadă de 3 ani, cu absențe în circumstanțe excepționale sau motivat, termen care poate fi reînnoit pentru o perioadă suplimentară de 3 ani;

(2) nu se supun niciunei instrucțiuni din partea, nici nu au legătură cu una dintre părți, nici cu vreo organizație care aderă la Scutul de confidențialitate, nici cu SUA, UE sau orice stat membru al UE sau orice altă autoritate guvernamentală, autoritate publică sau autoritate de aplicare a legii; și

(3) trebuie să fie autorizați să exercite o profesiune juridică în SUA și să fie experți în legislația SUA privind protecția vieții private, cu expertiză în legislația UE privind protecția datelor.

G. **Proceduri de arbitraj**

În conformitate cu legislația aplicabilă, în termen de 6 luni de la adoptarea deciziei privind caracterul adecvat, Departamentul Comerțului și Comisia Europeană sunt de acord să adopte o serie de proceduri de arbitraj ale SUA consacrate (cum ar fi AAA sau JAMS) care reglementează procedura în fața comitetului pentru Scutul de confidențialitate, sub rezerva fiecăreia dintre considerațiile următoare:

1. O persoană poate iniția un arbitraj obligatoriu, sub rezerva îndeplinirii dispoziției privind cerințele anterioare arbitrajului de mai sus, prin transmiterea unei „notificări" organizației. Notificarea trebuie să conțină un rezumat al măsurilor luate în conformitate cu punctul C pentru soluționarea cererii, o descriere a presupusei încălcări și, la alegerea persoanei, toate documentele și materialele justificative și/sau o discuție pe marginea legislației referitoare la presupusa încălcare.

([1]) Capitolul 2 din Federal Arbitration Act („FAA") prevede că „[u]n acord de arbitraj sau o hotărâre arbitrală care decurge dintr-o relație juridică, contractuală sau nu, care este considerată comercială, inclusiv o tranzacție, contract sau acord descrise în [secțiunea 2 din FAA], intră în sfera de aplicare a Convenției [privind recunoașterea și aplicarea hotărârilor arbitrale străine, din 10 iunie 1958, 21 U. S.T. 2519, T.I.A.S. nr. 6997 («Convenția de la New York»)." 9 U.S.C. § 202. De asemenea, FAA prevede că, „[u]n acord sau o hotărâre arbitrală care decurge dintr-o astfel de relație care este doar între cetățenii Statelor Unite se consideră că nu intră în domeniul de aplicare al Convenției [de la New York], cu excepția cazului în care această relație implică bunuri aflate în străinătate, prevede executarea sau aplicarea în străinătate sau are o altă relație cu unul sau mai multe state terțe." *Id.* În conformitate cu capitolul 2, „orice parte la arbitraj poate apela la orice instanță care are competență în temeiul prezentului capitol pentru o ordonanță prin care se confirmă hotărârea împotriva oricărei alte părți la arbitraj. Instanța confirmă hotărârea, cu excepția cazului în care constată că unul dintre motivele de refuz sau de amânare a recunoașterii sau a executării hotărârii este specificat în Convenția [de la New York] menționată." *Id.* § 207. Capitolul 2 prevede în continuare că „[i]nstanțele districtuale din Statele Unite. .. au jurisdicția inițială asupra. .. unei acțiuni sau proceduri [în temeiul Convenției de la New York], indiferent de suma în litigiu." *Id.* § 203.
Capitolul 2 prevede, de asemenea, că „dispozițiile capitolului 1 se aplică acțiunilor și procedurilor intentate în temeiul prezentului capitol, în măsura în care capitolul în cauză nu intră în conflict cu prezentul capitol sau cu Convenția [de la New York] astfel cum au fost ratificată de Statele Unite." *Id.* § 208. Capitolul 1, în schimb, prevede că „[o] dispoziție scrisă dintr-un... contract care demonstrează existența unei tranzacții care implică relații comerciale pentru a soluționa prin arbitraj o controversă, care decurge din acest contract sau tranzacție sau refuzul de a executa contractul în totalitate sau parțial sau un acord în scris de a supune arbitrajului o controversă existentă care decurge din acest contract, tranzacție sau refuz, este valabil, irevocabil și executoriu, cu excepția cazurilor în care există motive în drept sau în echitate în cazul revocării unui contract." *Id.* § 2. Capitolul 1 prevede, de asemenea, că „orice parte la procedura de arbitraj poate solicita instanței susmenționate o ordonanță care să confirme ulterior hotărârea, iar instanța trebuie să acorde o astfel de ordin, cu excepția cazului în care hotărârea este anulată, modificată sau rectificată, astfel cum se prevede în secțiunile 10 și 11 din [FAA]." *Id.* § 9.

2. Se vor elabora proceduri pentru a asigura că aceeași încălcare invocată de o persoană nu beneficiază de măsuri reparatorii sau proceduri duplicate.

3. Acțiunea FTC poate continua în paralel cu arbitrajul.

4. Niciun reprezentant al SUA, UE sau al oricărui stat membru al UE sau orice altă autoritate guvernamentală, autoritate publică sau autoritate de executare nu poate participa la aceste arbitraje, cu condiția ca, la cererea unei persoane din UE, autoritățile pentru protecția datelor din UE să poată oferi asistență doar în pregătirea notificării, fără ca APD din UE să aibă acces la materialele divulgate sau la orice alte materiale referitoare la aceste proceduri de arbitraj.

5. Locul arbitrajului este Statele Unite, iar persoana în cauză poate alege participarea telefonică sau video, servicii care vor fi furnizate gratuit. Nu va fi necesară participarea directă.

6. Limba procedurilor de arbitraj va fi limba engleză, cu excepția cazului în care părțile convin altfel. În urma unei cereri justificate și luând în considerare dacă persoana respectivă este reprezentată de un avocat, se oferă servicii de interpretare în cadrul ședinței de arbitraj, precum și traducerea materialelor de arbitraj fără ca persoana în cauză să suporte vreun cost, cu excepția cazului în care comitetul consideră că, în împrejurările specifice de arbitraj, aceasta ar putea conduce la costuri nejustificate sau disproporționate.

7. Materialele prezentate arbitrilor vor fi tratate confidențial și vor fi utilizate numai în legătură cu procedura de arbitraj.

8. Prezentarea dovezilor specifice persoanei în cauză poate fi permisă, dacă este necesar, iar dovezile vor fi tratate confidențial de către părți și vor fi utilizate numai în legătură cu procedura de arbitraj.

9. Arbitrajele trebuie finalizate în termen de 90 de zile de la transmiterea notificării către organizația în cauză, cu excepția cazului în care s-a convenit altfel de către părți.

H. **Costuri**

Arbitrii trebuie să ia măsurile necesare pentru a reduce la minimum costurile sau onorariile arbitrajelor.

Sub rezerva legislației aplicabile, Departamentul Comerțului va facilita instituirea unui fond la care organizațiile care aderă la Scutul de confidențialitate trebuie să plătească o cotizație anuală, bazată, parțial, pe dimensiunea organizației, care va acoperi costurile de arbitraj, inclusiv onorariile arbitrilor, până la sume maxime („plafoane”), în colaborare cu Comisia Europeană. Fondul va fi gestionat de un terț, care va raporta cu regularitate cu privire la activitățile Fondului. În cadrul revizuirii anuale, Departamentul Comerțului și Comisia Europeană vor revizui funcționarea fondului, inclusiv necesitatea de a ajusta valoarea cotizațiilor sau a plafoanelor, și va avea în vedere, printre altele, numărul de arbitri, costurile și calendarul arbitrajelor, cu înțelegerea că nu va exista o sarcină financiară excesivă impusă asupra organizațiilor care aderă la Scutul de confidențialitate. Onorariul avocatului nu este reglementat de prezenta dispoziție sau orice alt fond în temeiul acestei dispoziții.

ANEXA III

Scrisoare din partea Secretarul de Stat al SUA, John Kerry

7 iulie 2016

Stimată Doamnă Comisar Jourová,

Mă bucur că am ajuns la o înțelegere cu privire la Scutul de confidențialitate Uniunea Europeană-Statele Unite ale Americii, care va include un mecanism al Ombudsmanului prin intermediul căruia autoritățile din UE vor fi în măsură să prezinte cereri în numele cetățenilor UE în ceea ce privește practicile SUA de colectare de informații pe baza semnalelor electromagnetice.

La 17 ianuarie 2014, președintele Barack Obama a anunțat reforme importante privind serviciile de informații incluse în Directiva nr. 28 privind politica prezidențială (PPD-28). În temeiul PPD-28, am desemnat Subsecretarul de Stat Catherine A. Novelli, care îndeplinește, de asemenea, funcția de coordonator principal pentru diplomația internațională privind tehnologia informației, în calitate de punct de contact pentru administrațiile străine care doresc să își exprime preocuparea cu privire la activitățile SUA de colectare de informații pe baza semnalelor electromagnetice. Pe baza acestui rol, am instituit un mecanism al Ombudsmanului pentru Scutul de confidențialitate, în conformitate cu dispozițiile prevăzute în anexa A, care au fost actualizate de la scrisoarea mea din 22 februarie 2016. Am desemnat-o pe doamna Subsecretar Novelli să îndeplinească această funcție. Doamna Subsecretar Novelli este independentă de serviciile de informații ale Statelor Unite și îmi raportează direct.

Mi-am îndemnat echipa să aloce resursele necesare pentru punerea în aplicare a acestui nou mecanism al Ombudsmanului și am convingerea că acesta va constitui un mijloc eficace de a răspunde preocupărilor cetățenilor UE.

Cu stimă,

John F. Kerry

Anexa A

Un mecanism al Ombudsmanului pentru Scutul de confidențialitate UE-SUA

În ceea ce privește activitățile de colectare de informații pe baza semnalelor electromagnetice în semn de recunoaștere a importanței cadrului privind Scutul de confidențialitate UE-SUA, prezentul memorandum prezintă procesul de punere în aplicare a unui nou mecanism, compatibil cu Directiva nr. 28 privind politica prezidențială (PPD-28), în ceea ce privește activitățile de colectare de informații pe baza semnalelor electromagnetice ([1]).

La 17 ianuarie 2014, președintele Obama a ținut un discurs în care a anunțat reforme importante privind serviciile de informații. În acest discurs, președintele a subliniat „[e]forturile noastre de a proteja nu numai națiunea din care facem parte, ci și prietenii și aliații noștri. Eforturile noastre vor fi eficiente numai dacă cetățenii obișnuiți din alte țări au încredere că Statele Unite le respectă viața privată". Președintele Obama a anunțat emiterea unei noi directive prezidențiale –PPD-28— pentru a „stabili în mod clar ce facem și ce nu facem, atunci când este vorba despre activitățile noastre supraveghere peste hotare".

Secțiunea 4 litera (d) din PPD-28 obligă secretarul de stat să desemneze „un coordonator principal pentru diplomația internațională privind tehnologia informației" (coordonator principal), „care ... să servească drept punct de contact pentru administrațiile străine care doresc să își exprime îngrijorarea cu privire la activitățile Statelor Unite de colectare de informații pe baza semnalelor electromagnetice". Începând din ianuarie 2015, Subsecretar C. Novelli a servit drept coordonator principal.

Prezentul memorandum descrie un nou mecanism, prin care coordonatorul principal va urmări să faciliteze tratarea cererilor legate de accesul în scopul securității naționale la informații trimise din UE către Statele Unite în temeiul Scutului de confidențialitate, al clauzelor contractuale standard (CCS), al regulilor corporatiste obligatorii (RCO), al „derogărilor" ([2]) sau al „posibilelor derogări viitoare" ([3]), prin căi consacrate în temeiul legilor și politicii Statelor Unite, precum și răspunsul la astfel de cereri.

1. **Ombudsmanul pentru Scutul de confidențialitate.** Coordonatorul principal va servi drept Ombudsman pentru Scutul de confidențialitate și va desemna alți funcționari ai Departamentului de Stat, după caz, să asiste în executarea responsabilităților precizate în prezentul memorandum. (În continuare, coordonatorul și orice alți funcționari care exercită astfel de îndatoriri vor fi denumiți „ombudsmanul pentru Scutul de confidențialitate"). Ombudsmanul pentru Scutul de confidențialitate va colabora îndeaproape cu funcționari din alte departamente și agenții care sunt responsabili cu prelucrarea cererilor în conformitate cu legislația și politicile aplicabile în Statele Unite. Ombudsmanul este independent de serviciile de informații. Ombudsmanul se află în subordinea directă a Secretarului de Stat, care se va asigura că Ombudsmanul își îndeplinește rolul în mod obiectiv și în condiții de independență față de orice influențe neadecvate care riscă să afecteze răspunsul care urmează să fie oferit.

2. **O coordonare eficace.** Ombudsmanul pentru Scutul de confidențialitate va fi în măsură să utilizeze și să își coordoneze acțiunile în mod eficace cu organismele de supraveghere descrise mai jos, pentru a se asigura că răspunsul Ombudsmanului la solicitările care îi sunt adresate de organismul emitent din UE care tratează plângerile individuale se bazează pe informațiile necesare. Atunci când solicitarea se referă la compatibilitatea supravegherii cu

([1]) Cu condiția ca Decizia Comisiei privind caracterul adecvat al protecției oferite de Scutul de confidențialitate UE-SUA să se aplice Islandei, Liechtensteinului și Norvegiei, pachetul privind Scutul de confidențialitate va acoperi atât Uniunea Europeană, cât și aceste trei țări. În consecință, trimiterile la UE și statele sale membre vor fi interpretate ca incluzând Islanda, Liechtenstein și Norvegia.

([2]) În acest context, „derogări" se referă la un transfer sau transferuri comerciale care au loc, cu condiția ca: (a) persoana vizată să își dea consimțământul ferm la transferul avut în vedere; sau (b) transferul să fie 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; sau (c) transferul să fie necesar pentru încheierea sau executarea unui contract încheiat sau care urmează să fie încheiat în interesul persoanei vizate între operator și un terț; sau (d) transferul este necesar sau impus prin lege pentru apărarea unui interes public important sau pentru constatarea, exercitarea sau apărarea unui drept în justiție; sau (e) transferul să fie necesar apărării interesului vital al persoanei vizate; sau (f) transferul să fie 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.

([3]) În acest context, „posibile derogări viitoare" se referă la un transfer sau transferuri comerciale care au loc în una dintre următoarele condiții, în măsura în care condițiile constituie rațiuni legitime pentru transferurile de date cu caracter personal din UE către SUA: (a) persoana vizată și-a exprimat în mod explicit acordul cu privire la transferul propus, după ce a fost informată cu privire la riscurile acestor transferuri pentru persoanele vizate în lipsa unei decizii privind caracterul adecvat al nivelului de protecție și a garanțiilor corespunzătoare; sau (b) transferul este necesar în vederea protejării intereselor vitale ale persoanei vizate sau ale altor persoane, atunci când persoana vizată nu are capacitatea fizică sau juridică de a-și exprima acordul; sau (c) în cazul unui transfer către o țară terță sau o organizație internațională și atunci când nu este aplicabilă niciuna dintre celelalte derogări sau eventuale derogări viitoare nu este aplicabilă, numai în cazul în care transferul nu este repetitiv, se referă doar la un număr limitat de persoane vizate, este imperios necesar pentru realizarea interesului legitim urmărit de operator care să nu prejudicieze interesele sau drepturile și libertățile persoanei vizate și atunci când operatorul a evaluat toate circumstanțele aferente transferului de date și, pe baza acestei evaluări, a prezentat garanții corespunzătoare în ceea ce privește protecția datelor cu caracter personal.

legislația SUA, Ombudsmanul pentru Scutul de confidențialitate va fi în măsură să coopereze cu unul dintre organele de supraveghere independente care dispun de competențe de investigare.

a. Ombudsmanul pentru Scutul de confidențialitate va lucra îndeaproape cu alți agenți guvernamentali din Statele Unite, inclusiv organisme de supraveghere independente adecvate, pentru a se asigura că aceste cereri completate sunt prelucrate și soluționate în conformitate cu legislația și politicile aplicabile. În special, Ombudsmanul pentru Scutul de confidențialitate va putea să colaboreze îndeaproape cu Biroul Directorului Serviciului Național de Informații, Departamentul de Justiție și cu alte departamente și agenții implicate în securitatea națională din Statele Unite, după caz, și cu inspectorii generali, responsabilii pentru Legea privind liberul acces la informații (Freedom of Information Act) și responsabilii pentru protecția libertăților civile și a vieții private.

b. Guvernul Statelor Unite se bazează pe mecanisme pentru coordonarea și supravegherea în materie de securitate națională în diferitele departamente și agenții, pentru a contribui la asigurarea faptului că Ombudsmanul pentru Scutul de confidențialitate este în măsură să răspundă, în sensul secțiunii 4 litera (e), la cereri completate în temeiul secțiunii 3 litera (b).

c. Ombudsmanul pentru Scutul de confidențialitate poate sesiza problemele în legătură cu solicitările comitetului de supraveghere în materie de protecție a vieții private și a libertății civile în vederea examinării.

3. **Depunerea cererilor**

a. Cererile vor fi prezentate inițial autorităților statelor membre responsabile de supravegherea serviciilor de securitate națională și/sau de prelucrarea datelor cu caracter personal de către autoritățile publice. Cererile vor fi prezentate Ombudsmanului de către un organism centralizat al UE (denumite în continuare împreună: „organismul UE de tratare a plângerilor individuale"):

b. Organismul UE de tratare a plângerilor individuale se va asigura că cererea este completă, pe baza următoarelor acțiuni:

(i) Verifică identitatea persoanei în cauză și dacă persoana acționează în nume propriu și nu ca reprezentant al unei organizații guvernamentale sau interguvernamentale.

(ii) Se asigură că cererea se face în scris și conține următoarele informații de bază:

— orice informație care face obiectul cererii,

— natura informațiilor sau a măsurilor solicitate,

— entitățile Guvernului Statelor Unite despre care se crede că sunt implicate, dacă este cazul, și

— alte măsuri urmăresc să obțină informațiile sau măsurile solicitate și răspunsul primit prin intermediul măsurilor respective.

(iii) Verifică dacă cererea se referă la date despre care se poate considera în mod rezonabil că au fost transferate din UE către Statele Unite în temeiul Scutului de confidențialitate, al CCS, al RCO, al derogărilor sau posibilelor derogări viitoare.

(iv) Face o determinare inițială că cererea nu este neserioasă, nejustificată sau făcută cu rea-credință.

c. Pentru a se completa în scopul abordării ulterioare de către Ombudsmanul pentru Scutul de confidențialitate în temeiul prezentului memorandum, cererea nu trebuie să demonstreze că datele solicitantului au fost accesate de către guvernul Statelor Unite prin activități de colectare de informații pe baza semnalelor electromagnetice.

4. **Angajamentele de a comunica cu organismul emitent din UE de tratare a plângerilor individuale.**

a. Ombudsmanul pentru Scutul de confidențialitate va confirma primirea cererii organismului emitent din UE de tratare a plângerilor individuale.

b. Ombudsmanul pentru Scutul de confidențialitate va efectua o primă examinare pentru a verifica dacă cererea a fost completată în conformitate cu secțiunea 3 litera (b). În cazul în care Ombudsmanul pentru Scutul de confidențialitate constată deficiențe sau are întrebări referitoare la completarea cererii, Ombudsmanul pentru Scutul de confidențialitate va încerca să abordeze și să soluționeze aceste probleme cu organismul emitent din UE de tratare a plângerilor individuale.

c. În cazul în care, pentru a facilita prelucrarea adecvată a cererii, Ombudsmanul pentru Scutul de confidențialitate are nevoie de mai multe informații despre cerere sau dacă sunt necesare acțiuni specifice care să fie întreprinse de către persoana care a prezentat inițial cererea, Ombudsmanul pentru Scutul de confidențialitate informează în acest sens organismul emitent din UE de tratare a plângerilor individuale.

d. Ombudsmanul pentru Scutul de confidențialitate va urmări stadiul cererilor și va furniza actualizări, după caz, organismului emitent din UE de tratare a plângerilor individuale.

e. Odată ce o cerere a fost completată, astfel cum se descrie în secțiunea 3 din prezentul memorandum, Ombudsmanul pentru Scutul de confidențialitate va oferi în timp util un răspuns adecvat organismului emitent din UE de tratare a plângerilor individuale, sub rezerva menținerii obligației de a proteja informațiile în conformitate cu legislația și politicile aplicabile. Ombudsmanul pentru Scutul de confidențialitate va oferi un răspuns organismului emitent din UE de tratare a plângerilor individuale, confirmând că (i) plângerea a fost examinată în mod corespunzător și (ii) s-a respectat legislația SUA, statutul, ordinele executive, directivele prezidențiale și politicile agenției, care furnizează limitele și garanțiile descrise în scrisoarea ODNI sau, în caz de neconformitate, o astfel de neconformitate a fost remediată. Ombudsmanul pentru Scutul de confidențialitate nu va confirma, nici nu va infirma că persoana a fost vizată de acțiuni de supraveghere, nici nu va confirma calea de atac care a fost aplicată. Astfel cum s-a explicat în secțiunea 5, cererile FOIA vor fi prelucrate în conformitate cu statutul menționat și normele aplicabile.

f. Ombudsmanul pentru Scutul de confidențialitate va comunica direct cu organismul UE de tratare a plângerilor individuale, care, la rândul său, va fi responsabil pentru comunicarea cu solicitantul. În cazul în care comunicările directe fac parte din unul dintre procesele subiacente descrise mai jos, comunicările respective se vor efectua în conformitate cu procedurile existente.

g. Angajamentele din prezentul memorandum nu se aplică declarațiilor cu caracter general potrivit cărora Scutul de confidențialitate UE-SUA respectă cerințele Uniunii Europene privind protecția datelor. Angajamentele din prezentul memorandum se bazează pe înțelegerea comună de către Comisia Europeană și Guvernul SUA că, având în vedere domeniul de aplicare a angajamentelor asumate în temeiul acestui mecanism, pot apărea constrângeri legate de resurse, inclusiv în ceea ce privește cererile în baza Legii privind liberul acces la informații (Freedom of Information Act – FOIA). În cazul în care îndeplinirea funcțiilor Ombudsmanului pentru Scutul de confidențialitate depășește constrângerile rezonabile în materie de resurse și împiedică îndeplinirea acestor angajamente, guvernul SUA va discuta cu Comisia Europeană orice modificări care ar putea fi necesare pentru a remedia situația.

5. **Cererile de informații.** Cererile de acces la arhivele administrative din Statele Unite pot fi formulate și prelucrate în conformitate cu Legea privind liberul acces la informații (Freedom of Information Act – FOIA).

a. FOIA oferă posibilitate de acces oricărei persoane care solicită accesul la registrele agențiilor federale, indiferent de naționalitatea solicitantului. Acest statut este codificat în Codul Statelor Unite la 5 U.S.C § 552. Statutul, împreună cu informații suplimentare despre FOIA, sunt disponibile la adresele www.FOIA.gov și http://www.justice.gov/oip/foia-resources. Fiecare agenție are un funcționar-șef responsabil cu FOIA și a furnizat informații pe site-ul său web public cu privire la modul de depunere a unei cereri FOIA la agenție. Agențiile au procese de consultare între ele cu privire la cererile FOIA care implică registre deținute de o altă agenție.

b. De exemplu:

(i) Biroul Directorului Serviciului Național de Informații (ODNI) a creat un portal ODNI FOIA pentru ODNI: http://www.dni.gov/index.php/about-this-site/foia. Portalul oferă informații cu privire la depunerea unei cereri, verificarea statutului unei cereri existente, precum și în ceea ce privește accesul la informații care au fost comunicate și publicate de ODNI în temeiul FOIA. Portalul ODNI FOIA include link-uri către alte site-uri FOIA pentru elemente IC: http://www.dni.gov/index.php/about-this-site/foia/other-ic-foia-sites.

(ii) Biroul pentru politica de informare din cadrul Departamentului de Justiție oferă informații detaliate cu privire la FOIA: http://www.justice.gov/oip. Acesta cuprinde nu numai informații despre depunerea unei cereri FOIA la Departamentul de Justiție, ci oferă, de asemenea, orientări pentru guvernul Statelor Unite privind interpretarea și aplicarea cerințelor FOIA.

c. În temeiul FOIA, accesul la arhivele administrative este supus anumitor excepțări enumerate. Acestea includ limitări privind accesul la informații clasificate privind securitatea națională, informații cu caracter personal ale terților, precum și informații privind anchetele organelor de aplicare a legii și pot fi comparate cu limitele impuse de fiecare stat membru al UE prin propria legislație privind accesul la informații. Aceste restricții se aplică în egală măsură americanilor și persoanelor cu o altă cetățenie.

d. Litigiile privind eliberarea documentelor solicitate în temeiul FOIA, pot face obiectul unui recurs administrativ și apoi la un tribunal federal. Instanța este obligată să pronunțe o nouă hotărâre cu privire la faptul refuzul accesului la arhive este întemeiat, 5 U.S.C. § 552(a)(4)(B), și poate obliga guvernul să asigure accesul la arhive. În unele cazuri, instanțele au respins afirmațiile guvernului conform cărora ar trebui să se refuze accesul la informații ca fiind clasificate. Deși nu sunt disponibile despăgubiri financiare, instanțele pot acorda plata onorariilor avocaților.

6. **Cererile de măsuri suplimentare.** O cerere privind o presupusă încălcare a legii sau altă abatere va fi transmisă organismului administrativ american corespunzător, inclusiv organismelor independente de supraveghere cu competența de a examina cererea respectivă și de a soluționa neconformitatea, după cum este descris mai jos.

a. Inspectorii generali sunt independenți din punct de vedere statutar; aceștia au competență amplă de a efectua investigații, audituri și evaluări ale programelor, inclusiv cazuri de fraudă și abuz sau încălcare a legii și pot recomanda acțiuni corective.

(i) Legea privind Inspectorul general din 1978, astfel cum a fost modificată, a stabilit inspectorii generali (IG) federali ca unități independente și obiective în majoritatea agențiilor ale căror sarcini sunt de a lupta împotriva risipei, fraudei și abuzului în programele și operațiunile agențiilor respective. În acest scop, fiecare inspector general este responsabil pentru efectuarea de audituri și investigații privind programele și operațiunile agenției sale. În plus, inspectorii generali vor asigura conducerea și coordonarea și vor recomanda politici pentru activități menite să promoveze principiile economiei, eficienței și eficacității, precum și prevenirea și detectarea fraudelor și abuzurilor, în programele și activitățile agenției.

(ii) Fiecare element din cadrul serviciilor de informații are propriul birou al inspectorului general însărcinat cu supravegherea activităților serviciilor de informații străine, printre altele. O serie de rapoarte ale inspectorului general privind programele serviciilor de informații au fost făcute publice.

(iii) De exemplu:

— Biroul inspectorului general al serviciilor de informații (IC IG) a fost înființat în temeiul secțiunii 405 din Legea privind autorizarea serviciilor de informații din anul fiscal 2010. Biroul inspectorului general al serviciilor de informații este responsabil cu efectuarea de audituri, investigații, inspecții și evaluări care să identifice și să abordeze riscurile sistemice, punctele slabe și deficiențele care traversează misiunile agenției serviciilor de informații, pentru a avea un impact pozitiv asupra economiilor și eficienței la nivelul serviciilor de informații. IC IG este autorizat să investigheze reclamații sau informații cu privire la acuzațiile de încălcare a legii, a normelor și a reglementărilor, de risipă, de fraudă, de abuz de autoritate sau un pericol substanțial sau specific pentru sănătatea și siguranța publică în legătură cu programele și activitățile de colectare de informații ale ODNI și/sau IC. IG IC oferă informații privind modul în care puteți contacta direct IG IC pentru a prezenta un raport: http://www.dni.gov/index.php/about-this-site/contact-the-ig.

— Biroului inspectorului general (Office of the Inspector General – OIG) din cadrul Departamentului de Justiție al SUA (DOJ) este o entitate independentă creată din punct de vedere statutar a cărei misiune este detectarea și descurajarea risipei, a fraudei, a abuzurilor și abaterilor în cadrul programelor Departamentului de Justiție (DOJ) și în cazul personalului acestuia, precum și promovarea economiei și eficienței acestor programe. OIG investighează presupusele încălcări ale legislației civile și penale de către angajați DOJ și efectuează, de asemenea, audituri și inspecții ale programelor DOJ. OIG are competența de a examina toate reclamațiile de conduită necorespunzătoare înaintate împotriva Departamentului de Justiție, inclusiv Biroul Federal de Investigații; Administrația pentru Combaterea Traficului cu Droguri; Biroul Federal al Închisorilor; Serviciul Șerifilor SUA; Biroul pentru Alcool, Tutun, Arme de Foc și Explozivi; Birourile Procurorilor din Statele Unite ale Americii; și angajații care lucrează în alte unități sau birouri din cadrul Departamentului de Justiție. (Singura excepție o constituie acuzațiile de abuzuri săvârșite de un procuror din cadrul departamentului sau de personalul responsabil cu aplicarea legii în legătură cu exercitarea competenței procurorului de a investiga, de a acționa în instanță sau de a furniza

asistență juridică, care sunt responsabilitatea Biroului de responsabilitate profesională al Departamentului). În plus, în temeiul secțiunii 1001 din USA Patriot Act, promulgată la 26 octombrie 2001, Inspectorul General trebuie să examineze informații și să primească plângerile privind presupuse încălcări ale drepturilor civile și libertăților civile de către angajați ai Departamentului de Justiție. OIG menține un site internet public – https://www.oig.justice.gov – care include o „linie de asistență telefonică" pentru depunerea de plângeri – https://www.oig.justice.gov/hotline/index.htm.

b. Birourile și entitățile pentru protecția vieții private și a libertăților civile din cadrul guvernului Statelor Unite ale Americii au, de asemenea, responsabilități în domeniu. De exemplu:

(i) Secțiunea 803 din recomandările de punere în aplicare a Legii Comisiei 9/11 din 2007, codificate în Codul Statelor Unite la 42 U.S.C. § 2000-ee1, stabilește responsabili pentru protecția vieții private și a libertăților civile în unele departamente și agenții (inclusiv Departamentul de Stat, Departamentul de Justiție și ODNI). Secțiunea 803 prevede că responsabilii pentru protecția vieții private și a libertăților civile vor servi drept consilieri principali, printre altele, pentru a se asigura că departamentul, agenția sau elementul dispune de proceduri adecvate pentru soluționarea plângerilor adresate de persoane care susțin că departamentul, agenția sau elementul le-a încălcat dreptul la viață privată și libertățile civile.

(ii) Biroul pentru protecția vieții private și a libertăților civile al ODNI (ODNI CLPO) este condus de către responsabilul pentru protecția libertăților civile, poziție stabilită de Legea privind securitatea națională din 1948, astfel cum a fost modificată. Atribuțiile ODNI CLPO includ garantarea faptului că politicile și procedurile componentelor serviciilor de informații cuprind elemente adecvate de protecție a vieții private și a libertăților civile, precum și revizuirea și examinarea plângerilor legate de abuzuri sau de încălcarea libertăților civile și a vieții private în programele și activitățile ODNI. ODNI CLPO oferă publicului informații pe site-ul său internet, inclusiv instrucțiuni privind modul de depunere a unei plângeri: www.dni.gov/clpo. În cazul în care ODNI CLPO primește o plângere legată de viața privată și libertățile civile care implică programele și activitățile serviciilor de informații, acesta va asigura coordonarea cu alte componente ale serviciilor de informații privind modul în care această plângere ar trebui să fie examinată ulterior în cadrul serviciilor de informații. Este de remarcat că și Agenția Națională de Securitate (NSA) are un birou pentru protecția libertăților civile și a vieții private, care oferă informații cu privire la responsabilitățile sale pe site-ul acesteia – https://www.nsa.gov/civil_liberties/. Dacă informațiile indică faptul că agenția nu respectă cerințele de protecție a vieții private (de exemplu, o cerință în temeiul secțiunii 4 din PPD-28), agențiile dispun de mecanisme de asigurare a conformității care trebuie să revizuiască și să remedieze incidentul. Agențiile au obligația să raporteze la ODNI incidentele legate de conformitate în temeiul PPD-28.

(iii) Biroul pentru protecția vieții private și a libertăților civile (OPCL) din cadrul Departamentului de Justiție sprijină sarcinile și responsabilitățile responsabiluluișef pentru protecția vieții private și a libertăților civile din cadrul Departamentului (CPCLO). Misiunea principală a OPCL este protejarea vieții private și a libertăților civile ale cetățenilor americani prin examinarea, supravegherea și coordonarea operațiunilor în materie de protecție a vieții private ale Departamentului. OPCL furnizează consultanță juridică și îndrumări la nivel ministerial; asigură respectarea vieții private din partea Departamentului, inclusiv conformitatea cu Legea privind protecția informațiilor cu caracter personal din 1974, dispozițiile privind protecția vieții private atât din Legea privind eguvernarea din 2002, cât și din Legea privind gestionarea securității informațiilor, precum și cu directivele administrației adoptate pentru promovarea acestor legi; dezvoltă și furnizează formare în domeniul protecției vieții private la nivelul Departamentului; sprijină CPCLO în dezvoltarea politicii de confidențialitate a Departamentului; pregătește rapoarte privind protecția vieții private pentru președinte și Congres; și verifică practicile de gestionare a informațiilor ale Departamentului pentru a se asigura că acestea sunt în concordanță cu protecția vieții private și a libertăților civile. OPCL oferă publicului informații cu privire la responsabilitățile sale pe site-ul http://www.justice.gov/opcl.

(iv) În conformitate cu 42 U.S.C. § 2000ee și urm., comitetul de supraveghere a vieții private și a libertăților civile trebuie să revizuiască în mod continuu (i) politicile și procedurile, precum și punerea lor în aplicare, ale departamentelor, agențiilor și ale elementelor executivului referitoare la eforturile de a proteja țara împotriva terorismului pentru a asigura protecția vieții private și a libertăților civile și (ii) alte acțiuni întreprinse de executiv referitoare la aceste eforturi pentru a stabili dacă astfel de măsuri asigură o protecție corespunzătoare a vieții private și a libertăților civile și sunt în conformitate cu legislația aplicabilă, reglementările și politicile privind viața privată și libertățile civile. Acesta primește și examinează rapoartele și alte informații din partea responsabililor cu atribuții de protecție a vieții private și a libertăților civile și, după caz, formulează recomandări cu privire la activitățile lor. Secțiunea 803 din recomandările de punere în aplicare a Legii Comisiei 9/11 din 2007, codificate în Codul Statelor Unite la 42 U.S.C. § 2000ee-1, solicită responsabililor pentru protecția vieții private și a libertăților civile din opt agenții federale (inclusiv secretarul apărării, secretarul pentru securitate internă, directorul serviciilor de informații naționale și directorul Agenției Centrale

de Informații), precum și din orice altă agenție desemnată de comitet, să prezinte la PCLOB rapoarte periodice, inclusiv numărul, natura și soluționarea plângerilor primite de către agenție pentru presupuse încălcări. Statutul de abilitare al PCLOB obligă comitetul să primească aceste rapoarte și, dacă este cazul, să formuleze recomandări adresate responsabililor pentru protecția vieții private și a libertăților civile în ceea ce privește activitățile lor.

ANEXA IV

Scrisoarea președintei Comisiei Federale pentru Comerț, Edith Ramirez

7 iulie 2016

Prin EMAIL

Věra Jourová
Comisarul pentru justiție, consumatori și egalitate de gen
Comisia Europeană
Rue de la Loi/Wetstraat 200
1049 Bruxelles
Belgia

Stimată Doamnă Comisar Jourová,

Comisia Federală pentru Comerț a Statelor Unite („FTC") apreciază posibilitatea de a descrie modul de asigurare a respectării noului cadru privind Scutul de confidențialitate UE-SUA („cadrul privind Scutul de confidențialitate" sau „cadrul"). Considerăm că acest cadru va juca un rol esențial în facilitarea tranzacțiilor comerciale cu protejarea vieții private într-o lume din ce în ce mai interconectată. Acesta va permite întreprinderilor să efectueze operațiuni importante în economia globală, asigurând în același timp protecția vieții private a consumatorilor din UE. FTC s-a angajat de multă vreme să protejeze viața privată la nivel transfrontalier, iar punerea în aplicare a noului cadru constituie o prioritate majoră. În continuare, vom explica istoricul FTC de asigurare a respectării vieții private în general, inclusiv asigurarea respectării programului inițial privind sfera de siguranță, precum și abordarea FTC în ceea ce privește asigurarea respectării noului cadru.

FTC și-a exprimat pentru prima dată în mod public angajamentul de a aplica programul privind sfera de siguranță în anul 2000. La acel moment, președintele de atunci al FTC, Robert Pitofsky, a transmis Comisiei Europene o scrisoare evidențiind angajamentul FTC de a adera cu strictețe la principiile sferei de siguranță privind protecția vieții private. FTC a continuat să mențină acest angajament prin aproape 40 de măsuri de asigurare a respectării, numeroase anchete suplimentare și cooperarea cu autoritățile europene pentru protecția datelor (denumite în continuare „APD din UE") în chestiuni de interes comun.

După ce, în noiembrie 2013, Comisia Europeană și-a exprimat preocuparea cu privire la administrarea și asigurarea respectării programului privind sfera de siguranță, FTC și Departamentul Comerțului al SUA au început consultări cu funcționari din cadrul Comisiei Europene pentru a analiza modalitățile de consolidare a acestuia. În timpul desfășurării acestor consultări, la 6 octombrie 2015, Curtea Europeană de Justiție a pronunțat o hotărâre în cauza *Schrems* care, printre altele, anulează decizia Comisiei Europene cu privire la caracterul adecvat al programului privind sfera de siguranță. Ca urmare a hotărârii, am continuat să colaborăm îndeaproape cu Departamentul Comerțului al Statelor Unite ale Americii și Comisia Europeană, în efortul de a consolida măsurile de protecție a vieții private oferite persoanelor din UE. Cadrul privind Scutul de confidențialitate este rezultatul acestor consultări în curs. La fel ca în cazul programului privind sfera de siguranță, FTC se angajează la o punere în aplicare viguroasă a noului cadru. Prezenta scrisoare consacră acest angajament.

În special, ne afirmăm angajamentul în patru domenii principale: (1) prioritizarea sesizărilor și investigații; (2) abordarea afirmațiilor false sau frauduloase privind calitatea de participant la Scutul de confidențialitate; (3) monitorizarea continuă; și (4) consolidarea angajamentului și cooperarea cu autoritățile pentru protecția datelor din UE în vederea asigurării respectării. Prezentăm mai jos informații detaliate cu privire la fiecare dintre aceste angajamente și contextul relevant cu privire la rolul FTC în protejarea vieții private a consumatorilor și punerea în aplicare a programului privind sfera de siguranță, precum și contextul mai amplu al protecției vieții private în Statele Unite ([1]).

I. CONTEXTUL

A. **Activitățile FTC în materie de politică și de asigurare a respectării vieții private**

FTC dispune de o competență amplă de aplicare a legii de drept civil pentru a promova protecția consumatorilor și concurența în domeniul comercial. Ca parte a mandatului său de protecție a consumatorilor, FTC aplică o gamă largă de

([1]) În apendicele A oferim informații suplimentare cu privire la legislația federală și statală din SUA privind protecția vieții private. În plus, un rezumat al acțiunilor noastre recente de punere în aplicare în cazuri privind protecția vieții private și securitatea poate fi consultat pe site-ul FTC, la adresa https://www.ftc.gov/reports/privacy-data-security-update-2015.

norme de protecție a vieții private și de securitate a datelor consumatorilor. Legislația primară aplicată de FTC, Legea privind FTC, interzice actele sau practicile „neloiale" și „înșelătoare" în domeniul comerțului sau care afectează comerțul ([1]). O reprezentare, omisiune sau practică este înșelătoare în cazul în care aceasta este semnificativă și poate să inducă în eroare consumatorii care acționează în mod rezonabil în circumstanțele date ([2]).Un act sau o practică este considerată neloial(ă) în cazul în care cauzează sau este susceptibilă să cauzeze un prejudiciu important care ar fi putut fi evitat în mod rezonabil de către consumatori sau care nu este compensat prin avantajele pentru consumatori sau concurență ([3]). FTC aplică, de asemenea, statute specifice care protejează informațiile referitoare la sănătate, la credite și la alte aspecte financiare, precum și informații online despre copii și a publicat o serie de regulamente de punere în aplicare a fiecăruia dintre aceste statute.

Competența FTC în temeiul Legii privind FTC se referă la aspecte de natură „comercială". FTC nu are competență în aplicarea legii penale sau probleme de securitate națională. De asemenea, FTC nu poate aplica majoritatea celorlalte măsuri guvernamentale. În plus, există excepții de la competența FTC în activități comerciale, inclusiv în ceea ce privește băncile, companiile aeriene, activitățile de asigurare și activitățile de transport comune desfășurate de furnizorii de servicii de telecomunicații. De asemenea, FTC nu are competență în ceea ce privește cea mai mare parte a organizațiilor non-profit, dar are competență în ceea ce privește organizațiile caritabile fictive sau organizațiile non-profit care în realitate operează pentru profit. De asemenea, FTC dispune de competență în ceea ce privește organizațiile non-profit care funcționează în avantajul membrilor cu scop lucrativ, inclusiv prin furnizarea de beneficii economice pentru membrii respectivi ([4]). În anumite situații, competența FTC coexistă cu cea a altor agenții de aplicare a legii.

Am stabilit o serie de relații strânse cu autoritățile federale și de stat și colaborăm îndeaproape cu acestea pentru a coordona anchete sau pentru a face sesizări, după caz.

Asigurarea respectării este axa centrală a abordării FTC în ceea ce privește protecția vieții private. Până în prezent, FTC a introdus peste 500 de cazuri privind protecția vieții private și securitatea informațiilor consumatorilor. Acest ansamblu de cazuri acoperă atât informații offline, cât și online și include măsuri de asigurare a respectării împotriva companiilor mari și mici, susținând că acestea nu au eliminat în mod corespunzător datele sensibile ale consumatorilor, nu au protejat informațiile cu caracter personal ale consumatorilor, au urmărit consumatorii online în mod înșelător, au trimis mesaje spam consumatorilor, au instalat programe spion sau programe malware pe calculatoarele consumatorilor, au încălcat normele privind interdicția apelurilor și alte norme privind telemarketing-ul și au făcut schimb cu informațiile consumatorului colectate și comunicate în mod inadecvat pe dispozitive mobile. Măsurile de asigurare a respectării ale FTC – atât în mediul fizic, cât și în cel digital – transmit un mesaj important companiilor cu privire la nevoia de a proteja viața privată a consumatorilor.

De asemenea, FTC a urmărit numeroase inițiative de politică menite să sporească protecția vieții private a consumatorilorm care stau la baza activității sale de asigurare a respectării. FTC a a găzduit ateliere și a emis rapoarte cu recomandarea celor mai bune practici care vizează îmbunătățirea vieții private în ecosistemul mobil; creșterea transparenței industriei brokerajului de date; maximizarea beneficiilor volumelor mari de date, diminuând în același timp riscurile acestora, în special pentru consumatorii cu venituri mici și insuficient deserviți; și sublinierea implicațiilor (referitoare la viață privată și securitate) ale programelor de recunoaștere facială și ale internetului obiectelor, printre alte domenii.

De asemenea, FTC participă la educația consumatorilor și a mediului de afaceri pentru a îmbunătăți impactul inițiativelor sale de dezvoltare de politici și de asigurare a respectării. FTC a folosit o varietate de instrumente – publicații, resurse online, ateliere și social media – pentru a furniza materiale educaționale cu privire la o gamă largă de subiecte, inclusiv aplicații mobile, viața privată a copiilor, precum și securitatea datelor. Cel mai recent, Comisia a lansat inițiativa „Începe cu securitatea", care include noi orientări pentru întreprinderi pe baza lecțiilor învățate din cazurile agenției privind securitatea datelor, precum și o serie de ateliere în întreaga țară. De asemenea, FTC a fost mult timp lider în educarea consumatorilor cu privire la securitatea informatică de bază. Anul trecut, site-ul online OnGuard și corespondentul acestuia în limba spaniolă, Alerta en Línea, a avut peste 5 milioane de vizualizări de pagină.

B. **Protecția juridică în SUA de care beneficiază consumatorii UE**

Cadrul va funcționa în contextul american mai amplu al protecției vieții private, care protejează consumatorii europeni în mai multe moduri.

([1]) 15 U.S.C. § 45(a).
([2]) A se vedea Declarația de politică a FTC privind înșelătoria, anexată la Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984), disponibilă la adresa https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.
([3]) A se vedea 15 U.S.C. § 45. Declarația de politică a FTC privind caracterul abuziv, anexată la Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984), disponibilă la adresa https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.
([4]) A se vedea California Dental Ass'n/FTC, 526 U.S. 756 (1999).

Interdicția inclusă în Federal Trade Commission Act privind actele sau practicile neloiale sau frauduloase nu se limitează la protecția consumatorilor din SUA de întreprinderile din SUA, întrucât acesta include practicile care (1) cauzează sau riscă să cauzeze un prejudiciu previzibil în mod rezonabil în Statele Unite, sau (2) implică comportamente materiale în Statele Unite. De asemenea, FTC poate utiliza toate căile de atac, inclusiv restituirea, care sunt disponibile pentru a proteja consumatorii de la nivel național atunci când protejează consumatorii străini.

Într-adevăr, activitățile de asigurare a respectării întreprinse de FTC în SUA aduc beneficii atât consumatorilor americani, cât și celor străini. De exemplu, cazurile noastre de aplicare a articolului 5 din Federal Trade Commission Act au protejat dreptul consumatorilor americani și străini la viață privată. Într-un caz împotriva unui broker de informații, Accusearch, FTC a declarat că vânzarea de către această întreprindere de înregistrări telefonice confidențiale către terți fără consimțământul sau cunoștința consumatorilor a fost o practică neloială, încălcând articolul 5 din legea Federal Trade Commission Act. Accusearch a vândut informații referitoare atât la consumatori americani, cât și străini ([1]). Instanța a admis acțiunea în încetare împotriva Accusearch interzicând, printre altele, comercializarea sau vânzarea informațiilor personale ale consumatorilor, fără acordul scris al acestora, cu excepția cazului în care au fost obținute în mod legal din informații disponibile în mod public și a dispus confiscarea a aproximativ 200 000 USD ([2]).

Abordarea de către FTC a cazului TRUSTe reprezintă un alt exemplu. Aceasta asigură că toți consumatorii, inclusiv cei din Uniunea Europeană, se pot baza pe declarațiile făcute de o organizație mondială de autoreglementare cu privire la controlul și certificarea serviciilor online interne și externe ([3]). În special, acțiunile noastre împotriva TRUSTe consolidează, de asemenea, sistemul de autoreglementare privind protejarea vieții private în mai mare măsură prin asigurarea răspunderii entităților care joacă un rol important în sistemele de autoreglementare, inclusiv cadrele transfrontaliere de protecție a vieții private.

De asemenea, FTC asigură aplicarea altor legi specifice ale căror măsuri de protecție se extind la persoane care nu sunt cetățeni ai SUA, cum ar fi Legea privind protecția copiilor pe internet („COPPA"). Printre altele, COPPA impune operatorilor de servicii online și site-uri internet care vizează copiii sau de site-uri care vizează publicul general care colectează cu bună știință informații cu caracter personal de la copii sub vârsta de 13 ani, să furnizeze o notificare parentală și să obțină consimțământul verificabil al părinților. Site-urile internet și serviciile stabilite în SUA care fac obiectul COPPA și care colectează informații cu caracter personal de la copii străini sunt obligați să respecte dispozițiile COPPA. Site-urile internet și serviciile online stabilite în străinătate, trebuie, de asemenea, să respecte COPPA dacă vizează direct copii din Statele Unite ale Americii sau în cazul în care colectează în cunoștință de cauză informații cu caracter personal de la copii în Statele Unite. În plus față de legislația federală americană aplicată de FTC, alte legi specifice federale și statale de protecție a consumatorilor și a vieții private pot aduce beneficii suplimentare pentru consumatorii din UE.

C. **Asigurarea respectării programului privind sfera de siguranță**

În cadrul programului de asigurare a respectării vieții private și a securității, FTC a urmărit, de asemenea, să protejeze consumatorii europeni prin măsuri de asigurare a respectării legate de încălcări ale principiilor sferei de siguranță. FTC a introdus 39 de măsuri de asigurare a respectării referitoare la programul privind sfera de siguranță: 36 de acuzații de declarații de certificare false și trei cazuri – împotriva Google, Facebook și Myspace – care implică presupuse încălcări ale principiilor privind protecția vieții private din cadrul sferei de siguranță ([4]). Aceste cazuri demonstrează caracterul executoriu al certificărilor și repercusiunile pentru neconformitate. Ordonanțele prin consimțământ de douăzeci de ani impun companiilor Google, Facebook și MySpace să pună în aplicare programe cuprinzătoare de protecție a vieții private care trebuie să fie concepute în mod rezonabil pentru a aborda riscurile la adresa vieții private asociate cu dezvoltarea și gestionarea de produse și servicii noi și existente și pentru a proteja viața privată și confidențialitatea informațiilor personale. Programele cuprinzătoare de protecție a confidențialității, mandatate în conformitate cu aceste ordine, trebuie să identifice riscurile previzibile și să dispună de măsuri de control pentru a elimina riscurile respective. De asemenea, companiile trebuie să facă obiectul unor evaluări independente continue ale programelor de protejare a vieții private ale acestora, evaluări care trebuie efectuate de către FTC. De asemenea, ordinele interzic acestor companii să facă declarații false privind practicile lor în materie de protejare a vieții private și participarea lor la orice program de protecție a vieții private sau a securității. În plus, această interdicție se aplică acțiunilor și practicilor companiilor în temeiul noului cadru privind Scutul de confidențialitate. FTC poate asigura executarea acestor ordine prin solicitarea

([1]) A se vedea Biroul comisarului responsabil de protecția vieții private din Canada, Plângere în cazul PIPEDA/Accusearch, Inc., care desfășoară activități comerciale ca Abika.com, https://www.priv.gc.ca/cf-dc/2009/2009_009_0731_e.asp. Biroul comisarului responsabil de protecția vieții private din Canada a depus o cerere *amicus curiae* în recursul acțiunii FTC și a efectuat propria anchetă, concluzionând că practicile Accusearch au încălcat și legea canadiană.

([2]) A se vedea *FTC/Accusearch, Inc.*, nr. 06CV015D (D. Wyo. 20 dec. 2007), *aff'd* 570 F.3d 1187 (10th Cir. 2009).

([3]) A se vedea *In the Matter of True Ultimate Standards Everywhere, Inc.*, nr. C-4512 (F.T.C. 12 martie 2015) (decizie și ordin), disponibilă la adresa https://www ftc.gov/system/files/documents/cases/150318trust-edo.pdf.

([4]) A se vedea *In the Matter of Google, Inc.*, nr. C-4336 (F.T.C. 13 octombrie 2011) (decizie și ordin), disponibilă la adresa https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz; *In the Matter of Facebook, Inc.*, No. C-4365 (F.T.C. 27 iulie 2012) (decizie și ordin), disponibilă la adresa https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook; *In the Matter of Myspace LLC*, No. C-4369 (F.T.C. 30 august 2012) (decizie și ordin), disponibilă la adresa https://www.ftc.gov/news-events/press-releases/2012/09/ftc-finalizes-privacy-settlement-myspace.

unor sancțiuni de drept civil. Concret, în 2012 Google a plătit sancțiuni de drept civil în valoare de 22,5 milioane USD, ceea ce constituie un record, în urma acuzațiilor potrivit cărora a încălcat ordinul FTC. În consecință, astfel de ordine ale FTC contribuie la protejarea a peste un miliard de consumatori din întreaga lume, din care sute de milioane locuiesc in Europa.

Cazurile FTC s-au concentrat, de asemenea, asupra declarațiilor false, frauduloase sau înșelătoare cu privire la participarea la programul privind sfera de siguranță. FTC ia în considerare în mod serios astfel de afirmații. De exemplu, în cauza FTC/Karnani, FTC a formulat o acțiuneîn 2011 împotriva unui comerciant online din Statele Unite, afirmând că acesta și societatea sa au înșelat consumatorii britanici, făcându-i să creadă că societatea își avea sediul în Regatul Unit, inclusiv prin utilizarea extensiilor pe internet.uk și trimiterile la moneda britanică și sistemul poștal din Regatul Unit ([1]). Cu toate acestea, atunci când consumatorii au primit produsele, au descoperit taxe la import neașteptate, garanții care nu erau valide în Regatul Unit și cheltuieli asociate cu obținerea de rambursări. De asemenea, FTC a acuzat inculpații că au înșelat consumatorii cu privire la participarea lor la programul privind sfera de siguranță. De remarcat că toate victimele sunt consumatori din Regatul Unit.

Multe dintre celelalte cazuri ale noastre de asigurare a respectării programului privind sfera de siguranță au implicat organizații care au aderat la programul privind sfera de siguranță, dar nu și-au reînnoit certificarea anuală și au continuat să se prezinte drept participanți actuali. Astfel cum se arată mai jos, FTC se angajează, de asemenea, să abordeze afirmațiile false cu privire la participarea la cadrul privind Scutul de confidențialitate. Această activitate strategică de asigurare a respectării va completa acțiunile mai intense ale Departamentului Comerțului în vederea verificării conformității cu cerințele programului pentru certificare și recertificare, activitățile de monitorizare a conformității efective, inclusiv prin utilizarea unor chestionare în rândul participanților la cadru, precum și eforturile sporite pentru identificarea falșilor participanți la cadru și utilizarea necorespunzătoare a oricărei mărci de certificare a participării la cadru ([2]).

II. PRIORITIZAREA SESIZĂRILOR ȘI INVESTIGAȚII

Astfel cum a procedat în cadrul programului privind sfera de siguranță, FTC s-a angajat să acorde prioritate sesizărilor privind Scutul de confidențialitate primite din state membre ale UE. De asemenea, vom acorda prioritate sesizărilor privind încălcarea orientărilor de autoreglementare referitoare la cadrul privind Scutul de confidențialitate primite de la organizații de autoreglementare în materie de viață privată și de la alte organisme independente de soluționare a litigiilor.

Pentru a facilita primirea sesizărilor în temeiul cadrului Scutului de confidențialitate de la statele membre ale UE, FTC creează un proces de sesizare standard și oferă orientări pentru statele membre cu privire la tipul de informații care ar sprijini cel mai mult FTC în ancheta sa în legătură cu o sesizare. Ca parte a acestui efort, FTC va desemna un punct de contact în cadrul agenției pentru sesizările primite de la statele membre ale UE. Este foarte util ca autoritatea de trimitere să fi efectuat o anchetă preliminară în legătură cu presupusa încălcare și poate coopera cu FTC în cadrul unei investigații.

După primirea unei sesizări din partea unui stat membru al UE sau a unui organism de autoreglementare, FTC poate lua o serie de măsuri pentru a soluționa chestiunile în discuție. De exemplu, se pot revizui politicile de confidențialitate ale companiei, se obțin informații suplimentare direct de la companie sau de la terți, se asigură o monitorizare împreună cu entitatea emitentă, se evaluează dacă există mai multe încălcări sau un număr semnificativ de consumatori afectați, se determină dacă sesizarea implică chestiuni care țin de Departamentul Comerțului, se evaluează dacă ar fi utilă educația consumatorilor și a mediului de afaceri și, după caz, se poate iniția o procedură de executare.

FTC se angajează, de asemenea, să facă schimb de informații cu privire la sesizări cu autoritățile de executare emitente, inclusiv statutul sesizărilor, sub rezerva actelor cu putere de lege și a restricțiilor în materie de confidențialitate. În măsura în care este fezabil, având în vedere numărul și tipul de sesizări primite, informațiile furnizate vor include o evaluare a aspectelor sesizate, inclusiv o descriere a principalelor probleme ridicate, precum și orice măsuri luate în vederea soluționării cazurilor de încălcare a dreptului, care sunt de competența FTC. De asemenea, FTC va oferi feedback autorității de trimitere privind tipurile de sesizări primite pentru a spori eficacitatea eforturilor de combatere a comportamentului ilicit. În cazul în care o autoritate de executare emitentă solicită informații privind statutul unei anumite

([1]) A se vedea FTC/Karnani, nr. 2:09-cv-05276 (C.D. Cal. 20 mai 2011) (ordin final stipulat), disponibil la adresa https://www.ftc.gov/sites/default/files/documents/cases/2011/06/110609karnanistip.pdf; a se vedea, de asemenea Lesley Fair, FTC Business Center Blog, *Around the World in Shady Ways*, https://www.ftc.gov/blog/2011/06/around-world-shady-ways (9 iunie 2011).

([2]) Scrisoarea adresată de Ken Hyatt, Subsecretar interimar pentru comerț însărcinat cu comerțul internațional, Administrația pentru comerțul internațional, dnei Věra Jourová, comisar pentru justiție, consumatori și egalitate de gen.

sesizări în scopul desfășurării propriei proceduri de executare, FTC va răspunde, ținând cont de numărul de sesizări în cauză și cu condiția respectării cerințelor de confidențialitate și a altor cerințe juridice.

De asemenea, FTC va colabora îndeaproape cu autoritățile pentru protecția datelor din UE pentru a oferi asistență pentru asigurarea respectării. În cazurile corespunzătoare, aceasta ar putea include schimbul de informații și asistență pentru investigații în conformitate cu U.S. SAFE WEB Act, care autorizează FTC să acorde asistență agențiilor străine de asigurarea respectării atunci când agenția străină pune în aplicare legi care interzic practicile care sunt în mare măsură similare cu cele interzise de legislația aplicată de FTC ([1]). Ca parte a acestei asistențe, FTC poate împărtăși informațiile obținute în legătură cu o anchetă FTC, poate emite un ordin de proces obligatoriu în numele autorității pentru protecția datelor din UE care desfășoară propria anchetă și poate solicita depoziții orale ale martorilor sau inculpaților în cadrul procedurilor APD de asigurare a respectării, sub rezerva îndeplinirii cerințelor U.S. SAFE WEB Act. FTC utilizează periodic această competență pentru a ajuta alte autorități din întreaga lume cu privire la cazurile de protecție a vieții private și de protecție a consumatorilor ([2]).

Pe lângă prioritizarea sesizărilor în temeiul Scutului de confidențialitate primite din partea statelor membre ale UE și a organizațiilor de autoreglementare în materie de protecție a vieții private ([3]), FTC se angajează să analizeze din proprie inițiativă posibile încălcări ale cadrului Scutului de confidențialitate, după caz, prin utilizarea unei serii de instrumente.

Timp de mai mult de un deceniu, FTC a susținut un program solid de investigare a problemelor de confidențialitate și securitate care implică organizații comerciale. În cadrul acestor anchete, FTC a analizat periodic dacă entitatea în cauză a făcut observații legate de sfera de siguranță. Dacă entitatea a făcut astfel de observații și ancheta a divulgat încălcări clare ale principiilor privind protecția vieții private în temeiul sferei de siguranță, FTC a inclus în măsurile sale de asigurare a respectării acuzații de încălcări ale sferei de siguranță. Vom continua această abordare proactivă în temeiul noului cadru juridic. Important, FTC desfășoară mult mai multe investigații decât cele care se încheie prin luarea de măsuri publice de asigurare a respectării. Multe investigații FTC sunt închise deoarece personalul nu identifică o încălcare a legislației. Întrucât anchetele respective sunt confidențiale și nu sunt publice, de multe ori, încheierea unei investigații nu este făcută publică.

Cele aproape 40 de măsuri de asigurare a respectării inițiate de FTC legate de programul privind sfera de siguranță dovedesc angajamentul agenției în ceea ce privește aplicarea proactivă a programelor transfrontaliere de protecție a vieții private. FTC va căuta potențiale încălcări ale cadrului ca parte a investigațiilor în materie de protecție a vieții private și a securității pe care le desfășurăm în mod regulat.

III. ABORDAREA DECLARAȚIILOR FALSE SAU FRAUDULOASE DE PARTICIPARE LA SCUTUL DE CONFIDENȚIALITATE

Astfel cum este menționat mai sus, FTC va lua măsuri împotriva entităților care declară în mod fals că participă la cadrul Scutului de confidențialitate. FTC va examina cu prioritate sesizările primite de la Departamentul Comerțului cu privire la organizațiile identificate de acesta ca prezentând declarații false de participare actuală la cadru sau ca utilizând mărci de certificare ale Scutului de confidențialitate fără autorizație.

În plus, observăm că, dacă politica de confidențialitate a unei organizații afirmă că respectă principiile Scutului de confidențialitate, faptul că aceasta nu se înregistrează sau nu menține o înregistrare la Departamentul Comerțului nu poate, în sine, să scutească organizația de aplicarea de către FTC a acestor angajamente în temeiul Scutului de confidențialitate.

([1]) Atunci când decide dacă să își exercite competența în temeiul U.S. SAFE WEB Act, FTC consideră, printre altele: „(A) dacă agenția solicitantă a fost de acord să ofere sau va oferi asistență reciprocă Comisiei; (B) dacă îndeplinirea cererii ar aduce atingere interesului public al Statelor Unite; și (C) dacă ancheta sau procedura de executare a agenției solicitante se referă la acte sau practici care cauzează sau este probabil să cauzeze un prejudiciu unui număr semnificativ de persoane" 15 U.S.C. § 46(j)(3). Această competență nu se aplică în ceea ce privește punerea în aplicare a legislației în domeniul concurenței.

([2]) În anii fiscali 2012-2015, de exemplu, FTC și-a utilizat competența în temeiul U.S. SAFE WEB Act pentru a face schimb de informații ca răspuns la aproape 60 de cereri din partea agențiilor străine și a formulat aproape 60 de cereri de investigare civilă (echivalente cu citațiile administrative) pentru a ajuta 25 de anchete străine.

([3]) Deși FTC nu soluționează sau mediază plângeri ale consumatorilor individuali, FTC afirmă că va acorda prioritate sesizărilor în temeiul Scutului de confidențialitate din partea autorităților pentru protecția datelor din UE. De asemenea, FTC utilizează plângerile din baza de date a consumatorilor Sentinel, care poate fi accesată de un număr mare de alte agenții de aplicare a legii, pentru a identifica tendințele, pentru a stabili prioritățile în materie de asigurare a respectării și pentru a identifica posibilele obiective de investigare. Persoanele din UE pot utiliza același sistem de plângeri de care dispun cetățenii americani pentru a depune o plângere la Federal Trade Commission la adresa www.ftc.gov/complaint. Cu toate acestea, pentru plângerile individuale în temeiul Scutului de confidențialitate, ar putea fi mai util pentru persoanele din UE să depună plângeri la autoritatea pentru protecția datelor a statului lor membru sau la furnizorul de mecanisme de soluționare alternativă a litigiilor.

IV. MONITORIZAREA ORDINELOR

De asemenea, FTC își afirmă angajamentul de a monitoriza ordinele de executare pentru a asigura respectarea cadrului privind Scutul de confidențialitate.

Vom impune respectarea cadrului Scutului de confidențialitate prin intermediul unor dispoziții adecvate reparatorii în viitoare ordine FTC în temeiul cadrului. Aceasta include interzicerea declarațiilor false cu privire la cadrul Scutului de confidențialitate și alte programe de protecție a vieții private, atunci când acestea stau la baza acțiunii FTC.

Cazurile FTC care aplică programul inițial privind sfera de siguranță sunt foarte instructive. În 36 de cazuri care implică declarații false sau frauduloase de certificare a sferei de siguranță, fiecare ordin interzice pârâtului să facă declarații false privind participarea sa la sfera de siguranță sau la orice alt program de protecție a vieții private sau a securității și impune companiei să pună la dispoziția FTC rapoartele de conformitate. În cazurile care implică încălcări ale principiilor privind protecția vieții private în temeiul sferei de siguranță, companiile au obligația de a pune în aplicare programe cuprinzătoare de protecție a vieții private și de a obține evaluări independente efectuate de terți privind programele respective în fiecare an timp de douăzeci de ani, pe care aceștia trebuie să le transmită FTC.

Încălcările ordinelor administrative ale FTC pot conduce la sancțiuni de drept civil de până la 16 000 USD pentru fiecare încălcare sau 16 000 USD pe zi pentru o încălcare persistentă ([1]), care, în cazul practicilor care afectează mulți consumatori, se pot ridica la milioane de dolari. De asemenea, fiecare ordonanță prin consimțământ conține dispoziții de raportare și de conformitate. Entitățile reglementate de ordonanță trebuie să păstreze documentele care demonstrează conformitatea acestora timp de un anumit număr de ani. Ordonanțele trebuie, de asemenea, să fie transmise angajaților responsabili pentru asigurarea conformității cu ordonanța.

FTC monitorizează sistematic respectarea ordonanțelor referitoare la sfera de siguranță, astfel cum procedează în cazul tuturor ordinelor sale. FTC tratează cu seriozitate asigurarea respectării ordinelor sale privind protecția confidențialității și a securității datelor și ia măsuri să le pună în aplicare, atunci când este necesar. De exemplu, astfel cum s-a arătat mai sus, Google a plătit sancțiuni de drept civil în valoare de 22,5 milioane USD pentru soluționarea acuzațiilor că a încălcat ordinul FTC. Important, ordinele FTC vor continua să protejeze toți consumatorii din întreaga lume care interacționează cu o întreprindere, nu doar consumatorii care au depus plângeri.

În cele din urmă, FTC va continua să mențină o listă online a companiilor care fac obiectul ordinelor obținute în legătură cu asigurarea respectării atât a programului privind sfera de siguranță, cât și a noului cadru privind Scutul de confidențialitate ([2]). În plus, principiile Scutului de confidențialitate impun în prezent companiilor care fac obiectul unui ordin al FTC sau al unui ordin judecătoresc bazat pe nerespectarea principiilor să publice toate secțiunile relevante legate de cadru din orice raport de conformitate sau de evaluare transmis către FTC, în măsura în care acest lucru este în concordanță cu legislația și normele de confidențialitate.

V. ANGAJAMENTUL FAȚĂ DE AUTORITĂȚILE PENTRU PROTECȚIA DATELOR DIN UE ȘI COOPERAREA ÎN MATERIE DE ASIGURARE A RESPECTĂRII

FTC recunoaște rolul important pe care îl joacă autoritățile pentru protecția datelor din UE cu privire la respectarea cadrului privind Scutul de confidențialitate și încurajează sporirea consultării și cooperarea în vederea asigurării respectării. Pe lângă consultările cu autoritățile pentru protecția datelor cu privire la aspecte specifice cazurilor, FTC se angajează să participe la reuniuni periodice cu reprezentanții desemnați ai Grupului de lucru instituit prin articolul 29 să discute în termeni generali modalitățile de îmbunătățire a cooperării în vederea asigurării respectării cadrului. FTC va participa, de asemenea, împreună cu Departamentul Comerțului, Comisia Europeană și Grupul de lucru instituit prin articolul 29, la revizuirea anuală a cadrului pentru a discuta punerea sa în aplicare.

FTC încurajează, de asemenea, dezvoltarea unor instrumente care vor consolida cooperarea cu autoritățile pentru protecția datelor din UE în vederea asigurării respectării, precum și cu alte autorități pentru asigurarea respectării vieții private din întreaga lume. În special, FTC, împreună cu partenerii de asigurare a respectării din Uniunea Europeană și din întreaga lume, au lansat în anul precedent un sistem de alertă în cadrul rețelei globale de protecție a vieții private („GPEN") pentru a face schimb de informații cu privire la anchete și pentru a promova coordonarea aplicării. Acest instrument de alertă GPEN ar putea fi deosebit de util în contextul cadrului privind Scutul de confidențialitate. FTC și autoritățile pentru protecția datelor din UE ar putea să îl folosească pentru coordonare în ceea ce privește cadrul și alte investigații privind protecția vieții private, inclusiv ca punct de plecare pentru schimbul de informații în vederea realizării unei asigurări coordonate și mai eficace a protecției vieții private pentru consumatori. Așteptăm cu nerăbdare să ne continuăm activitatea desfășurată în colaborare cu autoritățile UE participante pentru a utiliza sistemul de alertă GPEN

([1]) 15 U.S.C. § 45(m); 16 C.F.R. § 1.98.
([2]) *A se vedea* FTC, Business Center, Legal Resources, https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field-consumer-protection-topics-tid=251.

într-un context mai larg și dezvoltarea altor instrumente pentru a îmbunătăți cooperarea în asigurarea respectării cu privire la cazurile de protecție a vieții private, inclusiv cele care implică Scutul de confidențialitate.

FTC are plăcerea să își afirme angajamentul în direcția punerii în aplicare a noului cadru privind Scutul de confidențialitate. De asemenea, așteptăm cu interes continuarea dialogului cu colegii din UE, pe măsură ce vom lucra împreună pentru a proteja viața privată a consumatorilor de pe ambele maluri ale Atlanticului.

Cu stimă,

Edith Ramirez

Președintă

Apendicele A

Cadrul Scutului de confidențialitate UE-SUA în context: o imagine de ansamblu a sistemului american în materie de protecție a vieții private și de securitate

Măsurile de protecție prevăzute de cadrul privind Scutul de confidențialitate UE-SUA („cadrul") se înscriu în contextul măsurilor mai generale de protecție a vieții private instituite de sistemul juridic american în ansamblul său. În primul rând, Comisia Federală pentru Comerț a SUA („FTC") dispune de un program solid de protecție a vieții private și a securității datelor pentru practicile comerciale din SUA, care protejează consumatorii din întreaga lume. În al doilea rând, peisajul protecției vieții private și a securității consumatorilor din Statele Unite a evoluat în mod considerabil începând din 2000, când a fost adoptat programul inițial al „sferei de siguranță" SUA-UE. Din acel moment, au fost promulgate numeroase legi federale și statale privind protecția vieții private și securitatea, iar numărul litigiilor care implică instituții publice și persoane private legate de asigurarea respectării drepturilor la protecția vieții private a crescut semnificativ. Prin domeniul lor larg de aplicare, măsurile americane de protecție juridică privind viața privată și securitatea consumatorilor care sunt aplicabile practicilor comerciale completează măsurile de protecție acordate persoanelor din UE de noul cadru.

I. PROGRAMUL GENERAL AL FTC DE ASIGURARE A RESPECTĂRII VIEȚII PRIVATE ȘI A SECURITĂȚII

FTC este principala agenție de protecție a drepturilor consumatorilor din SUA specializată în protecția vieții private în sectorul comercial. FTC are puterea de a îi urmări în justiție pe autorii actelor sau practicilor neloiale și înșelătoare care încalcă dreptul la viața privată al consumatorilor, precum și de a aplica legi mai specifice care protejează anumite informații financiare sau referitoare la starea de sănătate, informațiile referitoare la copii și informațiile utilizate pentru a lua anumite decizii de eligibilitate referitoare la consumatori

FTC dispune de o experiență incomparabilă în ceea ce privește asigurarea respectării vieții private a consumatorilor. Măsurile de asigurare a respectării legii luate de FTC au vizat practicile ilegale atât din mediul offline, cât și din cel online De exemplu, FTC a inițiat acțiuni de asigurare a respectării legii împotriva unor societăți renumite, cum ar fi Google, Facebook, Twitter, Microsoft, Wyndham, Oracle, HTC și Snapchat, precum și împotriva unor societăți mai puțin cunoscute. FTC a acționat în justiție întreprinderi acuzate că au trimis emailuri nesolicitate (mesaje spam) consumatorilor, că au instalat programe spion pe computere, că nu au securizat informațiile cu caracter personal ale consumatorilor, că au urmărit consumatorii online în mod fraudulos, că au încalcat dreptul la viață privată al copiilor, că au colectat în mod ilegal informații de pe dispozitivele mobile ale consumatorilor și că nu au securizat dispozitivele conectate la internet și utilizate pentru a stoca informații cu caracter personal. Ordonanțele adoptate în urma acestor acțiuni au prevăzut, în general, monitorizarea continuă de către FTC pe o perioadă de douăzeci de ani, au interzis comiterea de noi încălcări ale legii și au aplicat întreprinderilor importante sancțiuni financiare în cazul încălcării ordonanțelor. ([1]) Este important de semnalat că ordonanțele FTC nu urmăresc doar să protejeze persoanele fizice care au depus plângeri cu privire la o problemă dată; dimpotrivă, acestea protejează toți consumatorii care vor realiza tranzacții ulterior cu întreprinderea în cauză. În context transfrontalier, FTC are competența de a proteja consumatorii din întreaga lume împotriva practicilor care au loc în Statele Unite ([2]).

Până în prezent, FTC a urmărit în justiție peste 130 de cazuri de spam și de instalare de programe de tip spyware, peste 120 de cazuri de încălcare a dreptului de a nu primi apeluri telefonice comerciale de telemarketing, peste 100 de cazuri de acțiuni inițiate în temeiul Legii privind imparțialitatea rapoartelor privind solvabilitatea creditorilor, aproape 60 de cazuri referitoare la securitatea datelor, peste 50 acțiuni generale privind viața privată, aproape 30 de cazuri de încălcări ale Legii Gramm-Leach-Bliley și peste 20 de acțiuni de punere în aplicare a Legii privind respectarea vieții private a copiilor în mediul online (*Children's Online Privacy Protection Act* – COPPA) ([3]). În plus față de aceste cazuri, FTC a emis și publicat scrisori de avertizare ([4]).

([1]) Orice entitate care nu se conformează unei ordonanțe FTC este pasibilă de o amendă stabilită prin hotărâre judecătorească civilă de până la 16 000 USD pentru fiecare încălcare sau de până la 16 000 dolari pe zi pentru o încălcare continuă. *A se vedea* 15 U.S.C. § 45(l); 16 C. F.R. § 1.98(c).

([2]) Congresul a confirmat în mod expres competența FTC de a recurge la căi de atac în justiție, inclusiv restituirea, pentru orice acte sau practici inerente comerțului exterior și (1) care cauzează sau pot cauza un prejudiciu previzibil în mod rezonabil în Statele Unite sau (2) care presupun un comportament relevant pe teritoriul Statelor Unite. *A se vedea* 15 U.S.C. § 45(a)(4).

([3]) În anumite cazuri privind protecția vieții private și securitatea datelor deschise FTC, întreprinderile au fost acuzate de implicare atât în practici înșelătoare, cât și neloiale; în aceste cazuri au fost invocate uneori și presupuse încălcări ale mai multor acte legislative, precum Legea privind imparțialitatea rapoartelor privind solvabilitatea creditorilor, Legea Gramm-Leach-Bliley și COPPA.

([4]) A se vedea, de exemplu comunicatul de presă al FTC: „*FTC Warns Children's App Maker BabyBus About Potential COPPA Violations*" (22 decembrie 2014), https://www.ftc.gov/news-events/press-releases/2014/12/ftc-warns-childrens-app-maker-babybus-about-potential-coppa; comunicatul de presă al FTC: „*FTC Warns Data Broker Operations of Possible Privacy Violations*" (7 mai 2013), https://www.ftc.gov/news-events/press-releases/2013/05/ftc-warns-data-broker-operations-possible-privacy-violations; comunicatul de presă al FTC: „*FTC Warns Data Brokers That Provide Tenant Rental Histories They May Be Subject to Fair Credit Reporting Act*" (3 aprilie 2013), https://www.ftc.gov/news-events/press-releases/2013/04/ftc-warns-data-brokers-provide-tenant-rental-histories-they-may.

În cadrul activității sale anterioare legate de asigurarea respectării legislației privind confidențialitatea, FTC a detectat, de asemenea, în mod regulat eventualele încălcări ale sferei de siguranță. De la adoptarea acestui program, FTC a întreprins din proprie inițiativă un număr mare de investigații privind conformitatea cu sfera de siguranță și a inițiat 39 de proceduri împotriva societăților din SUA pentru încălcări ale „sferei de siguranță". FTC va continua această abordare proactivă, acordând prioritate punerii în aplicare a noului cadru.

II. MĂSURI DE PROTECȚIE A VIEȚII PRIVATE A CONSUMATORILOR LA NIVEL FEDERAL ȘI LA NIVEL STATAL

Studiul privind punerea în aplicare a principiilor „sferei de siguranță", care figurează ca anexă la decizia Comisiei Europene privind caracterul adecvat al principiilor „sferei de siguranță", oferă un rezumat al multora dintre legile federale și statale privind viața privată în vigoare în 2000, când a fost adoptat programul „sferei de siguranță" ([1]). În perioada respectivă, numeroase legi federale reglementau colectarea și utilizarea în scopuri comerciale a informațiilor cu caracter personal, în afară de secțiunea 5 din Legea privind Comisia Federală pentru Comerț, inclusiv legile următoare: *Cable Communications Policy Act, Driver's Privacy Protection Act, Electronic Communications Privacy Act, Electronic Funds Transfer Act, Fair Credit Reporting Act, Gramm-Leach-Bliley Act, Right to Financial Privacy Act, Telephone Consumer Protection Act* și *Video Privacy Protection Act*. Numeroase state aveau legi similare și în aceste domenii.

Începând cu 2000, s-au înregistrat numeroase evoluții atât la nivel federal, cât și la nivelul statelor, care le oferă consumatorilor măsuri suplimentare de protecție a vieții private ([2]). La nivel federal, de exemplu, FTC a modificat în 2013 Regulamentul COPPA pentru a furniza o serie de măsuri suplimentare de protecție a informațiilor cu caracter personal ale copiilor. FTC a emis, de asemenea, două regulamente de punere în aplicare a Legii Gramm-Leach-Bliley (Regulamentul privind respectarea vieții private – *Privacy Rule* și Regulamentul privind garanțiile – *Safeguards Rule*) care obligă instituțiile financiare ([3]) să își divulge practicile în materie de schimb de informații și să pună în aplicare un program cuprinzător de securitate a informațiilor pentru a proteja informațiile consumatorilor ([4]). În mod similar, Legea privind imparțialitatea și fiabilitatea operațiunilor de creditare (*Fair and Accurate Credit Transactions Act* – „FACTA"), adoptată în 2003, completează legislația existentă de mult timp în SUA privind activitățile de creditare, stabilind cerințe privind mascarea, schimbul și eliminarea anumitor date financiare sensibile. FTC a promulgat o serie de regulamente în temeiul FACTA în ceea ce privește, printre altele: dreptul consumatorilor la un raport anual gratuit privind solvabilitatea; cerințele privind eliminarea în condiții de siguranță a informațiilor care apar în rapoartele referitoare la consumatori; dreptul consumatorilor de a renunța la primirea anumitor oferte de credite și asigurări; dreptul consumatorilor de a renunța la utilizarea informațiilor furnizate de o întreprindere afiliată pentru a-și comercializa produsele și serviciile; precum și cerințe impuse instituțiilor financiare și creditorilor de a pune în aplicare programe de detectare și prevenire a furtului de identitate ([5]). Pe lângă aceasta, în 2013 au fost revizuite regulamentele promulgate în temeiul Legii privind portabilitatea și răspunderea în materie de asigurări de sănătate (*Health Insurance Portability and Accountability Act*), prin adăugarea unor garanții suplimentare destinate să protejeze viața privată și securitatea informațiilor cu caracter personal privind sănătatea ([6]). De asemenea, au intrat în vigoare regulamente de protecție a consumatorilor împotriva apelurilor de telemarketing nedorite, a apelurilor efectuate de roboți și a spamului. La rândul său, Congresul a adoptat legi care impun anumitor societăți ce colectează informații privind sănătatea să le transmită notificări consumatorilor în caz de încălcare ([7]).

Statele au fost, de asemenea, foarte active în ceea ce privește adoptarea de acte legislative în materie de protecție a vieții private și de securitate. Din 2000, patruzeci și șapte de state, Districtul Columbia, Guam, Puerto Rico și Insulele Virgine au adoptat legi care impun întreprinderilor să notifice persoanelor cazurile de încălcare a securității informațiilor cu

([1]) A se vedea documentul Ministerului Comerțului al SUA intitulat *Safe Harbor Enforcement Overview*, https://build.export.gov/main/safeharbor/eu/eg_main_018476.

([2]) Pentru o sinteză mai cuprinzătoare a măsurilor de protecție juridică din Statele Unite, a se vedea Daniel J. Solove & Paul Schwartz, *Information Privacy Law* (ediția a 5-a, 2015).

([3]) Legea Gramm-Leach-Bliley oferă o definiție foarte amplă a instituțiile financiare, care includă toate întreprinderile care sunt „se consacră într-o mare măsură" furnizării de produse sau servicii financiare Această definiție include, de exemplu, întreprinderile de încasare a cecurilor, societățile care acordă împrumuturi până la plata salariului, brokerii de credite ipotecare, societățile care acordă împrumuturi nebancare, evaluatorii de bunuri personale sau imobiliare și profesioniștii specializați în întocmirea declarațiilor fiscale.

([4]) În conformitate cu Legea privind protecția financiară a consumatorilor din 2010 (*Consumer Financial Protection Act* – „CFPA"), titlul X din Pub. L. 111-203, 124 Stat. 1955 (21 iulie 2010) (cunoscută, de asemenea, sub denumirea de „Legea Dodd-Frank pentru reforma activităților de pe Wall Street și pentru protecția consumatorilor") cea mai mare parte a competențelor decizionale de care dispune FTC în temeiul Legii Gramm-Leach-Bliley au fost transferate către Biroul de protecție a consumatorilor în sectorul financiar (*Consumer Financial Protection Bureau* – CFPB). FTC rămâne autoritatea de aplicare a legii în temeiul Legii Gramm-Leach-Bliley, precum și autoritatea decizională în cazul Regulamentului privind garanțiile (*Safeguards Rule*), păstrând o autoritate decizională limitată în conformitate cu Regulamentul privind respectarea vieții private (*Privacy Rule*) în ceea ce privește comercianții de automobile.

([5]) În temeiul CFPA, Comisia împarte cu CFPB rolul de asigurare a respectării legii, dar autoritatea decizională a fost transferată în mare parte către CFPB (cu excepția steguleților roșii și al regulamentelor privind eliminarea).

([6]) A se vedea 45 C.F.R., punctele 160, 162, 164.

([7]) A se vedea, de exemplu American Recovery & Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009) și regulamentele relevante, 45 C.F.R. §§ 164.404-164.414; 16 C.F.R. pt. 318.

caracter personalf ([1]). În cel puțin treizeci și două de state și în Puerto Rico sunt în vigoare legi privind eliminarea datelor, care instituie cerințe pentru distrugerea sau eliminarea informațiilor cu caracter personal ([2]). Mai multe state membre au adoptat, de asemenea, legi generale privind securitatea datelor. În plus, California a adoptat diferite legi privind protecția vieții private, inclusiv o lege care le impune întreprinderilor să adopte politici de confidențialitate și să își divulge practicile în materie de protecție împotriva monitorizării („Do Not Track" – „Nu monitoriza") ([3]), o lege cunoscută sub denumirea „Shine the Light" care impune un grad mai mare de transparență în ceea ce privește brokerii de date ([4]), precum și o lege care prevede punerea la dispoziție a unui „buton de radiere" care le permite minorilor să solicite eliminarea anumitor informații de pe platformele de comunicare socială ([5]).Aplicând aceste legi și exercitând alte puteri, guvernul federal și guvernele statelor membre ale federației au aplicat amenzi importante societăților care nu au protejat viața privată și securitatea informațiilor cu caracter personal ale consumatorilor ([6]).

Acțiunile introduse în justiție de către persoane private au condus, de asemenea, la pronunțarea de hotărâri și tranzacții favorabile care au îmbunătățit protecția vieții private și a securității datelor pentru consumatori. De exemplu, în 2015, societatea Target a convenit să plătească 10 milioane USD în temeiul unui acord tranzacțional încheiat cu clienții care au susținut că informațiile lor financiare cu caracter personal au fost compromise din cauza unei încălcări pe scară largă a securității datelor. În 2013, AOL a acceptat să plătească, în temeiul unui acord tranzacțional, 5 milioane USD pentru a pune capăt unei acțiuni colective (*class action*) ai cărei inițiatori au susținut că au fost afectați de anonimizarea insuficientă în legătură cu divulgarea căutărilor pe internet lansate de sute de mii de membri ai AOL. În plus, o curte federală a aprobat o plată de 9 milioane USD efectuată de Netflix ca urmare a acuzațiilor potrivit cărora a conservat istoricul de închiriere al abonaților, încălcând, astfel, Legea privind respectarea vieții private în cadrul furnizării de materiale video (*Video Privacy Protection Act*) din 1988. Instanțele federale din California au aprobat două tranzacții separate încheiate cu Facebook, una în valoare de 20 milioane USD și o alta în valoare de 9,5 milioane USD, legate de colectarea, utilizarea și schimbul de către societate al informațiilor cu caracter personal ale utilizatorilor săi. De asemenea, în 2008, o instanță judecătorească din California a aprobat un acord tranzacțional încheiat cu LensCrafters în valoare de 20 milioane USD pentru divulgarea ilegală a informațiilor medicale ale consumatorilor.

În concluzie, astfel cum evidențiază acest rezumat, Statele Unite asigură consumatorilor o importantă protecție juridică în materie de respectare a dreptului la viața privată al consumatorilor și de securitate. Noul cadru privind Scutul de confidențialitate, care le asigură persoanelor fizice din UE garanții semnificative, se va înscrie în acest context mai amplu, în care protecția vieții private și a securității consumatorilor rămâne o prioritate importantă.

([1]) A se vedea, de exemplu, documentul Conferinței naționale a legiuitorilor de stat (National Conference of State Legislatures „NCSL"), *State Security Breach Notification Laws* (4 ianuarie 2016), disponibil la http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

([2]) NCSL, *Data Disposal Laws* (12 ian. 2016), disponibil la http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

([3]) Cal. Bus. & Professional Code §§ 22575-22579.

([4]) Cal. Civ. Code §§ 1798.80-1798.84.

([5]) Cal. Bus. & Professional Code § 22580-22582.

([6]) A se vedea Jay Cline, *U.S. Takes the Gold in Doling Out Privacy Fines*, Computerworld (17 februarie 2014), disponibil la adresa: http://www.computerworld.com/s/article/9246393/Jay-Cline-U.S.-takes-the-gold-in-doling-out-privacy-fines?taxonomyId=17&pageNumber=1.

ANEXA V

Scrisoarea Secretarului Departamentului Transporturilor al SUA, domnul Anthony Foxx

19 februarie 2016

Comisar Vera Jourová
Comisia Europeană
Rue de la Loi/Wetstraat 200
l 049 Brussels
Belgia

Re: Cadrul privind Scutul de confidențialitate UE-SUA

Stimată Doamnă Comisar Jourová,

Departamentul Transporturilor al Statelor Unite ale Americii („Departamentul" sau „DOT") apreciază posibilitatea de a descrie rolul său în aplicarea cadrului privind Scutul de confidențialitate UE-SUA. Acest cadru joacă un rol esențial în protecția datelor cu caracter personal furnizate în cursul tranzacțiilor comerciale într-o lume din ce în ce mai interconectată. Aceasta permite întreprinderilor să efectueze operațiuni importante în economia globală, asigurând în același timp protecția vieții private a consumatorilor din UE.

Departamentul Transporturilor și-a exprimat pentru prima dată, în mod public, angajamentul față de asigurarea respectării cadrului privind sfera de siguranță într-o scrisoare adresată Comisiei Europene cu peste 15 de ani în urmă. În scrisoarea respectivă, Departamentul Transporturilor s-a angajat să adere cu strictețe la principiile privind protecția vieții private ale sferei de siguranță. Departamentul Transporturilor continuă să își mențină angajamentul, iar prezenta scrisoare consacră acest angajament

În special, Departamentul Transporturilor își reînnoiește angajamentul în următoarele domenii esențiale: (1) prioritizarea anchetării unor presupuse încălcări ale Scutului de confidențialitate; (2) punerea în aplicare corespunzătoare a unor măsuri împotriva entităților care fac declarații false sau frauduloase de autocertificare cu privire la Scutul de confidențialitate; și (3) monitorizarea și publicarea ordinelor de executare privind încălcările Scutului de confidențialitate. Prezentăm informații cu privire la fiecare dintre aceste angajamente și, pentru contextul necesar, istoricul pertinent privind rolul Departamentului Transporturilor în protecția vieții private a consumatorilor și aplicarea cadrului privind Scutul de confidențialitate.

I. CONTEXTUL

A. **Competența în materie de confidențialitate a Departamentului Transporturilor**

Departamentul Transporturilor este ferm hotărât să asigure confidențialitatea informațiilor furnizate de consumatori companiilor aeriene și agenților care livrează bilete de avion. Competența Departamentului Transporturilor de a lua măsuri de punere în aplicare în acest domeniu în temeiul titlului 49 articolul 41712 din U.S.C., care interzice unui transportator „orice practică neloială sau frauduloasă sau orice act de concurență neloială" pentru vânzarea serviciilor de transport aerian, care aduce sau este susceptibilă de a aduce prejudicii consumatorului. Articolul 41712 este formulat după modelul articolului 5 din Federal Trade Commission Act (15 U.S.C 45). Interpretăm statutul nostru privind practicile neloiale sau frauduloase în sensul că interzice unei companii aeriene sau unui agent care livrează bilete de avion: (1) să încalce termenii politicii sale de confidențialitate; sau (2) să colecteze sau să dezvăluie informații cu caracter privat într-un mod care încalcă ordinea publică, este imoral sau cauzează un prejudiciu substanțial de consum nu sunt compensate de orice beneficii compensatorii. De asemenea, interpretăm articolul 41712 în sensul că interzice transportatorilor și agenților care livrează bilete de avion: (1) să încalce orice regulă emisă de Departamentul Transporturilor care identifică practicile specifice de protecție a vieții private ca neloiale sau frauduloase; sau (2) să încalce Legea privind protecția copiilor pe internet („COPPA") sau normele FTC de punere în aplicare a COPPA. În temeiul Legii Federale, Departamentul Transporturilor dispune de competențe exclusive de a reglementa practicile de protecție a vieții private ale companiilor aeriene și împarte competența cu FTC în ceea ce privește practicile de protecție a vieții private ale agenților care livrează bilete de avion la vânzarea serviciilor de transport aerian.

Astfel, după ce un operator de transport sau un vânzător de servicii de transport aerian se angajează public să adere la principiile de confidențialitate ale cadrului privind Scutul de confidențialitate, Departamentul poate să recurgă la atribuțiile care îi sunt conferite de articolul 41712 pentru a asigura respectarea acestor principii. Prin urmare, atunci când un pasager furnizează informații unui transportator sau unui agent care livrează bilete de avion care și-a luat angajamentul să respecte principiile de protecție a vieții private ale Scutului de confidențialitate, orice nerespectare a acestui angajament de către transportator sau agentul care livrează bilete de avion ar constitui o încălcare a articolului 41712.

B. **Practici de asigurare a respectării**

Biroul „Aviation Enforcement and Proceeding" al Departamentului Transporturilor (Biroul „Aviation Enforcement and Proceeding") investighează și intentează acțiuni în justiție în temeiul titlului 49 articolul 41712 din U.S.C. Acesta pune în aplicare interdicțiile legale din articolul 41712 împotriva practicilor neloiale și frauduloase, în principal, prin negocierea, pregătirea ordinelor administrative de încetare și elaborarea de ordonanțe de evaluare a sancțiunilor de drept civil. Biroul ia cunoștință de încălcările potențiale, în mare măsură, din plângerile pe care le primește din partea persoanelor particulare, a agențiilor de turism, a companiilor aeriene și agențiilor guvernamentale din Statele Unite ale Americii și din străinătate. Consumatorii pot face uz de site-ul Departamentului Transporturilor pentru a depune plângeri în materie de confidențialitate împotriva companiilor aeriene și agenților care livrează bilete de avion ([1]).

În situația în care nu se ajunge la o înțelegere rezonabilă și adecvată într-un caz, Biroul „Aviation Enforcement and Proceeding"are competența să inițieze o procedură de executare care implică o audiere probatorie în fața unui judecător de drept administrativ (ALJ) al Departamentului Transporturilor. ALJ are competența de a emite ordine administrative de încetare și sancțiuni civile. Nerespectarea dispozițiilor articolului 41712 poate avea ca rezultat emiterea de ordine administrative de încetare și aplicarea de sancțiuni de drept civil de până la 27 500 USD pentru fiecare încălcare a articolului 41712.

Departamentul nu are competența de a acorda daune-interese sau o despăgubire pecuniară reclamantului. Cu toate acestea, Departamentul Transporturilor are competența de a aproba soluționările diferendelor care rezultă în urma anchetelor desfășurate de Biroul „Aviation Enforcement and Proceeding", care să aducă beneficii directe atât consumatorilor (de exemplu, în numerar, tichete), pentru a compensa penalizările plătibile în alte moduri guvernului SUA. Acest lucru s-a întâmplat în trecut și este posibil, de asemenea, în contextul cadrului privind Scutul de confidențialitate atunci când circumstanțele justifică acest lucru. Încălcările repetate ale articolului 41712 de către o companie aeriană ar pune, de asemenea, la îndoială bunele intenții ale companiei aeriene de a-și respecta angajamentul și, în situații extreme, s-ar putea considera că respectiva companie nu mai este aptă de exploatare și, în consecință, riscă să-și piardă licența de exploatare.

Până în prezent, Departamentul Transporturilor a primit relativ puține plângeri care implică presupuse încălcări ale vieții private de către agenții care livrează bilete de avion sau de către companiile aeriene. Atunci când apar, acestea sunt anchetate în conformitate cu principiile enunțate mai sus.

C. **Măsuri de protecție juridică ale Departamentului Transporturilor în beneficiul consumatorilor din UE**

În temeiul articolului 41712, interzicerea practicilor neloiale sau frauduloase în transportul aerian sau vânzarea serviciilor de transport aerian se aplică companiilor aeriene americane și străine, precum și agenților care livrează bilete de avion. Departamentul Transporturilor ia frecvent măsuri împotriva companiilor aeriene americane și străine pentru practicile care afectează atât consumatorii străini, cât și americani, pe baza faptului că practicile companiei aeriene au avut loc în cadrul furnizării de servicii de transport către sau dinspre Statele Unite. Departamentul Transporturilor utilizează și va continua să utilizeze toate căile de atac disponibile pentru a proteja atât consumatorii străini, cât și americani împotriva practicilor neloiale sau frauduloase în transportul aerian asigurat de către entități reglementate.

Departamentul Transporturilor asigură, de asemenea, în ceea ce privește companiile aeriene, aplicarea altor legi specifice ale căror măsuri de protecție se extind la consumatori care nu sunt cetățeni ai SUA, precum COPPA. Printre altele, COPPA impune operatorilor de servicii online și site-uri internet care vizează copiii sau de site-uri care vizează publicul general și care colectează cu bună știință informații cu caracter personal de la copii sub vârsta de 13 ani, să furnizeze o notificare parentală și să obțină consimțământul verificabil al părinților. Site-urile internet și serviciile stabilite în SUA care fac obiectul COPPA și care colectează informații cu caracter personal de la copii străini sunt obligați să respecte dispozițiile COPPA. Site-urile internet și serviciile online stabilite în străinătate, trebuie, de asemenea, să respecte COPPA dacă vizează direct copii din Statele Unite ale Americii sau în cazul în care colectează în cunoștință de cauză informații cu caracter personal de la copii în Statele Unite. În măsura în care companiile aeriene americane sau străine care își desfășoară activitatea în Statele Unite încalcă COPPA, Departamentul Transporturilor ar avea competența de a adopta măsuri de punere în aplicare.

II. ASIGURAREA RESPECTĂRII SCUTULUI DE CONFIDENȚIALITATE

În cazul în care o companie aeriană sau un agent care livrează bilete de avion alege să participe la cadrul privind Scutul de confidențialitate și departamentul primește o plângere că o astfel de companie sau agent care livrează bilete de avion ar fi încălcat cadrul, Departamentul Transporturilor va lua următoarele măsuri pentru a pune ferm în aplicare cadrul respectiv.

([1]) http://www.transportation.gov/airconsumer/privacy-complaints.

A. **Prioritizarea anchetării presupuselor încălcări**

Biroul „Aviation Enforcement and Proceeding" al Departamentului Transporturilor va ancheta fiecare plângere împotriva unor presupuse încălcări ale Scutului de confidențialitate (inclusiv plângeri primite de la autorități pentru protecția datelor din UE) și va lua măsuri de executare, în cazul în care există dovezi ale unei încălcări. În plus, Biroul „Aviation Enforcement and Proceeding" va coopera cu FTC și Departamentul Comerțului și va acorda prioritate acuzațiilor că entitățile reglementate nu ar respecta angajamentele privind protecția vieții private asumate ca parte a cadrului privind Scutul de confidențialitate.

La primirea unei acuzații de încălcare a cadrului privind Scutul de confidențialitate, Biroul „Aviation Enforcement and Proceeding" din cadrul Departamentului Transporturilor poate lua o serie de măsuri în cadrul anchetei sale. De exemplu, acesta poate revizui politicile de confidențialitate ale companiei aeriene sau ale agentului care livrează bilete de avion, poate obține informații suplimentare din partea companiei aeriene sau a agentului care livrează bilete de avion sau de la terți, poate asigura o monitorizare împreună cu entitatea emitentă și poate evalua dacă există mai multe încălcări sau un număr semnificativ de consumatori afectați. În plus, acesta ar determina dacă problema se referă la chestiuni care intră în domeniul de competență a Departamentului Comerțului sau FTC, poate să evalueze dacă ar fi utilă educarea consumatorilor sau a mediului de afaceri și, după caz, poate iniția o procedură de executare.

În cazul în care Departamentul Transporturilor ia cunoștință de posibile încălcări ale Scutului de confidențialitate comise de agenți care livrează bilete de avion, acesta va asigura coordonarea cu FTC în această privință. De asemenea, comunicăm FTC și Departamentului Comerțului rezultatul acțiunilor de aplicare a Scutului de confidențialitate.

B. **Abordarea declarațiilor false sau frauduloase privind calitatea de participant**

Departamentul Transporturilor își menține angajamentul de a ancheta încălcările dispozițiilor Scutului de confidențialitate, inclusiv declarații false sau înșelătoare privind calitatea de participant la programul privind Scutul de confidențialitate. Vom acorda prioritate sesizărilor din partea Departamentului Comerțului în ceea ce privește organizațiile identificate de acesta ca declarând în mod nejustificat a fi participanți actuali la Scutul de confidențialitate și ca utilizând fără autorizație marca de certificare a cadrului privind Scutul de confidențialitate.

În plus, observăm că, dacă politica de confidențialitate a unei organizații afirmă că respectă principiile de fond ale Scutului de confidențialitate, faptul că aceasta nu s-a înregistrat sau nu a menținut o înregistrare la Departamentul Comerțului ca atare, nu scutește organizația de punerea în aplicare a acestor angajamente de către Departamentul Transporturilor.

C. **Monitorizarea și publicarea titlurilor executorii în ceea ce privește Scutul de confidențialitate**

Biroul „Aviation Enforcement and Proceeding" din cadrul Departamentului Transporturilor își reafirmă, de asemenea, angajamentul de a monitoriza titlurile executorii pentru a asigura respectarea programului privind Scutul de confidențialitate. Mai precis, în cazul în care biroul emite o hotărâre prin care se indică unei companii aeriene sau unui agent care livrează bilete să înceteze și să se abțină de la orice încălcare a dispozițiilor Scutului de confidențialitate și a articolului 41712, acesta va monitoriza respectarea de către entitate a dispoziției de acțiune în încetare din ordin. În plus, Biroul se va asigura că ordinele care decurg din cazuri legate de Scutul de confidențialitate sunt disponibile pe site-ul său internet.

Așteptăm cu interes continuarea activității noastre cu partenerii de la nivel federal și cu părțile interesate din UE cu privire la chestiuni legate de Scutul de confidențialitate.

Sper că aceste informații vă vor fi utile. Vă stau la dispoziție pentru orice informații suplimentare.

Cu stimă,

Anthony R. Foxx

Secretarul Transporturilor

ANEXA VI

Scrisoarea domnului Robert Litt, consilier general
Biroul Directorului Serviciului Național de Informații

22 februarie 2016

Dl Justin S. Antonipillai
Consilier
Departamentul Comerțului al SUA
1401 Constitution Ave., NW
Washington, DC 20230

Dl Ted Dean
Secretar adjunct
Administrația Comerțului Internațional
1401 Constitution Ave., NW
Washington, DC 20230

Stimate domnule Antonipillai și domnule Dean:

Pe parcursul ultimilor doi ani și jumătate, în contextul negocierilor pentru Scutul de confidențialitate UE-SUA, Statele Unite au furnizat informații substanțiale cu privire la activitatea de colectare de informații pe baza semnalelor electromagnetice a serviciilor de informații din SUA. Acestea au inclus informații cu privire la cadrul juridic de reglementare, supravegherea pe mai multe niveluri a acestor activități, transparența extinsă cu privire la aceste activități și protecția generală a vieții private și a libertăților civile, în scopul de a asista Comisia Europeană în a concluziona cu privire la caracterul adecvat al măsurilor de protecție respective, în ceea ce privește excepția de la principiile Scutului de confidențialitate pe motivul securității naționale. Prezentul document rezumă informațiile care au fost furnizate.

I. PD-28 ȘI DESFĂȘURAREA DE CĂTRE SUA DE ACTIVITĂȚI DE COLECTARE DE INFORMAȚII PE BAZA SEMNALELOR ELECTROMAGNETICE

Serviciile de informații ale Statelor Unite colectează informații externe într-un mod controlat cu atenție, în strictă conformitate cu legislația SUA și cu niveluri importante de supraveghere, concentrându-se pe informațiile externe importante și prioritățile naționale de securitate. Un mozaic de legi și politici ale SUA reglementează activitățile de colectare de informații pe baza semnalelor electromagnetice, inclusiv Constituția SUA, Legea privind supravegherea activităților străine de spionaj (Foreign Intelligence Surveillance Act – FISA) (50 U.S.C § 1801 și urm.), Decretul 12333 și procedurile sale de punere în aplicare, orientări prezidențiale, numeroase proceduri și orientări, aprobate de Curtea de Supraveghere a Activităților Străine de Spionaj și procurorul general, prin care se stabilesc norme suplimentare care limitează colectarea, păstrarea, utilizarea și difuzarea de informații externe ([1]).

a. **Prezentare generală PPD 28**

În ianuarie 2014, președintele Obama a ținut un discurs în care a prezentat diverse reforme privind activitățile SUA de colectare de informații pe baza semnalelor electromagnetice și a emis Directiva nr. 28 privind politica prezidențială (PPD-28) cu privire la activitățile respective ([2]). Președintele a subliniat că activitățile SUA de colectare de informații pe baza semnalelor electromagnetice contribuie la garantarea securității nu numai a țării noastre și a libertăților noastre, ci și a securității și a libertăților altor țări, inclusiv ale statelor membre ale UE, care se bazează pe informațiile obținute de serviciile de informații americane pentru a-și proteja propriii cetățeni.

PPD-28 stabilește o serie de principii și cerințe care să se aplice tuturor activităților SUA de colectare de informații pe baza semnalelor electromagnetice și pentru toți oamenii, indiferent de cetățenie sau de locație. În special, aceasta stabilește anumite cerințe pentru procedurile referitoare la colectarea, păstrarea și difuzarea informațiilor cu caracter personal referitoare la persoane care nu sunt cetățeni americani, obținute în cursul activităților SUA de colectare de informații pe baza semnalelor electromagnetice. Aceste cerințe sunt descrise în detaliu mai jos, pe scurt:

— PPD reiterează faptul că Statele Unite colectează informații pe baza semnalelor electromagnetice doar conform legii, decretului sau altei directive prezidențiale.

([1]) Informații suplimentare privind activitățile de colectare de informații externe ale SUA sunt publicate online și sunt accesibile publicului prin intermediul platformei „IC on the Record" (www.icontherecord.tumblr.com), site-ul public al ODNI dedicat îmbunătățirii vizibilității publice a activităților desfășurate de serviciile de informații ale guvernului.

([2]) Disponibil la adresa https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

— PPD stabilește proceduri pentru a se asigura că activitățile de colectare de informații pe baza semnalelor electromagnetice se desfășoară doar în scopuri legitime și autorizate, motivate de securitatea națională.

— PPD impune, de asemenea, ca protecția vieții private și a libertăților civile să fie preocupări esențiale în planificarea activităților de colectare de informații pe baza semnalelor electromagnetic. În special, Statele Unite nu colectează informații pentru a suprima sau a îngreuna critica sau opoziția; pentru a defavoriza persoane pe criterii legate de etnie, rasă, gen, orientare sexuală sau religie; sau pentru a oferi un avantaj comercial competitiv companiilor din SUA și sectoarelor de activitate din SUA.

— PPD prevede că activitățile de colectare de informații pe baza semnalelor electromagnetice trebuie să fie cât mai adaptate posibil și că informațiile colectate în masă pe baza semnalelor electromagnetice pot fi utilizate numai pentru scopuri specifice enumerate.

— PPD autorizează serviciile de informații să adopte proceduri „concepute în mod rezonabil pentru a reduce la minimum difuzarea și păstrarea informațiilor cu caracter personal colectate din activitățile de colectare de informații pe baza semnalelor electromagnetice", în special, extinderea anumitor măsuri de protecție aplicate informațiilor cu caracter personal ale cetățenilor americani la informațiile persoanelor care nu sunt cetățeni americani.

— Procedurile agenției de punere în aplicare a PPD-28 au fost adoptate și publicate.

Aplicabilitatea procedurilor și a măsurilor de protecție a vieții private stabilite în directivă în ceea ce privește Scutul de confidențialitate este clară. În cazul în care datele au fost transferate către societăți din Statele Unite în temeiul Scutului de confidențialitate, sau prin orice alte mijloace, serviciile de informații americane pot solicita datele de la aceste societăți numai dacă cererea respectă FISA sau este depusă în temeiul uneia dintre dispozițiile legale din Scrisoarea privind securitatea națională, care sunt discutate mai jos ([1]). În plus, fără a confirma sau a nega rapoartele mass-media care pretind că serviciile de informații din SUA colectează date de la cabluri transatlantice, în timp ce acestea sunt transmise către Statele Unite, în cazul în care serviciile de informații americane ar colecta date de la cablurile transatlantice, acestea ar face acest lucru sub rezerva limitărilor și măsurilor de protecție stabilite, inclusiv cerințele PPD-28.

b. **Limitări de colectare**

PPD-28 stabilește o serie de principii generale care reglementează colectarea de informații electromagnetice:

— Colectarea de informații pe baza semnalelor electromagnetice trebuie să fie autorizată prin lege sau autorizare prezidențială și trebuie să fie efectuată în conformitate cu constituția și legea.

— Viața privată și libertățile civile trebuie să fie considerente integrante în planificarea activităților de colectare de informații pe baza semnalelor electromagnetice.

— Informațiile pe baza semnalelor electromagnetice vor fi colectate numai atunci când există un scop valid legat de colectarea de informații externe și contrainformații.

— Statele Unite nu vor colecta informații pe baza semnalelor în scopul suprimării sau a îngreunării criticii sau opoziției.

— Statele Unite nu vor colecta informații pe baza semnalelor electromagnetice pentru a defavoriza persoane pe criterii legate de etnie, rasă, gen, orientare sexuală sau religie.

— Statele Unite nu vor colecta informații pe baza semnalelor electromagnetice pentru a conferi un avantaj comercial competitiv companiilor și sectoarelor de activitate din SUA.

— Activitate SUA de colectare de informații pe baza semnalelor electromagnetice trebuie să fie întotdeauna, în egală măsură, adaptată atât cât este posibil, ținând seama de disponibilitatea altor surse de informații. Aceasta înseamnă, printre altele, că ori de câte ori este posibil, activitățile de colectare de informații pe baza semnalelor electromagnetice se desfășoară într-un mod direcționat, mai degrabă decât în masă.

Cerința ca activitatea de colectare de informații pe baza semnalelor electromagnetice să fie „cât mai adaptată posibil\" se referă la modul în care se colectează informații pe baza semnalelor electromagnetice, precum și la ceea ce se colectează

([1]) Autoritățile de aplicare a legii sau agențiile de reglementare pot solicita informații de la întreprinderi în scop investigativ în Statele Unite în temeiul altor competențe penale, civile și de reglementare care sunt în afara domeniului de aplicare a prezentului document, care se limitează la autoritățile de securitate națională.

efectiv. De exemplu, pentru a decide dacă să colecteze sau nu informații pe baza semnalelor electromagnetice, serviciile de informații trebuie să țină seama de disponibilitatea altor informații, inclusiv surse publice sau diplomatice, precum și să acorde prioritate colectării prin aceste mijloace, dacă este oportun și fezabil. În plus, politicile privind elementele serviciilor de informații ar trebui să prevadă că, ori de câte ori este posibil, colectarea ar trebui să se concentreze asupra unor obiective sau teme specifice de informații externe prin utilizarea unor criterii de discriminare (de exemplu, infrastructuri specifice, termeni de selecție și identificatori).

Este important să se ia în considerare informațiile furnizate Comisiei în ansamblul lor. Deciziile legate de ceea ce este „fezabil" sau „realizabil" nu sunt lăsate la latitudinea persoanelor, ci fac obiectul politicilor pe care agențiile le-au elaborat în temeiul PPD-28 – care au fost puse la dispoziția publicului – și celorlalte procese descrise ([1]). Astfel cum prevede PPD-28, colectarea masivă de informații pe baza semnalelor electromagnetice este colectarea care „având în vedere considerațiile de ordin tehnic sau operațional, se obține fără a se utiliza elemente de discriminare (de exemplu, identificatori specifici, termeni de selecție etc.)." În acest sens, PPD-28 recunoaște faptul că elemente ale serviciilor de informații trebuie să colecteze informații masive pe baza semnalelor electromagnetice în anumite circumstanțe, pentru a identifica amenințări noi sau emergente și alte informații vitale de securitate națională care sunt adesea ascunse în sistemul vast și complex de comunicații globale moderne. De asemenea, PPD recunoaște preocupările legate de viața privată și libertățile civile semnalate atunci când sunt colectate informații masive pe baza semnalelor electromagnetice. Prin urmare, PPD-28 îndeamnă serviciile de informații să acorde prioritate unor alternative care să permită desfășurarea unor activități de colectare de informații specifice pe baza semnalelor electromagnetice, mai degrabă decât o colectare în masă de informații pe baza semnalelor electromagnetice. Prin urmare, ori de câte ori este posibil, elementele serviciilor de informații ar trebui să desfășoare activități specifice de colectare de informații pe baza semnalelor electromagnetice, mai degrabă decât o colectare în masă de informații pe baza semnalelor electromagnetice. ([2]) Aceste principii garantează că excepția pentru colectarea masivă de date nu va asimila regula generală.

În ceea ce privește noțiunea de „rezonabilitate", este un principiu de bază al legislației SUA. Aceasta înseamnă că elementele serviciilor de informații nu vor fi obligate să adopte orice măsură posibilă în teorie, ci vor trebui să echilibreze eforturile depuse pentru protecția vieții private și a libertăților civile legitime cu necesitățile practice ale activităților de colectare de informații pe baza semnalelor electromagnetice. Politicile agențiilor au fost puse la dispoziție, de asemenea, în acest caz și pot oferi asigurarea că formularea „concepute în mod rezonabil pentru a reduce la minimum difuzarea și păstrarea informațiilor cu caracter personal" nu aduce atingere regulii generale.

PPD-28 prevede, de asemenea, că informațiile colectate în masă pe baza semnalelor electromagnetice pot fi utilizate numai pentru șase obiective specifice: detectarea și combaterea anumitor activități ale puterilor străine; combaterea terorismului; combaterea proliferării; securitatea informatică; detectarea și combaterea amenințărilor la adresa forțelor armate ale SUA și a forțelor aliate; și combaterea amenințărilor infracționale transnaționale, inclusiv sancționarea fraudei. Consilierul pe probleme de securitate națională al președintelui, în consultare cu directorul pentru serviciile naționale de informații (Director for National Intelligence – DNI), va revizui anual aceste utilizări permise ale informațiilor colectate în masă pe baza semnalelor electromagnetice pentru a vedea dacă acestea ar trebui modificate. DNI va pune această listă la dispoziția publicului, în măsura posibilului, în concordanță cu securitatea națională. Acest lucru constituie o limitare importantă și transparentă în ceea ce privește utilizarea colectării de informații în masă pe baza semnalelor electromagnetice.

În plus, elementele serviciilor de informații care pun în aplicare PPD-28 au consolidat standardele și practicile analitice existente pentru a efectua căutări în informațiile neevaluate obținute pe baza semnalelor electromagnetice ([3]). Analiștii trebui să își structureze întrebările sau alți termeni și tehnici de căutare, pentru a se asigura că acestea sunt adecvate pentru a identifica informațiile relevante pentru o sarcină validă legată de aplicarea legii sau informații externe. În acest scop, elementele comunității serviciilor de informații trebuie să concentreze întrebările despre persoane pe categorii de informații obținute pe baza semnalelor electromagnetice care îndeplinesc o cerință a autorităților de aplicare a legii sau a serviciilor de informații externe, astfel încât să se prevină utilizarea informațiilor cu caracter personal care nu sunt relevante pentru cerințele autorităților de aplicare a legii sau ale serviciilor de informații externe.

Este important să se sublinieze faptul că activitățile de colectare masivă de date privind comunicațiile pe internet pe care le desfășoară serviciile de informații prin obținerea de informații pe baza semnalelor electromagnetice funcționează într-o proporție mică pe internet. În plus, utilizarea de întrebări specifice, astfel cum s-a descris mai sus, garantează că doar acele elemente despre care se crede că ar putea fi importante pentru serviciile de informații sunt prezentate pentru a fi examinate de analiști. Aceste limite sunt destinate să protejeze viața privată și libertățile civile ale tuturor persoanelor, indiferent de naționalitatea acestora și indiferent unde ar locui.

([1]) Disponibile la adresa www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#ppd-28. Aceste proceduri pun în aplicare conceptele de direcționare și adaptare discutate în prezenta scrisoare într-un mod specific pentru fiecare element al serviciilor de informații.

([2]) Pentru a da un singur exemplu, procedurile de punere în aplicare ale NSA în temeiul PPD-28 precizează că „[o]ri de câte ori este posibil, colectarea va avea loc prin utilizarea unuia sau a mai multor termeni de selecție pentru a concentra colectarea asupra unor ținte specifice ale informațiile externe (de exemplu, un anumit terorist sau grup de terorism internațional cunoscut) sau informații externe pe teme specifice (de exemplu, proliferarea armelor de distrugere în masă de către o putere străină sau agenții săi)."

([3]) Disponibil la http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf.

Statele Unite ale Americii au creat procese pentru a se asigura că activitățile de colectare de informații electromagnetice sunt efectuate numai în scopuri de securitate națională adecvată. În fiecare an, președintele stabilește cele mai importante priorități naționale pentru colectarea de informații externe, după un îndelung proces formal între agenții. DNI este responsabilă de transpunerea acestor priorități ale serviciilor de informații în Cadrul național de priorități ale serviciilor de informații (National Intelligence Priorities Framework – NIPF). PPD-28 a consolidat și a îmbunătățit procesul dintre agenții menit să asigure că toate prioritățile în materie de informații ale serviciilor de informații sunt analizate și aprobate de către factorii de decizie de la nivel înalt. Directiva privind serviciile de informații (ICD) 204 oferă orientări suplimentare cu privire la NIPF și a fost actualizată în ianuarie 2015 pentru a include cerințele PPD-28 ([1]). Deși NIPF sunt informații clasificate, referitoare la prioritățile specifice ale SUA cu privire la informațiile externe, acestea sunt prezentate anual în documentul declasificat al DNI Evaluarea amenințărilor la nivel mondial (Worldwide Threat Assessment), care este disponibil, de asemenea, pe site-ul ODNI.

Prioritățile NIPF prezintă un nivel destul de ridicat de generalitate. Acestea includ teme cum ar fi urmărirea materialelor nucleare și capacități în materie de rachete balistice ale anumitor adversari externi, efectele corupției cauzate de cartelurile care fac trafic de droguri și abuzurile în materie de drepturile omului din anumite țări. Acestea se aplică nu numai informațiilor colectate pe baza semnalelor electromagnetice, ci tuturor activităților serviciilor de informații. Organizația care este responsabilă de traducerea priorităților din NIPF în colectarea efectivă de informații pe baza semnalelor electromagnetice este Comitetul național pentru colectarea de informații pe baza semnalelor electromagnetice sau SIGCOM. Acesta funcționează sub conducerea directorului Agenției Naționale de Securitate (NSA), care este desemnat prin Decretul 12333 ca „administrator funcțional pentru obținerea de informații pe baza semnalelor electromagnetice”, responsabil cu supravegherea și coordonarea în comunitatea serviciilor de informații, aflat sub supravegherea atât a Secretarului Apărării, cât și a DNI. SIGCOM este format din reprezentanți ai tuturor elementelor comunității serviciilor de informații și, întrucât Statele Unite pune pe deplin în aplicare PPD-28, acesta va avea, de asemenea, reprezentare deplină din partea altor departamente și agenții cu un interes politic în obținerea informațiilor pe baza semnalelor electromagnetice.

Toate departamentele și agențiile din SUA care sunt consumatori de informații externe își prezintă cererile de colectare la SIGCOM. SIGCOM examinează aceste cereri, se asigură că sunt conforme cu NIPF și le ordonează în funcție de prioritate, pe baza unor criterii precum:

— Pot informațiile colectate pe baza semnalelor electromagnetice să furnizeze informații utile în acest caz sau există surse mai bune sau mai rentabile de informații pentru a aborda această cerință, cum ar fi imagini sau informații cu sursă deschisă?

— Cât de importante sunt aceste nevoi de informații? În cazul în care aceasta este o prioritate de prim rang în NIPF, de cele mai multe ori, va fi o prioritate ridicată pentru obținerea de informații pe baza semnalelor electromagnetice.

— Ce tip de informații colectate pe baza semnalelor electromagnetice pot fi utilizate?

— Este colectarea cât mai adaptată posibil? Ar trebui să existe restricții de timp, geografice sau alte restricții?

Procesul de stabilire a cerințelor SUA de colectare de informații pe baza semnalelor electromagnetice necesită, de asemenea, luarea în considerare în mod explicit a altor factori, și anume:

— Sunt obiectivul colectării sau metodologia utilizată pentru colectare deosebit de sensibile? În cazul unui răspuns afirmativ, acest lucru va necesita examinarea de către factori de decizie.

— Va prezenta colectarea un risc nejustificat pentru viața privată și libertățile civile, indiferent de naționalitate?

— Sunt necesare garanții suplimentare pentru diseminarea și păstrarea confidențialității pentru a proteja confidențialitatea sau interesele de securitate națională?

În cele din urmă, la încheierea procesului, membrii personalului instruit al NSA preiau prioritățile validate de SIGCOM și cercetează și identifică anumiți termeni, cum ar fi numere de telefon, adrese de e-mail, care ar trebui să colecteze informații externe în măsură să răspundă la aceste priorități. Orice selector trebuie să fie revizuit și aprobat înainte de a fi introdus în sistemele de colectare ale NSA. Cu toate acestea, faptul dacă și momentul când are loc colectarea efectivă depinde, în parte, de elemente suplimentare, cum ar fi disponibilitatea resurselor adecvate de colectare. Acest proces

([1]) Disponibil la adresa http://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf.

asigură că țintele activităților SUA de colectare de informații pe baza semnalelor electromagnetice reflectă nevoi pertinente și importante de informații externe. De asemenea, atunci când colectarea este efectuată în conformitate cu FISA, NSA și alte agenții trebuie să respecte restricții suplimentare aprobate de Curtea de Supraveghere a Activităților Străine de Spionaj (Foreign Intelligence Surveillance Court). Pe scurt, nici NSA, nici orice altă agenție de informații din SUA nu decide pe cont propriu ce să colecteze.

În general, acest proces garantează că toate prioritățile de informații ale SUA sunt stabilite de factori de decizie politică de rang înalt care se află în cea mai bună poziție pentru a identifica cererile SUA de informații externe și că acești factori de decizie iau în considerare nu numai valoarea potențială a colectării de informații, ci și riscurile asociate acestei colectări, inclusiv riscurile la adresa vieții private, a intereselor economice naționale și a relațiilor externe.

Cu privire la datele transmise către Statele Unite în temeiul Scutului de confidențialitate, deși Statele Unite nu poate confirma sau infirma metode sau operațiuni specifice ale serviciilor de informații, cerințele PPD-28 se aplică oricărei operațiuni de colectare de informații pe baza semnalelor electromagnetice desfășurate de Statele Unite, indiferent de tipul sau sursa datelor care sunt colectate. În plus, limitările și garanțiile aplicabile colectării de informații pe baza semnalelor electromagnetice se aplică informațiilor astfel colectate în scopuri autorizate, inclusiv pentru relații externe și în scopuri de securitate națională.

Procedurile menționate anterior demonstrează un angajament clar de a împiedica colectarea arbitrară și nediscriminatorie a informațiilor pe baza semnalelor electromagnetice și de a pune în aplicare – de la cele mai înalte niveluri ale administrației – principiul caracterului rezonabil. PPD-28 și procedurile de punere în aplicare ale agenției clarifică limitările existente și cele noi și descriu cu mai multă precizie scopul pentru care Statele Unite colectează și utilizează informațiile obținute pe baza semnalelor electromagnetice. Acestea ar trebui să garanteze faptul că activitățile de colectare de informații pe baza semnalelor electromagnetice sunt și vor continua să fie efectuate numai pentru a îndeplini obiective legitime legate de colectarea de informații externe.

c. **Limitările referitoare la păstrare și difuzare**

Secțiunea 4 din PPD-28 impune fiecărui element al comunității serviciilor de informații să aibă limite explicite privind păstrarea și difuzarea informațiilor cu caracter personal referitoare la persoane care nu sunt cetățeni americani colectate pe bază de semnale electromagnetice, comparabile cu limitele pentru cetățenii americani. Aceste norme sunt încorporate în proceduri pentru fiecare agenție, care au fost publicate în februarie 2015 și sunt accesibile publicului. Pentru a se califica pentru păstrarea și difuzarea de informații externe, informațiile cu caracter personal trebuie să se refere la o cerere autorizată de informații, după cum se stabilește în cursul procesului NIPF descris mai sus; se consideră în mod rezonabil a fi dovezi ale unei infracțiuni; sau îndeplinesc unul dintre celelalte standardele pentru păstrarea informațiilor referitoare la persoana din SUA identificate în Decretul 12333 secțiunea 2.3.

Informațiile pentru care nu s-a făcut o astfel de determinare nu pot fi păstrate mai mult de cinci ani, cu excepția cazului în care DNI stabilește în mod explicit că păstrarea în continuare este în interesul securității naționale al Statelor Unite. Prin urmare, elementele serviciilor de informații trebuie să șteargă informațiile persoanei din afara SUA colectate pe baza semnalelor electromagnetice după cinci ani, cu excepția cazului în care, de exemplu, informațiile au fost considerate a fi relevante pentru o cerere autorizată de informații externe sau dacă DNI stabilește, luând în considerare opiniile responsabilului ODNI pentru protecția libertăților civile și a funcționarilor agenției pentru protecția vieții private și a libertăților civile, că păstrarea în continuare este în interesul securității naționale.

În plus, în prezent, toate politicile agențiilor care pun în aplicare PPD-28 prevăd în mod explicit că informațiile referitoare la o persoană nu pot fi transmise numai pentru motivul că o persoană este din afara SUA, iar ODNI a emis o directivă pentru toate elementele serviciilor de informații ([1]) pentru a reflecta această cerință. Membrii personalului comunității serviciilor de informații sunt obligați să ia în considerare interesele legate de viața privată ale persoanelor care nu sunt cetățeni americani la elaborarea și difuzarea de rapoarte de informații. În special, informațiile obținute pe baza semnalelor electromagnetice despre activitățile obișnuite ale unei persoane străine nu ar trebui considerate informații externe care ar putea fi diseminate sau păstrate în permanență prin acest simplu fapt, cu excepția cazului în care aceste informații răspund în alt mod unei cereri neautorizate de informații externe. Aceasta recunoaște o limitare importantă și răspunde preocupărilor Comisiei Europene cu privire la amploarea definiției informațiilor externe, astfel cum se prevede în Decretul 12333.

([1]) Directiva privind comunitatea serviciilor de informații (DCI) 203, disponibilă la adresa http://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.

d. **Conformitatea și supravegherea**

Sistemul american de control al informațiilor externe oferă supraveghere riguroasă și pe mai multe niveluri pentru a asigura conformitatea cu legile și procedurile aplicabile, inclusiv cele referitoare la colectarea, păstrarea și difuzarea informațiilor referitoare la persoane care nu sunt cetățeni ai SUA, obținute pe baza semnalelor electromagnetice, astfel cum prevede PPD-28. Printre acestea:

— Comunitatea serviciilor de informații dispune de sute de membri ai personalului cu atribuții de supraveghere. Doar ANS dispune de 300 de persoane cu atribuții speciale de asigurare a conformității, iar alte elemente dispun, de asemenea, de birouri de supraveghere. În plus, Departamentul de Justiție asigură măsuri ample de supraveghere a activităților serviciilor de informații, iar Ministerul Apărării asigură, de asemenea, măsuri de supraveghere.

— Fiecare element din cadrul serviciilor de informații are propriul birou al inspectorului general însărcinat cu supravegherea activităților serviciilor de informații străine, printre altele. Inspectorii generali sunt independenți din punct de vedere statutar; aceștia au competență amplă de a efectua investigații, audituri și evaluări ale programelor, inclusiv cazuri de fraudă și abuz sau încălcare a legii și pot recomanda acțiuni corective. Deși recomandările inspectorului general nu au caracter obligatoriu, rapoartele inspectorului general sunt deseori puse la dispoziția publicului și, în orice caz, sunt transmise Congresului Statelor Unite; această prevedere include rapoarte de monitorizare în cazul în care măsurile corective recomandate în rapoartele anterioare nu au fost încă finalizate. Prin urmare, Congresul este informat cu privire la orice neconformitate și poate exercita presiune, inclusiv prin mijloace bugetare, pentru a obține măsuri corective. O serie de rapoarte ale inspectorului general privind programele serviciilor de informații au fost făcute publice ([1]).

— Biroul pentru protecția vieții private și a libertăților civile (CLPO) al ODNI este responsabil cu asigurarea faptului că serviciile de informații funcționează într-un mod care promovează securitatea națională, protejând în același timp libertățile civile și dreptul la viață privată. ([2]) Alte elemente ale comunității serviciilor de informații au proprii responsabili pe probleme de confidențialitate.

— Comitetul de supraveghere în materie de protecție a vieții private și a libertății civile (PCLOB), organism independent, constituit prin lege, este însărcinat să analizeze și să revizuiască programele și politicile de combatere a terorismului, inclusiv utilizarea informațiilor colectate pe baza semnalelor electromagnetice, pentru a asigura protejarea adecvată a vieții private și a libertăților civile. Acesta a emis mai multe rapoarte publice referitoare la activitățile serviciilor de informații.

— Astfel cum se precizează în detaliu mai jos, Curtea de Supraveghere a Activităților Străine de Spionaj, instanță formată din judecători federali independenți, este responsabilă cu supravegherea și conformitatea activităților de colectare de informații pe baza semnalelor electromagnetice desfășurate în temeiul FISA.

— În sfârșit, Congresul SUA, și anume Camera Reprezentanților și comisiile Senatului pentru informații și pentru sistemul judiciar, au responsabilități de supraveghere semnificative cu privire la toate activitățile de spionaj ale SUA, inclusiv activitățile SUA de colectare de informații pe baza semnalelor electromagnetice.

Pe lângă aceste mecanisme oficiale de supraveghere, comunitatea serviciilor de informații dispune de numeroase mecanisme concepute să garanteze că serviciile de informații respectă limitările privind colectarea descrise mai sus. De exemplu:

— Funcționarii guvernamentali trebuie să își valideze necesarul anual de informații colectate pe baza semnalelor electromagnetice.

— ANS verifică țintele activității de colectare de informații pe baza semnalelor electromagnetice pe tot parcursul procesului de colectare pentru a stabili dacă acestea furnizează efectiv informații externe valoroase care răspund priorităților și va întrerupe colectarea de la ținte care nu îndeplinesc această condiție. Proceduri suplimentare asigură că termenii de selecție sunt revizuiți periodic.

([1]) A se vedea, de exemplu, Raportul inspectorului general al Departamentului de Justiție al SUA intitulat „O revizuire a activităților Biroului Federal de Investigații în temeiul articolului 702 din Legea privind supravegherea activităților străine de spionaj din 2008” (septembrie 2012), disponibil la adresa https://oig.justice.gov/reports/2016/o1601a.pdf.

([2]) A se vedea www.dni.gov/clpo.

— În baza unei recomandări din partea Grupului independent de examinare desemnat de președintele Obama, DNI a instituit un nou mecanism pentru a monitoriza colectarea și difuzarea de informații colectate pe baza semnalelor electromagnetice care sunt deosebit de sensibile din cauza naturii țintei sau a mijloacelor de colectare, pentru a se asigura că aceasta este în concordanță cu hotărârile factorilor de decizie.

— În cele din urmă, ODNI examinează anual alocarea resurselor serviciilor de informații în funcție de prioritățile NIPF și misiunea serviciilor de informații în ansamblu. Această revizuire include evaluări ale valorii tuturor tipurilor de colectare de informații, inclusiv informațiile colectate pe baza semnalelor electromagnetice, și analizează retrospectiv – cât de mult succes au avut serviciile de informații în atingerea obiectivelor acestora? – și anticipativ – de ce vor avea nevoie serviciile de informații în viitor? Acest lucru garantează că resursele de informații colectate pe baza semnalelor electromagnetice sunt utilizate pentru cele mai importante priorități naționale.

Astfel cum reiese din această imagine de ansamblu, serviciile de informații nu decid singure cu privire la conversațiile pe care să le asculte, nu încearcă să colecteze toate datele sau să opereze fără control. Activitățile acestora se axează pe priorități stabilite de către factorii de decizie, printr-o procedură care implică contribuția guvernului și care este supervizată atât în interiorul NSA, cât și de către ODNI, Departamentul de Justiție și Departamentul Apărării.

PPD-28 conține, de asemenea, numeroase alte dispoziții care garantează că informațiile cu caracter personal colectate în cadrul activităților de colectare de informații pe baza semnalelor electromagnetice sunt protejate, indiferent de naționalitate. De exemplu, PPD-28 include dispoziții privind securitatea datelor, accesul și proceduri de verificare a calității pentru a proteja informațiile cu caracter personal colectate prin activitățile de colectare de informații pe baza semnalelor electromagnetice și prevede cursuri obligatorii de formare pentru a garanta că forța de muncă are cunoștință de responsabilitatea de a proteja datele personale, indiferent de naționalitate. PPD prevede, de asemenea, mecanisme suplimentare de supraveghere și de conformitate. Printre acestea se numără și revizuiri periodice și audituri efectuate de funcționari corespunzători cu sarcini de supraveghere și de asigurare a conformității cu privire la practicile de protejare a informațiilor personale conținute în informațiile obținute pe baza semnalelor electromagnetice. Evaluările trebuie să examineze, de asemenea, conformitatea cu procedurile agențiilor pentru protecția acestor informații.

În plus, PPD-28 prevede că problemele de conformare semnificative legate de persoanele care nu sunt cetățeni americani vor fi abordate la niveluri de conducere din cadrul administrației publice. În cazul în care apare o problemă importantă de conformare care implică informații cu caracter personal ale unei persoane, obținute ca urmare a activităților de colectare de informații pe baza semnalelor electromagnetice, problema respectivă, și alte cerințe de raportare existente, trebuie raportate fără întârziere la DNI. În cazul în care problema se referă la informațiile cu caracter personal ale unei persoane care nu este cetățean american, DNI, în consultare cu secretarul de stat și șeful serviciului de informații în cauză, va stabili dacă ar trebui să se ia măsuri pentru a informa guvernul străin respectiv, în conformitate cu normele de protecție a surselor și metodelor și a personalului american. În plus, în conformitate cu indicațiile PPD-28, secretarul de stat a identificat un înalt funcționar, Subsecretarul Catherine Novelli, care să servească drept punct de contact pentru administrațiile străine care doresc să își exprime preocuparea cu privire la activitățile Statelor Unite de colectare de informații pe baza semnalelor electromagnetice. Acest angajament de implicare la nivel înalt demonstrează eforturile depuse de guvernul SUA în ultimii ani pentru a inspira încredere în măsurile de protecție a vieții private, numeroase și care coincid, care sunt valabile pentru informațiile persoanelor din SUA și ale persoanelor din afara SUA.

e. **Sinteză**

Procesele Statelor Unite instituite pentru colectarea, păstrarea și difuzarea de informații externe oferă măsuri importante de protecție a confidențialității pentru informațiile cu caracter personal ale tuturor persoanelor, indiferent de naționalitate. În special, aceste procese asigură că serviciile noastre de informații se concentrează asupra misiunii lor de securitate națională, astfel cum prevede legislația aplicabilă, decretele și directivele prezidențiale; protejează informațiile împotriva accesului, utilizării și divulgării neautorizate; și își desfășoară activitățile sub supraveghere și mai multe niveluri de control, inclusiv comitetele de supraveghere din cadrul Congresului. PPD-28 și procedurile sale de punere în aplicare reprezintă eforturile noastre de a extinde anumite principii de reducere la minimum și alte principii de protecție a datelor la informațiile cu caracter personal ale tuturor persoanelor, indiferent de naționalitate. Informațiile cu caracter personal obținute prin activitățile SUA de colectare de informații pe baza semnalelor electromagnetice respectă principiile și cerințele legislației SUA și ale directivei prezidențiale, inclusiv măsurile de protecție prevăzute în PPD-28. Aceste principii și cerințe asigură că toate persoanele sunt tratate cu demnitate și respect, indiferent de naționalitate sau reședință și recunosc faptul că toate persoanele au așteptări legitime de confidențialitate în tratarea informațiilor cu caracter personal ale acestora.

II. LEGEA PRIVIND SUPRAVEGHEREA ACTIVITĂȚILOR STRĂINE DE SPIONAJ – SECȚIUNEA 702

Colectarea în temeiul secțiunii 702 din Legea privind supravegherea activităților străine de spionaj ([1]) nu este „în masă și arbitrară", ci este strict orientată asupra colectării de informații externe de la ținte legitime identificate individual; este abilitată în mod clar prin competențe legale explicite; și este supusă atât controlului judiciar independent, cât și revizuirii substanțiale și supravegherii în cadrul executivului și al Congresului. Colectarea în temeiul secțiunii 702 este considerată colectare de informații pe baza semnalelor electromagnetice care fac obiectul cerințelor PPD-28 ([2]).

Colectarea în temeiul secțiunii 702 este una dintre cele mai importante surse de informații care protejează atât Statele Unite, cât și partenerii europeni. Informații detaliate cu privire la funcționarea și supravegherea în temeiul secțiunii 702 sunt puse la dispoziția publicului. Numeroase acțiuni introduse, hotărâri judecătorești și rapoarte de supraveghere referitoare la program au fost declasificate și publicate pe site-ul ODNI pentru publicarea informațiilor, www.icontherecord.tumblr.com. În plus, secțiunea 702 a fost analizată în profunzime de PCLOB, într-un raport care este disponibil la adresa https://www.pclob.gov/library/702-Report.pdf ([3]).

Secțiunea 702 a fost adoptată ca parte din Legea de modificare a FISA din 2008 ([4]), după o amplă dezbatere publică în Congres. Aceasta permite obținerea de informații externe prin vizarea persoanelor care nu sunt cetățeni americani aflate în afara Statelor Unite, cu sprijinul obținut prin ordin judecătoresc al furnizorilor americani de servicii de comunicații electronice. Secțiunea 702 autorizează procurorul general și DNI – doi funcționari de la nivelul cabinetului numiți de Președinte și confirmați de către Senat – să prezinte certificări anuale Curții FISA ([5]). Aceste certificări identifică anumite categorii de informații care trebuie să fie colectate, cum ar fi informații referitoare la combaterea terorismului sau la armele de distrugere în masă, care trebuie să se încadreze în categoriile de informații externe definite de Legea FISA ([6]). Astfel cum a menționat PCLOB, „[a]ceste limitări nu permit colectarea de informații cu privire la străinii fără restricții" ([7]).

De asemenea, certificările trebuie să includă „direcționarea" și „reducerea la minimum" a procedurilor care trebuie examinate și aprobate de Curtea FISA ([8]). Procedurile de direcționare sunt menite să asigure că activitatea de colectare are loc doar astfel cum a fost autorizată de lege și se încadrează în domeniul de aplicare a certificării; procedurile de reducere la minimum sunt concepute pentru a limita achiziționarea, diseminarea și păstrarea informațiilor privind cetățeni americani, dar și pentru a cuprinde dispoziții care oferă o protecție considerabilă informațiilor despre persoane care nu sunt cetățeni americani, astfel cum este descris mai jos. În plus, astfel cum s-a descris mai sus, în PPD-28, Președintele a decis ca serviciile de informații să prevadă măsuri suplimentare de protecție pentru informațiile cu caracter personal referitoare la persoane care nu sunt cetățeni americani și că aceste măsuri de protecție se aplică informațiilor colectate în conformitate cu secțiunea 702.

După ce instanța aprobă procedurile de direcționare și de reducere la minimum, colectarea în conformitate cu secțiunea 702 nu este masivă sau arbitrară, ci „constă în întregime din vizarea anumitor persoane stabilite în mod individual", după cum a declarat PCLOB ([9]). Colectarea este direcționată prin utilizarea de selectoare individuale, cum ar fi adrese de e-mail sau numere de telefon, pe care personalul serviciilor americane de informații le-a stabilit că pot fi utilizate pentru

([1]) 50 U.S.C. § 1881a.

([2]) De asemenea, Statele Unite pot obține ordine judecătorești în temeiul altor dispoziții din FISA pentru producerea de date, inclusiv datele transferate în temeiul Scutului de confidențialitate. A se vedea 50 U.S.C. § 1801 și Titlurile I și III din FISA, care autorizează supravegherea electronică și, respectiv, percheziții fizice, solicită un ordin judecătoresc (cu excepția situațiilor de urgență) și necesită întotdeauna un motiv întemeiat de a crede că ținta este o putere străină sau un agent al unei puteri străine. TITLUL IV din FISA autorizează utilizarea interceptărilor (pen registers) și a dispozitivelor de capturare și trasabilitate (trap and trace), în conformitate cu un ordin judecătoresc (cu excepția situațiilor de urgență), în investigații autorizate ale informațiilor externe, contrainformații sau de combatere a terorismului. TITLUL V din FISA permite FBI, în conformitate cu un ordin judecătoresc (cu excepția situațiilor de urgență), să obțină documente comerciale care sunt relevante pentru investigații autorizate ale informațiilor externe, contrainformații sau de combatere a terorismului. După cum s-a arătat mai jos, USA FREEDOM Act interzice în mod specific utilizarea ordinelor de interceptare sau de confiscare a registrelor comerciale în temeiul FISA pentru colectarea masivă de date și impune cerința unui „termen specific de selecție" pentru a se asigura că acestea sunt utilizate într-un mod direcționat.

([3]) Comitetul pentru protecția vieții private și a libertății civile, „Raport privind programul de supraveghere care funcționează în conformitate cu secțiunea 702 din Legea privind supravegherea activităților străine de spionaj" (2 iulie 2014) („Raportul PCLOB").

([4]) A se vedea Pub. L. No. 110-261, 122 Stat. 2436 (2008).

([5]) A se vedea 50 U.S.C. § 1881a(a) și (b).

([6]) A se vedea idem § 1801(e).

([7]) A se vedea Raportul PCLOB la 99.

([8]) A se vedea 50 U.S.C. § 1881a(d) și (e).

([9]) A se vedea Raportul PCLOB la 111.

a comunica informații externe de tipul celor acoperite de certificare prezentate în instanță ([1]). Baza pentru selecția țintei trebuie să fie documentată, iar documentația pentru fiecare selector este revizuită ulterior de Departamentul de Justiție ([2]). Guvernul SUA a publicat informații care arată că, în anul 2014, au existat aproximativ 90 000 de persoane vizate în conformitate cu secțiunea 702, o fracțiune minusculă din cele peste 3 miliarde de utilizatori ai internetului din întreaga lume ([3]).

Au fost făcute publice informații colectate în conformitate cu secțiunea 702 care fac obiectul procedurilor aprobate de instanță de reducere la minimum oferind astfel măsuri de protecție persoanelor care nu sunt cetățeni americani, precum și cetățenilor americani ([4]). De exemplu, comunicații obținute în temeiul secțiunii 702, fie ale unor cetățeni americani sau ale unor persoane care nu sunt cetățeni americani, sunt stocate în baze de date cu controale de acces stricte. Acestea pot fi revizuite numai de către membri ai personalului serviciilor de informații care au fost instruiți în ceea ce privește procedurile de reducere la minimum de protecție a confidențialității și care au fost aprobate în mod expres pentru acest acces pentru îndeplinirea funcțiilor lor autorizate ([5]). Utilizarea datelor se limitează la identificarea informațiilor privind servicii străine de spionaj sau dovezi ale unei infracțiuni ([6]). În temeiul PPD-28, aceste informații pot fi difuzate numai dacă există un scop valid legat de colectarea de informații externe sau în scopul aplicării legii; simplul fapt că o parte la comunicare nu este cetățean american nu este suficient ([7]). Procedurile de reducere la minimum și PPD-28 prevăd limite de timp în care pot fi păstrate datele obținute în conformitate cu punctul 702 ([8]).

Supravegherea în temeiul secțiunii 702 are loc la scară largă și este realizată de toate cele trei ramuri ale guvernului. Agențiile de aplicare a legii au diferite niveluri de control intern, inclusiv controale efectuate de către inspectorii generali independenți și controalele tehnologice în ceea ce privește accesul la date. Departamentul de Justiție și ODNI examinează îndeaproape și controlează utilizarea secțiunii 702 pentru a verifica conformitatea cu dispozițiile legale în vigoare; agențiile au, de asemenea, obligația independentă de a raporta potențiale incidente de neconformitate. Aceste incidente sunt anchetate și toate incidentele de conformitate sunt raportate Curții de Supraveghere a Activităților Străine de Spionaj, Comitetului de supraveghere a serviciilor de informații al Președintelui și Congresului Consiliului și sunt remediate în mod corespunzător. ([9]) Până în prezent, nu au existat incidente care să implice tentative de încălcare intenționată a legii sau de eludare a cerințelor juridice ([10]).

Curtea FISA joacă un rol important în punerea în aplicare a secțiunii 702. Aceasta este formată din judecători federali independenți numiți pentru un mandat de șapte ani la Curtea FISA, dar care, la fel ca toți judecătorii federali, sunt judecători pe viață. Astfel cum s-a menționat mai sus, Curtea trebuie să examineze certificările anuale și procedurile de direcționare și de reducere la minimum în conformitate cu legea. În plus, astfel cum s-a menționat mai sus, guvernul are obligația de a notifica imediat Curtea cu privire la problemele de conformitate ([11]) și mai multe avize ale curții au fost declasificate și publicate, demonstrând nivelul excepțional de control judiciar și independență exercitat în revizuirea acestor incidente.

Procesele riguroase ale Curții au fost descrise de către fostul președinte al completului de judecată într-o scrisoare adresată Congresului, care a fost făcută publică ([12]). De asemenea, ca rezultat al USA FREEDOM Act, astfel cum se descrie mai jos, în prezent Curtea este autorizată în mod explicit să numească un avocat extern ca avocat independent în numele protecției vieții private în cazurile care prezintă elemente de noutate sau aspecte juridice importante ([13]). Acest grad de implicare al unui sistem judiciar independent național în activitățile de spionaj străin care vizează persoane care nu sunt cetățeni ai țării respective, nici aflate în interiorul acesteia, este neobișnuit, dacă nu fără precedent, și contribuie la garantarea faptului că activitățile de colectare de informații în temeiul secțiunii 702 au loc în limitele legale corespunzătoare.

([1]) *Id*.

([2]) *Id*. la 8; 50 U.S.C. § 1881a(l); a se vedea, de asemenea, Raportul directorului NSA pentru protecția libertăților civile și a vieții private, „Punerea în aplicare de către NSA a secțiunii 702 din Legea privind supravegherea activităților străine de spionaj" (denumit în continuare „Raportul NSA") la punctul 4, disponibil la adresa http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

([3]) Raportul privind transparența din 2014 al Directorului serviciilor naționale de informații, disponibil la adresa http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014.

([4]) Procedurile de reducere la minimum disponibile la adresa: http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf (Procedurile de reducere la minimum ale NSA); http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf; și http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf.

([5]) A se vedea Raportul NSA la 4.

([6]) A se vedea, de exemplu, Procedurile de reducere la minimum ale NSA la 6.

([7]) Procedurile Agenției de Informații în temeiul PPD-28 disponibile la adresa http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

([8]) A se vedea Procedurile de reducere la minimum ale NSA; PPD-28 articolul 4.

([9]) A se vedea 50 U.S.C. § 1881(l); a se vedea, de asemenea raportul PCLOB la paginile 66-76.

([10]) A se vedea Evaluarea bianuală a conformității cu procedurile și orientările emise în temeiul secțiunii 702 din Legea privind supravegherea activităților străine de spionaj, transmisă de procurorul general și directorul serviciilor naționale de informații la 2–3, disponibilă la adresa http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf.

([11]) Norma nr. 13 din Regulamentul de procedură al Curții de Supraveghere a Activităților Străine de Spionaj, disponibil la adresa http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

([12]) Scrisoarea din 29 iulie 2013 a distinsului Reggie B. Walton către distinsul Patrick J. Leahy, disponibilă la adresa http://fas.org/irp/news/2013/07/fisc-leahy.pdf.

([13]) A se vedea articolul 401 din USA FREEDOM Act, P.L. 114-23.

Congresul își exercită competența de supraveghere prin rapoarte impuse prin lege transmise comisiilor privind serviciile de informații și sistemul judiciar, precum și prin întâlniri de informare și audieri frecvente. Printre acestea se numără un raport bianual elaborat de către procurorul general privind utilizarea secțiunii 702 și orice incidente de conformitate ([1]); o evaluare bianuală separată efectuată de către procurorul general și DNI privind respectarea procedurilor de direcționare și reducere la minimum, inclusiv conformitatea cu procedurile menite să se asigure că se colectează în scopuri valide legate de informații externe ([2]); și un raport anual al șefilor serviciilor de informații care să includă o atestare a faptului că activitățile de colectare de informații în temeiul secțiunii 702 continuă să producă informații privind servicii străine de spionaj ([3]).

Pe scurt, colectarea în temeiul secțiunii 702 este autorizată prin lege; face obiectul mai multor niveluri de control, supraveghere judiciară și control; și, astfel cum a declarat Curtea FISA într-un aviz declasificat recent, „nu este efectuată în masă sau nediferențiat", ci „prin... decizii de direcționare discrete pentru unități individuale de [comunicații]" ([4]).

III. LEGEA SUA PRIVIND LIBERTATEA (USA FREEDOM ACT)

USA FREEDOM Act, promulgată în iunie 2015, a modificat în mod semnificativ măsurile de supraveghere din SUA și alte mecanisme naționale de securitate și a sporit transparența publică cu privire la utilizarea acestor competențe și cu privire la deciziile Curții FISA, astfel cum se arată mai jos. ([5]) Legea garantează faptul că profesioniștii din domeniul informațiilor și aplicării legii dispun de mecanismele de care au nevoie pentru a proteja țara, continuând să asigure în același timp protecția corespunzătoare a vieții private a persoanelor, atunci când sunt utilizate aceste mecanisme. Aceasta îmbunătățește protecția vieții private și a libertăților civile și crește transparența.

Legea interzice colectarea masivă de date, inclusiv ale cetățenilor americani și ale persoanelor care nu sunt cetățeni americani, în temeiul diferitelor dispoziții din FISA sau prin intermediul scrisorilor privind securitatea națională, o formă de citație administrativă autorizată de lege ([6]). Această interdicție include în mod specific metadatele telefoanelor legate de apeluri dintre persoane din SUA și persoanele din afara SUA și va include, de asemenea, colectarea de informații în baza Scutului de confidențialitate în temeiul acestor mecanisme. Legea prevede că guvernul trebuie să își fundamenteze orice cerere pentru înregistrări în temeiul acestor mecanisme pe un „termen specific de selecție" – un termen care identifică în mod specific o persoană, un cont, o adresă sau un dispozitiv personal într-un mod care să limiteze domeniul de aplicare a informațiilor solicitate, în cea mai mare măsură posibilă în mod rezonabil ([7]). Aceasta asigură în continuare faptul că activitățile de colectare de informații în scopuri de spionaj sunt bine orientate și direcționate.

De asemenea, legea a introduse modificări semnificative ale procedurilor în fața Curții FISA, care sporesc gradul de transparență și oferă garanții suplimentare privind protecția confidențialității. Astfel cum s-a menționat mai sus, legea a autorizat crearea unui grup permanent de avocați cu autorizație de securitate, specializați în protecția vieții private și a libertăților civile, colectare de informații, tehnologia comunicațiilor sau în alte domenii, care ar putea fi desemnați să apară în fața instanței în calitate de amicus curiae în cazuri care implică interpretări de drept noi sau importante. Acești avocați sunt autorizați să prezinte argumente juridice care favorizează protecția vieții private și a libertăților civile și vor avea acces la orice informații, inclusiv informații clasificate, pe care Curtea le consideră necesare pentru îndeplinirea atribuțiilor acestora ([8]).

Legea se bazează, de asemenea, pe transparența fără precedent a guvernului SUA privind activitățile de spionaj, care solicită ca DNI, în consultare cu procurorul general, să declasifice sau să publice un rezumat neclasificat al fiecărei decizii, ordonanțe sau aviz emis de Curtea FISA sau de instanța de revizuire FISA care include o analiză sau interpretare importantă a unei dispoziții de drept.

([1]) A se vedea 50 U.S.C. § 1881f.
([2]) A se vedea id. § 1881a(l)(1).
([3]) A se vedea id. § 1881a(l)(3). Unele dintre aceste rapoarte sunt clasificate.
([4]) Mem. Aviz și ordin la 26 (FISC 2014), disponibile la adresa http://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.
([5]) A se vedea USA FREEDOM Act din 2015, Pub. L. No. 114-23, § 401, 129 Stat. 268.
([6]) A se vedea id. §§ 103, 201, 501. Scrisorile privind securitatea națională sunt autorizate printr-o varietate de legi și permit FBI-ului să obțină informațiile cuprinse în rapoartele de credit, evidențe contabile și documentele electronice ale abonaților și istoricul tranzacțiilor de la anumite tipuri de societăți, doar pentru a proteja împotriva terorismului internațional sau a activităților clandestine ale serviciilor de informații. A se vedea 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-1681v; 18 U.S.C. § 2709. Scrisorile privind securitatea națională sunt de obicei utilizate de FBI pentru a colecta informații esențiale în primele faze ale investigațiilor de combatere a terorismului și contrainformații, precum identitatea abonatului la un cont care ar fi putut comunica cu agenți ai unei grupări teroriste precum ISIL. Destinatarii unei scrisori de securitate națională au dreptul de a le contesta în justiție. A se vedea 18 U.S.C. § 3511.
([7]) *A se vedea id.*
([8]) *A se vedea id.* § 401.

În plus, legea prevede divulgări extensive despre activitățile de colectare de informații în temeiul FISA și cererile prin scrisoare privind securitatea națională. Statele Unite trebuie să informeze Congresul și să publice în fiecare an numărul de ordine și certificări FISA solicitate și primite; estimări ale numărului de cetățeni americani și ale persoanelor care nu sunt cetățeni americani vizate și afectate de supraveghere; și numărul numirilor de amici curiae, printre alte informații ([1]). Legea impune, de asemenea, rapoarte publice suplimentare din partea guvernului cu privire la numărul de cereri referitoare la scrisoarea privind securitatea națională, referitoare atât la cetățeni americani, cât și la persoane care nu sunt cetățeni americani ([2]).

În ceea ce privește transparența întreprinderilor, legea oferă întreprinderilor o serie de opțiuni pentru a prezenta un raport public privind numărul total de ordine FISA și directive sau scrisori privind securitatea națională pe care le primește din partea guvernului, precum și numărul de conturi ale clienților vizați de aceste ordine ([3]). Mai multe întreprinderi au făcut deja astfel de dezvăluiri, care au evidențiat un număr limitat de clienți ale căror date au fost solicitate.

Aceste rapoarte de transparență corporativă demonstrează că solicitările serviciilor de informații ale SUA afectează doar o fracțiune minusculă a datelor. De exemplu, un raport de transparență recent al unei companii importante arată că aceasta a primit cereri privind securitatea națională (în conformitate cu FISA sau cu scrisorile privind securitatea națională) care afectează mai puțin de 20 000 din conturile sale, în condițiile în care aceasta are cel puțin 400 de milioane de abonați. Cu alte cuvinte, toate cererile privind securitatea națională din SUA raportate de această companie au afectate mai puțin de 0,005 % din abonații acesteia. Chiar dacă fiecare dintre cereri ar fi vizat date în temeiul programului privind sfera de siguranță, ceea ce, desigur, nu este cazul, este evident că solicitările sunt specifice și adecvate ca proporție și nu sunt nici în masă, nici arbitrare.

În cele din urmă, deși legile care autorizează scrisorile privind securitatea națională deja restricționau condițiile în care un destinatar al unei astfel de scrisori ar putea fi exclus de la comunicarea acesteia, legea prevede, de asemenea, că astfel de cerințe de confidențialitate trebuie să fie revizuite periodic; legea prevede că destinatarii scrisorilor privind securitatea națională trebuie notificați în cazul în care faptele nu mai pot justifica o obligație de confidențialitate; și proceduri codificate pentru destinatari, pentru a contesta cerințele de confidențialitate ([4]).

În concluzie, modificările importante aduse de USA FREEDOM Act în ceea ce privește autoritățile americane în materie de informații reprezintă o dovadă clară a efortului pe scară largă depus de Statele Unite de a plasa protecția datelor cu caracter personal, a vieții private, a libertăților civile și a transparența pe primul loc în toate practicile serviciilor americane de informații.

IV. TRANSPARENȚĂ

În plus față de transparența impusă de USA FREEDOM Act, serviciile de informații ale Statelor Unite oferă publicului mai multe informații suplimentare, oferind un exemplu puternic în ceea ce privește transparența în cadrul activităților serviciilor de informații. Serviciile de informații au publicat numeroase informații cu privire la politicile, procedurile, deciziile Curții de Supraveghere a Activităților Străine de Spionaj și alte materiale declasificate, oferind un grad extraordinar de transparență. În plus, serviciile de informații și-au intensificat în mod substanțial comunicarea statisticilor privind utilizarea mecanismelor de colectare de informații privind securitatea națională de către guvern. La 22 aprilie 2015, comunitatea serviciilor de informații a emis cel de al doilea raport anual al său, care prezintă statistici privind frecvența cu care guvernul utilizează aceste mecanisme. De asemenea, ODNI a publicat pe site-ul internet ODNI și pe platforma IC On the Record un set de principii concrete de transparență ([5]) și un plan de punere în aplicare pentru a transpune principiile în inițiative concrete, măsurabile ([6]). În octombrie 2015, directorul serviciilor naționale de informații a decis că fiecare agenție de informații trebuie să desemneze un responsabil cu transparența informațiilor din cadrul conducerii sale pentru a promova transparența și pentru a conduce la inițiative privind transparența ([7]). Responsabilul pentru transparență va colabora îndeaproape cu responsabilul pentru protecția vieții private și a libertăților civile al fiecărei agenții de informații pentru a se asigura că transparența, viața privată și libertățile civile continuă să rămână priorități de maximă importanță.

([1]) *A se vedea id.* § 602.
([2]) *A se vedea id.*
([3]) *A se vedea id.* § 603.
([4]) *A se vedea id.* §§ 502(f)–503.
([5]) Disponibile la adresa http://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles.
([6]) Disponibil la adresa http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Principles%20of%20Intelligence%20Transparency%20Implementation%20Plan.pdf.
([7]) *A se vedea id.*

Pentru a exemplifica aceste eforturi, responsabilul-șef pentru protecția vieții private și a libertăților civile din cadrul NSA a publicat mai multe rapoarte neclasificate în ultimii ani, inclusiv rapoarte cu privire la activitățile desfășurate în temeiul secțiunii 702, al Decretului 12333 și al USA FREEDOM Act ([1]). În plus, serviciile de informații colaborează îndeaproape cu PCLOB, Congresul și comunitatea de promovare a protecției vieții private din SUA pentru a oferi o mai mare transparență cu privire la activitățile de spionaj ale SUA, atunci când acest lucru este fezabil și compatibil cu protecția surselor de informații sensibile și a metodelor de obținere a acestora. Luate în ansamblu, activitățile de spionaj ale SUA sunt la fel de transparente sau mai transparente decât ale oricărei alte țări din lume și sunt cât de transparente posibil pentru a fi în concordanță cu necesitatea de a apăra sursele de informații sensibile și metodele de obținere a acestora.

Pentru a sintetiza transparența amplă care există cu privire la activitățile serviciilor de informații din SUA:

— Comunitatea serviciilor de informații a pus la dispoziție și a publicat online mii de pagini de avize judecătorești și proceduri ale agenției care definesc procedurile și cerințele specifice ale activităților serviciilor de informații. Am publicat, de asemenea, rapoarte privind respectarea restricțiilor aplicabile de către agențiile de informații.

— Periodic, cadrele superioare ale serviciilor de informații vorbesc public despre rolul și activitățile organizațiilor lor, prezentând inclusiv descrieri ale regimurilor de conformitate și ale garanțiilor care reglementează activitatea acestora.

— Serviciile de informații au publicat numeroase documente suplimentare cu privire la activitățile serviciilor de informații în conformitate cu Legea privind libertatea de informare.

— Președintele a emis PPD-28, stabilind restricții suplimentare asupra activităților serviciilor de informații, iar ODNI a emis două rapoarte publice privind punerea în aplicare a acestor restricții.

— În prezent, serviciile de informații au obligația prin lege să comunice avizele semnificative emise de FISA sau rezumate ale acestor avize.

— Guvernul trebuie să prezinte un raport anual privind amploarea utilizării anumitor mecanisme de securitate națională, iar companiile sunt autorizate să facă același lucru.

— PCLOB a emis mai multe rapoarte publice detaliate privind activitățile de spionaj și va continua să facă acest lucru.

— Serviciile de informații furnizează ample informații clasificate comitetelor de supraveghere din cadrul Congresului.

— DNI a emis principii de transparență pentru a reglementa activitățile serviciilor de informații.

Această transparență extinsă va continua în viitor. Orice informații divulgate publicului vor trebui, bineînțeles, să fie disponibile atât pentru Departamentul Comerțului, cât și pentru Comisia Europeană. Revizuirea anuală între Departamentul Comerțului și Comisia Europeană privind punerea în aplicare a Scutului de confidențialitate va oferi o oportunitate pentru Comisia Europeană de a discuta orice chestiune evidențiată de orice noi informații comunicate, precum și orice alte aspecte legate de Scutul de confidențialitate și funcționarea acestuia și înțelegem că Departamentul poate, la alegerea sa, să invite reprezentanți ai altor agenții, inclusiv serviciile de informații, să participe la acest control. Acest lucru este valabil, bineînțeles, pe lângă mecanismul prevăzut în PPD-28 pentru statele membre ale UE de a prezenta preocupările privind activitățile de supraveghere unui funcționar desemnat din cadrul Departamentului de stat.

V. CĂI DE ATAC

Legislația Statelor Unite prevede o serie de căi de atac pentru persoanele care au făcut obiectul supravegherii electronice ilegale în scopuri legate de securitatea națională. În temeiul FISA, dreptul la căi de atac într-o instanță americană nu este limitat la cetățeni americani. O persoană care poate dovedi calitatea sa procesuală activă pentru a introduce o acțiune în

([1]) Disponibile la adresele https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf.

instanță, ar dispune de căi de atac pentru a contesta supravegherea electronică ilegală în temeiul FISA. De exemplu, FISA permite persoanelor supuse supravegherii electronice ilegale să introducă o acțiune în nume propriu în instanță împotriva guvernului SUA, pentru obținerea de daune-interese, inclusiv daune punitive și plata onorariilor avocaților, A se vedea 50 U.S.C. § 1810. Persoanele care pot demonstra calitatea lor procesuală activă pentru a acționa în justiție au, de asemenea, o cauză civilă pentru daune, inclusiv cheltuielile de judecată, împotriva Statelor Unite ale Americii, în cazul în care informații cu privire la acestea, obținute prin activități de supraveghere electronică în temeiul FISA, au fost utilizate sau divulgate ilegal și în mod intenționat, A se vedea 18 U.S.C. § 2712. În cazul în care guvernul intenționează să utilizeze sau să dezvăluie informațiile obținute sau provenite din supravegherea electronică ale persoanei prejudiciate în temeiul FISA împotriva persoanei respective în cadrul unei proceduri judiciare sau administrative în Statele Unite, acesta trebuie să își anunțe intenția Tribunalului și persoanei, care poate contesta legalitatea supravegherii și poate încerca să elimine informațiile, A se vedea 50 U.S.C. § 1806. În cele din urmă, FISA prevede, de asemenea, sancțiuni penale pentru persoanele care se angajează în mod intenționat în activități de supraveghere electronică în conformitate cu litera legii sau care, în mod intenționat, utilizează sau divulgă informațiile obținute prin supraveghere ilegală, A se vedea 50 U.S.C. § 1809.

Cetățenii UE dispun de alte căi de a introduce recurs împotriva funcționarilor guvernamentali americani, pentru utilizarea sau accesul ilegal la date, inclusiv funcționari guvernamentali care încalcă legea în cursul accesului sau a utilizării ilegale a informațiilor în așa-zise scopuri legate de securitatea națională. Legea privind fraudele și abuzurile informatice interzice accesul neautorizat intenționat (care depășește accesul autorizat) pentru a obține informații de la o instituție financiară, dintr-un sistem informatic al guvernului SUA sau cu ajutorul unui computer care poate fi accesat prin intermediul internetului, precum și amenințările de a distruge computere protejate în scopuri de extorcare sau fraudă, A se vedea 18 U.S.C. § 1030. Orice persoană, indiferent de naționalitate, care suferă daune sau pierderi ca urmare a unei încălcări a acestui drept poate să îl acționeze în justiție pe vinovat (inclusiv un funcționar guvernamental) pentru despăgubiri și acțiuni în încetare sau alte măsuri corective în conformitate cu articolul 1030 litera (g), indiferent dacă s-a început urmărirea penală, dacă fapta implică cel puțin una dintre circumstanțele prevăzute în lege. Legea privind confidențialitatea comunicațiilor electronice (Electronic Communications Privacy Act – ECPA) reglementează accesul administrației publice la comunicații electronice stocate și înregistrări ale tranzacțiilor și informații privind abonații deținute de furnizori terți de servicii de comunicații, A se vedea 18 U.S.C. §§ 2701-2712. ECPA autorizează persoana vătămată să introducă o acțiune în justiție împotriva funcționarilor guvernamentali, pentru accesul ilegal intenționat la datele stocate. ECPA se aplică tuturor persoanelor, indiferent de cetățenie și persoanele vătămate pot primi despăgubiri și plata onorariilor avocaților. Legea privind dreptul la confidențialitate financiară (Right to Financial Privacy Act – RFPA) limitează accesul guvernului SUA la datele bancare și la registrele de brokeraj ale clienților individuali, A se vedea 12 U.S.C. §§ 3401-3422. În temeiul cadrului RFPA, o bancă sau clientul unei firme de brokeraj poate intenta o acțiune în justiție împotriva guvernului SUA, pentru daunele legale, efective și punitive pentru obținerea pe nedrept a accesului la evidențele clientului, iar constatarea faptului că un astfel de acces ilicit a fost intenționat declanșează în mod automat o anchetă privind eventuale măsuri disciplinare împotriva funcționarilor publici în cauză, A se vedea 12 U.S.C. § 3417.

În cele din urmă, Legea privind liberul acces la informații (Freedom of Information Act – F OIA) oferă un instrument oricărei persoane pentru a solicita accesul la înregistrările agențiilor federale, pe orice temă, sub rezerva anumitor categorii de excepții, A se vedea 5 U.S.C. § 552(b). Acestea includ limitări privind accesul la informații privind securitatea națională, informațiile cu caracter personal ale altor persoane, precum și informații privind anchetele în scopul aplicării legii și pot fi comparate cu limitele impuse de țările prin propriile legi privind accesul la informații. Aceste restricții se aplică în egală măsură americanilor și persoanelor cu o altă cetățenie. Litigiile privind eliberarea documentelor solicitate în temeiul FOIA, pot face obiectul unui recurs administrativ și apoi la un tribunal federal. Instanța este obligată să pronunțe o nouă hotărâre cu privire la faptul refuzul accesului la arhive este întemeiat, 5 U.S.C. § 552(a)(4)(B), și poate obliga guvernul să asigure accesul la arhive. În unele cazuri, instanțele au respins afirmațiile guvernului conform cărora ar trebui să se refuze accesul la informații ca fiind clasificate ([1]). Deși nu sunt disponibile despăgubiri financiare, instanțele pot acorda plata onorariilor avocaților.

VI. CONCLUZIE

Statele Unite recunosc că activitățile de colectare de informații pe baza semnalelor electromagnetice și alte activități de spionaj trebuie să ia în considerare faptul că toate persoanele ar trebui să fie tratate cu demnitate și respect, indiferent de naționalitate sau de locul de reședință, și că toate persoanele au așteptări legitime de confidențialitate în tratarea informațiilor cu caracter personal ale acestora. Statele Unite utilizează informații obținute pe baza semnalelor electromagnetice doar pentru a-și promova interesele de politică externă și de securitate națională și pentru a proteja de pericole proprii cetățeni, precum și cetățenii aliaților și partenerilor săi. Pe scurt, serviciile de informații nu sunt implicate în activități de supraveghere arbitrară a niciunei persoane, inclusiv cetățenii europeni obișnuiți. Colectarea de informații are loc doar atunci când aceasta este autorizată în mod corespunzător și într-un mod care respectă cu strictețe aceste limite; numai după analizarea disponibilității unor surse alternative, inclusiv din surse publice și diplomatice; și într-un mod în care se

([1]) A se vedea, de exemplu, New York Times/Departamentul Justiției, 756 F.3d 100 (2d Cir. 2014); Uniunea Americană pentru Libertăți Civile/CIA, 710 F.3d 422 (D.C. Cir. 2014).

acordă prioritate unor alternative adecvate și fezabile. Ori de câte ori este posibil, activitățile de colectare de informații pe baza semnalelor electromagnetice se desfășoară doar prin colectarea direcționată de informații externe de la ținte specifice sau pe teme specifice prin utilizarea unor elemente de discriminare.

Politica SUA în această privință a fost afirmată în PPD-28. În acest cadru, agențiile de informații americane nu au competența juridică, resursele, capacitatea tehnică sau dorința de a intercepta toate comunicațiile din lume. Aceste agenții nu citesc e-mail-urile tuturor persoanelor din Statele Unite sau din lume. În conformitate cu PPD-28, Statele Unite prevăd măsuri solide de protecție a informațiilor cu caracter personal ale persoanelor care nu sunt cetățeni americani care sunt colectate prin activitățile de colectare de informații pe baza semnalelor electromagnetice. În cea mai mare măsură posibilă în conformitate cu securitatea națională, aceasta include politici și proceduri pentru reducerea la minimum a păstrării și difuzării informațiilor cu caracter personal referitoare la persoane care nu sunt cetățeni americani, comparabile cu măsurile de protecție de care beneficiază cetățenii americani. În plus, astfel cum s-a arătat mai sus, primul regim de supraveghere cuprinzător al mecanismului prevăzut în secțiunea 702 din FISA este fără precedent. În sfârșit, modificările substanțiale ale legislației americane în domeniul informațiilor prevăzute în USA FREEDOM Act și inițiativele conduse de ODNI de promovare a transparenței în cadrul serviciilor de informații sporesc în mod considerabil protecția vieții private și a libertăților civile ale tuturor persoanelor fizice, indiferent de cetățenie.

Cu stimă,

Robert S. Litt

21 iunie 2016

Dl Justin S. Antonipillai
Consilier
Departamentul Comerțului al SUA
1401 Constitution Avenue, N.W.
Washington, DC 20230

Dl Ted Dean
Secretar adjunct
Administrația Comerțului Internațional
1401 Constitution Avenue, N.W.
Washington, DC 20230

Stimate domnule Antonipillai, Stimate domnule Dean,

Vă adresez această scrisoare pentru a oferi detalii suplimentare despre modul în care Statele Unite efectuează colectarea în masă a informațiilor secrete prin interceptarea de semnale. Astfel cum se explică la nota de subsol 5 din Directiva prezidențială nr. 28 (PPD28), colectarea „în masă" se referă la achiziționarea unui volum relativ important de informații secrete obținute prin interceptarea de semnale sau a unui volum de date în condiții în care serviciile de informații nu pot utiliza un identificator asociat unei ținte specifice (precum adresa de e-mail sau numărul de telefon al țintei) pentru a orienta colectarea. Cu toate acestea, acest lucru nu înseamnă că acest tip de colectare are loc „în masă" sau „într-un mod nediferențiat". Într-adevăr, PPD-28 prevede, de asemenea, că „[a]ctivitățile de colectare de informații secrete prin interceptarea de semnale sunt adaptate la nevoi în cea mai mare măsură posibilă". În cadrul acestui mandat, comunitatea serviciilor de informații ia măsuri pentru a se asigura că, inclusiv în cazul în care nu putem folosi identificatori specifici pentru a direcționa colectarea, datele care trebuie colectate ar putea conține informații secrete externe care vor răspunde cerințelor formulate de responsabilii politici din Statele Unite ale Americii în temeiul procedurii explicate în scrisoarea mea anterioară, și reduce la minimum cantitatea de informații irelevante colectate.

De exemplu, comunității serviciilor de informații i se poate cere să obțină informații secrete prin interceptarea de semnale cu privire la activitățile unui grup terorist care operează într-o regiune a unei țări din Orientul Mijlociu, despre care se presupune că plănuiește atacuri împotriva țărilor din Europa de Vest, fără a cunoaște însă numele, numerele de telefon, adresele de e-mail sau alte date de identificare ale persoanelor asociate cu acest grup terorist. Am avea posibilitatea de a viza acest grup prin colectarea comunicațiilor către și din această regiune, pentru a le verifica și a le analiza ulterior, în vederea detectării comunicațiilor care au legătură cu acest grup. Acționând astfel, comunitatea serviciilor de informații ar încerca să restrângă colectarea cât mai mult posibil. Această activitate ar fi considerată drept colectare „în masă", deoarece nu pot fi utilizate elemente de discriminare, dar nu este nici „în masă", nici „nediferențiată"; dimpotrivă, colectarea ar fi orientată cât mai exact posibil.

Astfel, chiar și în cazul în care nu este posibilă direcționarea prin utilizarea de selectoare specifice, Statele Unite nu colectează toate comunicațiile care provin din toate echipamentele de comunicații din întreaga lume, ci aplică filtre și alte instrumente tehnice pentru a-și concentra activitatea de colectare asupra instalațiilor care sunt susceptibile să conțină comunicații de informații secrete externe valoroase. În acest mod, activitățile de colectare de informații secrete prin interceptarea de semnale desfășurate de Statele Unite ating numai o proporție scăzută a comunicațiilor care tranzitează internetul.

Mai mult, după cum am menționat în scrisoarea mea anterioară, deoarece colectarea „în masă" presupune un risc mai mare de colectare a unor comunicații irelevante, PPD-28 limitează la șase obiective specifice modul în care comunitatea serviciilor de informații poate utiliza colectarea în masă de informații secrete prin interceptarea de semnale. PPD-28 și politicile agențiilor care pun în aplicare această directivă impun, de asemenea, restricții privind păstrarea și difuzarea informațiilor cu caracter personal obținute prin intermediul informațiilor secrete colectate prin interceptarea de semnale, indiferent dacă informațiile au fost colectate în masă sau cu o țintă precisă și indiferent de naționalitatea persoanei.

Astfel, colectarea „în vrac" de comunitatea serviciilor de informații nu este efectuată „în masă" sau „în mod nediferențiat", ci presupune aplicarea de metode și de instrumente de filtrare a colectării, pentru a o direcționa către materiale care vor răspunde cerințelor formulate de factorii de decizie politică în materie de informații secrete externe, reducând totodată la

minimum colectarea de informații nepertinente, și prevede norme stricte pentru a proteja informațiile nepertinente care ar putea fi obținute. Politicile și procedurile descrise în prezenta scrisoare se aplică tuturor activităților de colectare de informații secrete în masă prin interceptarea de semnale, inclusiv oricărei colectări în masă de comunicații către și dinspre Europa, fără să confirme sau să infirme realitatea unei astfel de colectări.

Ați solicitat, de asemenea, mai multe informații cu privire la Consiliul de supraveghere a vieții private și a libertăților civile (Privacy and Civil Liberties Oversight Board – PCLOB) și la inspectorii generali, precum și cu privire la competențele lor. PCLOB este o agenție independentă din cadrul executivului american. Cei cinci membri ai consiliului provin din cele două mari partide americane și sunt numiți de Președinte, fiind confirmați de Senat ([1]). Fiecare membru al consiliului are un mandat de șase ani. Membrii consiliului și personalul său dispun de autorizări de securitate corespunzătoare pentru a-și îndeplini pe deplin obligațiile și responsabilitățile statutare ([2]).

PCLOB are misiunea de a se asigura că eforturile depuse de guvernul federal pentru prevenirea terorismului sunt contrabalansate de necesitatea de a proteja viața privată și libertățile civile. Consiliul are două responsabilități fundamentale: supravegherea și consilierea. PCLOB își stabilește propriul program de lucru și determină ce activități de consiliere sau de supraveghere dorește să întreprindă.

În cadrul rolului său de *supraveghere*, PCLOB verifică și analizează acțiunile întreprinse de puterea executivă pentru a proteja națiunea împotriva terorismului, asigurându-se că necesitatea unei astfel de acțiuni este contrabalansată de necesitatea protejării vieții private și a libertăților civile ([3]). Cea mai recentă reexaminare finalizată de PCLOB în acest domeniu s-a axat pe programele de supraveghere desfășurate în temeiul secțiunii 702 din FISA ([4]). În prezent PCLOB desfășoară o reexaminare a activităților serviciilor de informații desfășurate în temeiul Ordinului executiv 12333 ([5]).

În cadrul rolului său *consultativ*, PCLOB se asigură că preocupările legate de libertate sunt luate în considerare în mod corespunzător cu ocazia elaborării și a punerii în aplicare a legilor, reglementărilor și politicilor legate de eforturile de a apăra națiunea împotriva terorismului ([6]).

Pentru îndeplinirea misiunii sale, consiliul este autorizat prin lege să aibă acces la toate înregistrările, rapoartele, auditurile, analizele, documentele, dosarele, recomandările și orice alte materiale pertinente ale agențiilor relevante, inclusiv la informații clasificate în conformitate cu legea ([7]). În plus, consiliul poate interoga, lua declarații sau mărturii publice de la orice responabil sau angajat al puterii executive ([8]). De asemenea, consiliul poate solicita în scris ca Procurorul General să emită, în numele consiliului, citații care să oblige părțile care nu aparțin puterii executive să furnizeze informații relevante ([9]).

În fine, PCLOB este supus unor obligații statutare de transparență publică. Este vorba, printre altele, de informarea cetățenilor cu privire la activitățile sale prin organizarea de audieri publice și prin punerea rapoartelor sale la dispoziția publicului, în cea mai mare măsură posibilă, în conformitate cu protecția informațiilor clasificate ([10]). În plus, PCLOB trebuie să prezinte un raport atunci când o agenție din cadrul executivului refuză să urmeze avizul său.

Inspectorii generale (IG) din cadrul comunității serviciilor de informații (IC) efectuează audituri, inspecții și reexaminări ale programelor și activităților IC pentru a identifica și a trata riscurile sistemice, vulnerabilitățile și deficiențele. În plus, IG investighează plângerile sau informațiile cu privire la acuzațiile de încălcare a legislației, normelor sau reglementărilor

([1]) 42 U.S.C. 2000ee(a), (h).
([2]) 42 U.S.C. 2000ee(k).
([3]) 42 U.S.C. 2000ee(d)(2).
([4]) A se vedea, în general, https://www.pclob.gov/library.html#oversightreports.
([5]) A se vedea, în general https://www.pclob.gov/events/2015/may13.html.
([6]) 42 U.S.C. 2000ee(d)(1); a se vedea, de asemenea, PCLOB Advisory Function Policy and Procedure, Policy 2015-004, disponibil la adresa https://www.pclob.gov/library/Policy-Advisory_Function_Policy_Procedure.pdf.
([7]) 42 U.S.C. 2000ee(g)(1)(A).
([8]) 42 U.S.C. 2000ee(g)(1)(B).
([9]) 42 U.S.C. 2000ee(g)(1)(D).
([10]) 42 U.S.C. 2000eee(f).

ori cu privire la gestiunea defectuoasă; risipa masivă de fonduri; abuzul de autoritate sau cu privire la un pericol important și specific pentru sănătatea și siguranța publică în programele și activitățile IC. Independența IG este o componentă esențială pentru obiectivitatea și integritatea fiecăruia dintre rapoartele, constatările și recomandările emise de IG. Unele dintre cele mai importante componente pentru menținerea independenței IG includ numirea și revocarea acestora; separarea competențelor operaționale, bugetare și în materie de personal; și cerințele de raportare dublă către directorii agențiilor din cadrul puterii executive și către Congres.

Congresul a înființat câte un birou IG independent în fiecare agenție din cadrul executivului, inclusiv în fiecare element al IC ([1]). Odată cu adoptarea Legii privind autorizarea serviciilor de informații pentru exercițiul fiscal 2015 (*Intelligence Authorization Act for Fiscal Year 2015*), aproape toți IG care supraveghează un element al IC, inclusiv Ministerul Justiției, Agenția Centrală de Informații, Agenția Națională de Securitate și comunitatea serviciilor de informații, sunt numiți de Președinte și confirmați de Senat ([2]). În plus, acești funcționari IG dispun de posturi permanente, nu aparțin niciunui partid și nu pot fi revocați decât de către Președinte. Deși Constituția SUA prevede că Președintele are puterea de a revoca IG, aceasta a fost rareori exercitată, iar Președintele trebuie să ofere Congresului o justificare scrisă cu 30 de zile înaintea revocării unui IG ([3]). Acest proces de numire a IG asigură faptul că nu există influențe nejustificate din partea funcționarilor puterii executive în selecția, numirea sau revocarea unui IG..

În al doilea rând, IG dispun de importante competențe statutare pentru a efectua audituri, investigații și analize ale programelor și operațiunilor ramurii executive. În plus față de investigațiile și reexaminările de supraveghere prevăzute prin lege, IG dispun de o largă marjă de apreciere pentru a își exercita competențele de supraveghere, putând alege programele și activitățile pe care doresc să le reexamineze ([4]). În exercitarea acestei competențe, legea asigură faptul că IG dispun de resursele independente necesare pentru a-și îndeplini responsabilitățile, inclusiv de competența de a-și angaja personalul propriu și de a-și motiva separat solicitările bugetare adresate Congresului ([5]). Legea garantează că IG au acces la informațiile necesare pentru a-și îndeplini responsabilitățile. IG sunt autorizați, printre altele, să aibă acces direct la toate înregistrările și informațiile agențiilor care descriu în detaliu programele și operațiunile agenției, independent de clasificare; să emite citații pentru a obține informații și documente; și să obțină declarații sub jurământ ([6]). Într-un număr limitat de cazuri, șeful unei agenții executive poate interzice o activitate a IG dacă, de exemplu, un audit sau o investigație a IG ar avea importante consecințe negative asupra intereselor de securitate națională ale Statelor Unite. Și în acest caz, exercitarea acestei competențe este foarte neobișnuită și prevede că șeful agenției are obligația să informeze Congresul în termen de 30 de zile în legătură cu motivele de exercitare a competenței respective. ([7]) Astfel, directorul serviciilor naționale de informații nu a exercitat niciodată această competență limitativă asupra niciunei activități a IG.

În al treilea rând, IG au responsabilități legate de informarea completă și constantă a șefilor de agenții din cadrul executivului și a Congresului prin rapoarte privind fraudele și alte probleme, abuzuri, precum și deficiențe grave în ceea ce privește programele și activitățile puterii executive ([8]). Obligația de dublă raportare consolidează independența IG prin asigurarea transparenței cu privire la procesul de supraveghere exercitat de IG și permite șefilor de agenții să aibă ocazia de a pune în aplicare recomandările IG înaintea oricărei acțiuni legislative inițiate de către Congres. De exemplu, IG sunt obligați prin lege să finalizeze rapoarte semestriale care descriu astfel de probleme, precum și acțiunilor corective întreprinse până la acea dată ([9]). Agențiile din cadrul executivului iau în serios constatările și recomandările

([1]) Secțiunile 2 și 4 din Legea privind inspectorii generali din 1978, astfel cum a fost modificată (denumită în continuare „IG Act"); secțiunea 103H literele (b) și (e) din Legea privind securitatea națională din 1947, cu modificările ulterioare (denumită în continuare „Nat'l Sec. Act"); Secțiunea 17 litera (a) din Legea privind Agenția Centrală de Informații (denumită în continuare „CIA Act").

([2]) A se vedea Pub. L. No. 113-293, 128 Stat. 3990, (19 dec. 2014). Doar IG pentru Agenția de Informații de Apărare (*Defense Intelligence Agency*) și pentru Agenția Națională de Informații Geospațiale (*National Geospatial-Intelligence Agency*) nu sunt numiți de Președinte; cu toate acestea, IG din cadrul Ministerului Apărării și al IC au competențe concurente asupra acestor agenții.

([3]) Secțiunea 3 din „IG Act" din 1978, astfel cum a fost modificată; Secțiunea 103H(c) din „Nat'l Sec. Act"; și secțiunea 17 litera (b) din „CIA Act".

([4]) A se vedea secțiunile 4(a) și 6(a) (2) din „IG Act" din 1947; Secțiunea 103H(e) și (g)(2)(A) din „Nat'l Sec. Act"; Secțiunea 17(a) și (c) din „CIA Act".

([5]) Secțiunile 3(d), 6(a)(7) și 6(f) din „IG Act"; Secțiunile 103H(d), (i), (j) și (m) din „Nat'l Sec. Act"; Secțiunile 17(e)(7) și (f) „CIA Act".

([6]) Secțiunea 6(a)(1), (3), (4), (5) și (6) din „IG Act"; Secțiunile 103H(g)(2) din „Nat'l Sec. Act"; Secțiunea 17(e)(1), (2), (4) și (5) din „CIA Act".

([7]) A se vedea, de exemplu secțiunile 8(b) și 8E(a) din „IG Act"; Secțiunea 103H(f) din „Nat'l Sec. Act"; și secțiunea 17 (b) din „CIA Act".

([8]) Secțiunea 4(a)(5) din „IG Act"; Secțiunea 103H literele (a), (b) (3) și (4) din „Nat'l Sec. Act"; Secțiunea 17(a)(2) și (4) din „CIA Act".

([9]) Secțiunea 2(3), 4(a) și 5 din „IG Act"; Secțiunea 103H(k) din „Nat'l Sec. Act"; secțiunea 17(d) din „CIA Act". Inspectorul general al Departamentului de Justiție pune la dispoziție rapoartele destinate publicului pe internet la adresa http://oig.justice.gov/reports/all.htm. De asemenea, inspectorul general pentru comunitatea serviciilor de informații își publică rapoartele semestriale la adresa https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig.

formulate de IG și reușesc adesea să indice faptul că au acceptat și au pus în aplicare recomandările formulate de IG în rapoartele semestriale susmenționate, precum și în alte rapoarte transmise Congresului, și, în unele cazuri, publicului ([1]). În plus față de această structură de raportare pe linie dublă, IG sunt, de asemenea, responsabili pentru direcționarea denunțătorilor din cadrul puterii executive către comisiile de supraveghere competente din cadrul Congresului, pentru a divulga informații privind presupuse fraude, risipe sau abuzuri care ar fi avut loc în cadrul programelor și activităților executivului. Identitatea persoanelor care transmit astfel de semnalări nu este dezvăluită puterii executive, ceea ce protejează denunțătorii față de eventuale măsuri de represalii interzise, de ordin profesional sau vizând autorizarea de securitate, luate ca urmare a faptului că au comunicat informațiile respective către IG ([2]). Dat fiind că denunțătorii constituie adesea sursa aflată la originea investigațiilor întreprinse de IG, posibilitatea de a-și comunica preocupările direct către Congres, fără influențe din partea puterii executive, sporește eficacitatea supravegherii exercitate de IG. Din cauza acestei independențe, IGS poate promova economia, eficiența și responsabilitatea în agențiile executive, cu obiectivitate și integritate.

În fine, Congresul a instituit Consiliul pentru integritate și eficiență al inspectorilor generali. Acest consiliu, printre altele, elaborează standarde IG pentru audituri, investigații și analize; promovează formarea profesională; și are autoritatea de a analiza acuzațiile de abateri grave ale IG, supunând astfel spiritului critic acești funcționari care, prin atribuțiile exercitate, îi supraveghează pe toți ceilalți. ([3])

Sper ca aceste informații să vă fie utile.

Cu stimă,
Robert S. Litt
Consilier general

([1]) Secțiunea 2(3), 4(a) și 5 din „IG Act"; Secțiunea 103H(k) din „Nat'l Sec. Act"; secțiunea 17(d) din „CIA Act". Inspectorul general al Departamentului de Justiție pune la dispoziție rapoartele destinate publicului pe internet la adresa http://oig.justice.gov/reports/all.htm. De asemenea, inspectorul general pentru comunitatea serviciilor de informații își publică rapoartele semestriale la adresa https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig.

([2]) Secțiunea 7 din „IG Act"; Secțiunea 103H(g)(3) din „Nat'l Sec. Act"; Secțiunea 17(e)(3) din „IG Act";

([3]) Secțiunea 11 din „IG Act"

ANEXA VII

Scrisoarea procurorului general adjunct și consilier pentru afaceri internaționale, Bruce Swartz, Departamentul de Justiție al SUA

19 februarie 2016

Dl Justin S. Antonipillai
Consilier
Departamentul Comerțului al SUA
1401 Constitution Ave., NW
Washington, DC 20230

Dl Ted Dean
Secretar adjunct
Administrația Comerțului Internațional
1401 Constitution Ave., NW
Washington, DC 20230

Stimate domnule Antonipillai, Stimate domnule Dean,

Prezenta scrisoare cuprinde o scurtă descriere a principalelor instrumente de anchetă utilizate pentru obținerea de date comerciale și alte informații din registrul societăților în Statele Unite pentru aplicarea legii penale sau în interes public (civil și de reglementare), inclusiv limitări privind accesul prevăzute în aceste mecanisme ([1]). Aceste procese juridice sunt nediscriminatorii în aceea că sunt utilizate pentru a obține informații de la companii din Statele Unite, inclusiv din companii care vor să se autocertifice prin Scutul de confidențialitate SUA/UE, fără a ține cont de cetățenia persoanei vizate. În plus, companiile care beneficiază de calitate procesuală în Statele Unite pot introduce o acțiune în instanță, astfel cum este descris mai jos ([2]).

De remarcat cu privire la confiscarea datelor de către autoritățile publice este al patrulea amendament la Constituția Statelor Unite, care prevede că „[n]u se va încălca dreptul cetățenilor de a fi siguri în ceea ce privește persoanele, locuințele, documentele și efectele, împotriva perchezițiilor și sechestrelor nerezonabile, și nu se vor emite mandate fără un motiv întemeiat, susținut de jurământ sau declarație solemnă, care include în special descrierea spațiului care urmează să fie percheziționat, persoanele care urmează să fie arestate sau obiectele care urmează să fie confiscate" (Constituția Statelor Unite, al patrulea amendament). Astfel cum a afirmat Curtea Supremă a Statelor Unite ale Americii în hotărârea Berger/Statul New York, „[s]copul de bază al acestei modificări, astfel cum este recunoscut în numeroase hotărâri ale Curții, urmărește să protejeze viața privată și securitatea persoanelor împotriva invaziei arbitrare din partea funcționarilor guvernamentali", a se vedea 388 U.S. 41, 53 (1967) [citând Camara/Tribunalul Municipal din San Francisco, 387 U.S. 523, 528 (1967)]. În anchetele penale interne, al patrulea amendament impune, în general, ofițerilor responsabili cu aplicarea legii să obțină un mandat judecătoresc înainte de a efectua o percheziție, A se vedea Katz/ Statele Unite, 389 U.S. 347, 357 (1967). Atunci când cerința mandatului nu se aplică, activitatea autorității publice este supusă unui test de „rezonabilitate" în temeiul celui de al patrulea amendament. Prin urmare, Constituția garantează faptul că guvernul SUA nu are putere nelimitată sau arbitrară de a reține informațiile cu caracter privat.

Autoritățile de aplicare a legii penale:

Procurorii federali, care sunt funcționari ai Departamentului de Justiție (DOJ) și agenți federali, inclusiv agenții federali din cadrul Biroului Federal de Investigații (FBI), agenție de aplicare a legii din cadrul Departamentului de Justiție, sunt în

([1]) Această prezentare generală nu descrie instrumentele de anchetă privind securitatea națională de către autoritățile de aplicare a legii în investigații privind terorismul și alte investigații de securitate națională, inclusiv scrisorile privind securitatea națională (National Security Letters – NSL) pentru anumite informații din rapoartele de credit, evidențele contabile și documentele electronice ale abonaților și istoricul tranzacțiilor, a se vedea 12 U.S.C. § 3414; 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 18 U.S.C. § 2709, și pentru măsurile de supraveghere electronică, mandatele de percheziție, evidențele întreprinderii și alte seturi de comunicări în conformitate cu Legea privind supravegherea activităților străine de spionaj, a se vedea 50 U.S.C. § 1801 *et seq*.

([2]) Acest document discută aplicarea legii federale și autoritățile de reglementare; încălcările statului de drept sunt investigate de către state și sunt judecate în instanțele de stat. Autoritățile de aplicare a legii utilizează mandatele și citațiile emise conform legislației statului, în esență, în același mod cum este descris în prezentul document, dar cu posibilitatea ca procesul juridic de stat să poată face obiectul unor măsuri de protecție prevăzute de constituțiile statelor care le depășesc pe cele din Constituția Statelor Unite ale Americii. Măsurile de protecție din legislația statului trebuie să fie cel puțin egale cu cele din Constituția SUA, inclusiv, dar fără a se limita la, al patrulea amendament.

măsură să impună companiilor din Statele Unite să prezinte documente și alte informații pentru scopuri de cercetare penală prin mai multe tipuri de procese juridice obligatorii, inclusiv citații emise de marele juriu, citații administrative și mandate de percheziție și pot obține alte comunicări în baza mecanismelor de interceptare a convorbirilor (Pen Register).

Citațiile pentru a apărea în fața marelui juriu sau la proces: Citațiile sunt utilizate pentru a sprijini anchetele direcționate ale autorităților de aplicare a legii. O citație pentru a apărea în fața marelui juriu este emisă de un mare juriu (de regulă, la cererea unui procuror federal), pentru a sprijini o anchetă a marelui juriu în cazul unei anumite presupuse încălcări a dreptului penal. Marile jurii reprezintă ramura de anchetare a Curții și sunt convocate de un judecător sau magistrat. O citație poate impune unei persoane să depună mărturie într-o procedură sau să producă sau să pună la dispoziție documente comerciale, informații stocate electronic sau alte elemente tangibile. Informațiile trebuie să fie relevante pentru investigație și citația nu poate fi nerezonabilă, pentru că este amplă sau pentru că este abuzivă sau împovărătoare. Persoana citată poate depune o propunere de a contesta o citație întemeiată pe baza acestor motive. A se vedea Fed. R. Crim. p. 17. În anumite circumstanțe, citațiile de documente pot fi utilizate după punerea sub acuzare de către marele juriu.

Competența administrativă de citare: Competențele administrative de citare pot fi exercitate în anchete penale sau civile. În contextul aplicării dreptului penal, mai multe legi federale autorizează utilizarea unor citații administrative pentru a produce sau a pune la dispoziție documente comerciale, informații stocate electronic sau alte elemente tangibile în investigații care implică frauda serviciilor de sănătate, abuzuri împotriva copiilor, protecția Serviciului Secret, cazuri de substanțe controlate și anchete ale inspectorului general care implică agențiile guvernamentale. În cazul în care autoritatea publică dorește să aplice o citație administrativă în instanță, destinatarul citației administrative, la fel ca destinatarul unei citații emise de marele juriu poate susține că aceasta este inadmisibilă deoarece este excesiv de cuprinzătoare sau pentru că este abuzivă sau împovărătoare.

Hotărârile judecătorești pentru interceptare (Pen Register) și capturare și trasabilitate (Trap and Traces): În temeiul dispozițiilor privind interceptarea (Pen Register) și capturarea și trasabilitatea (Trap and Traces), autoritățile de aplicare a legii pot obține un ordin judecătoresc pentru a obține informații în timp real, apelurile fără conținut, routing, adresare și semnalarea despre un număr de telefon sau o adresă de e-mail la certificarea faptului că informațiile furnizate sunt relevante pentru o anchetă penală în curs, A se vedea 18 U.S.C. §§ 3121-3127. Utilizarea sau instalarea unui astfel de dispozitiv în afara legii federale este o infracțiune la nivel federal.

Legea privind confidențialitatea comunicațiilor electronice (Electronic Communications Privacy Act – ECPA): Norme suplimentare reglementează accesul guvernului la informațiile privind abonații, traficul și conținutul stocat al comunicațiilor deținute de furnizorii de servicii de internet deținute, companii de telefonie sau alți furnizori de servicii terți, în temeiul titlului II din ECPA, denumită și Legea comunicațiilor stocate (Stored Communications Act – SCA), 18 U.S.C. §§ 2701–2712. SCA stabilește un sistem de drepturi legale la viață privată care limitează accesul autorităților de aplicare a legii la date dincolo de ceea ce este necesar în temeiul dreptului constituțional de la clienți și abonați ai furnizorilor de servicii de internet. SCA prevede creșterea nivelului de protecție a vieții private în funcție de caracterul intruziv al colectării. Pentru informațiile de înregistrare ale abonaților, adresele IP și elementele temporale asociate, precum și informațiile privind facturarea, autoritățile de aplicare a legii trebuie să obțină o citație. Pentru majoritatea celorlalte informații fără conținut stocate, cum ar fi e-mail fără subiect, autoritățile de aplicare a legii trebuie să prezinte unui judecător faptele specifice care să demonstreze că informațiile solicitate sunt relevante și semnificative pentru o anchetă penală în curs. Pentru a obține conținutul comunicațiilor electronice stocate, în general, autoritățile de aplicare a legii obțin un mandat de la un judecător pe baza unui motiv întemeiat de a crede că acel cont conține dovezi ale unei infracțiuni. SCA prevede, de asemenea, răspunderea civilă și sancțiuni penale.

Hotărârile judecătorești de supraveghere în temeiul legii federale privind interceptarea convorbirilor: În plus, autoritățile de aplicare a legii pot intercepta în timp real comunicații orale sau electronice pentru scopuri de cercetare penală în temeiul legii federale de interceptare a convorbirilor, A se vedea 18 U.S.C. §§ 2510-2522. Această competență este disponibilă numai în temeiul unei hotărâri judecătorești, prin care un judecător constată, printre altele, că există un

motiv întemeiat să se creadă că interceptarea convorbirilor sau interceptarea electronică va face dovada unei infracțiuni federale sau va dezvălui locul în care se află un fugar care se sustrage de la urmărirea penală. Legea prevede răspunderea civilă și sancțiuni penale pentru încălcările dispozițiilor privind interceptarea.

Mandatul de percheziție – Norma 41: Autoritățile de aplicarea legii pot să percheziționeze fizic spații din Statele Unite în cazul în care sunt autorizate în acest sens de către un judecător. Autoritățile de aplicare a legii trebuie să demonstreze judecătorului, pe baza unui motiv întemeiat, că o infracțiune a fost comisă sau este pe cale de a fi comisă și că aspectele legate de infracțiune sunt susceptibile de a fi găsite în locul specificat pe mandat. Această competență este adesea folosită atunci când este necesară efectuarea unei percheziții fizice a unui spațiu de către poliție, având în vedere pericolul ca probele să fie distruse în cazul în care întreprinderii i se trimite o citație sau un alt tip de ordin care solicită producerea de documente. A se vedea Constituția Statelor Unite, al patrulea amendament (discutat în detaliu mai sus), Fed. R. Crim. p. 41. Entitatea care face obiectul unui mandat de percheziție poate acționa în sensul anulării mandatului, ca fiind excesiv de cuprinzător, vexatoriu sau obținut în alt mod necorespunzător și părțile vătămate care au calitate procesuală pot introduce o acțiune pentru a elimina orice probe obținute într-o percheziție ilegală, *A se vedea Mapp/Ohio*, 367 U.S. 643 (1961).

Orientări și politici ale Departamentului de Justiție: Pe lângă aceste norme, limitări constituționale, legale și bazate pe norme privind accesul autorităților publice la date, Procurorul General a emis orientări care introduc limite suplimentare asupra accesului la date al autorităților de aplicare a legii, care includ, de asemenea, măsuri de protecție a vieții private și a libertății civile. De exemplu, Orientările procurorului general pentru operațiunile interne ale Biroului Federal de Investigații (FBI) (septembrie 2008) (denumite în continuare Orientările AG FBI), disponibile la adresa http://www.justice.gov/archive/opa/docs/guidelines.pdf, stabilesc limite privind utilizarea mijloacelor de cercetare pentru a căuta informații cu privire la anchetele care implică infracțiuni federale. Aceste orientări prevăd că FBI utilizează cele mai puțin invazive metode de anchetă fezabile, luând în considerare impactul asupra vieții private și libertăților civile și eventualele daune aduse reputației. De asemenea, acestea iau act de faptul că „este evident faptul că FBI trebuie să își desfășoare anchetele și alte activități în mod legal și rezonabil respectând libertatea și viața privată și să evite intervențiile inutile în viața cetățenilor care respectă legea". A se vedea Orientările FBI ale Procurorului General la 5. FBI a pus în aplicare aceste orientări prin Ghidul FBI privind investigațiile și operațiunile interne (Domestic Investigations and Operations Guide – DIOG), disponibil la adresa https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20(DIOG), un manual cuprinzător care include limite detaliate privind utilizarea unor instrumente de anchetă și orientări pentru a se asigura că libertățile publice și viața privată sunt protejate în fiecare anchetă. Norme suplimentare și politici care impun limitări asupra activităților de investigare ale procurorilor federali sunt stabilite în **Manualul procurorilor americani** (United States Attorneys' Manual – USAM), disponibil, de asemenea, online la adresa http://www.justice.gov/usam/united-states-attorneys-manual.

Autoritățile civile și de reglementare (interesul public):

De asemenea, există limitări semnificative în ceea ce privește accesul civil sau de reglementare (și anume, „interesul public") la datele deținute de companii din Statele Unite. Agențiile cu responsabilități civile și de reglementare pot emite citații companiilor pentru documente comerciale, informații stocate electronic sau alte elemente tangibile. Aceste agenții sunt limitate în ceea ce privește exercitarea competenței administrative sau civile de citație nu numai prin statutele lor, ci și prin reexaminarea judiciară independentă a unor citații emise înainte de punerea în aplicare a unor potențiale decizii judiciare. *A se vedea, de exemplu* Fed. R. Civ. P. 45. Agențiile pot solicita accesul numai la datele care sunt relevante pentru chestiuni care intră în sfera lor de autoritate de reglementare. În plus, destinatarul unei somații administrative poate contesta executarea respectivei somații în instanță prin prezentarea de dovezi conform cărora agenția nu a acționat în conformitate cu standardele de bază privind caracterul rezonabil, astfel cum s-a menționat anterior.

Există alte temeiuri juridice pentru care companiile pot să conteste solicitările de date provenind de la agenții administrative, pe baza propriilor produse și a tipurilor de date pe care le dețin. De exemplu, instituțiile financiare pot contesta citațiile administrative care solicită anumite tipuri de informații ca încălcări ale Legii secretului bancar și ale regulamentelor sale de punere în aplicare, A se vedea 31 U.S.C., § 5318, C.F.R. titlul 31 partea X. Alte întreprinderi pot invoca Fair Credit Reporting Act, a se vedea 15 U.S.C. § 1681b, sau o serie de alte legi sectoriale specifice. Folosirea abuzivă a autorității de somare de către o agenție poate avea ca rezultat răspunderea agenției sau răspunderea personală a funcționarilor agenției, A se vedea, de exemplu, Legea privind dreptul la confidențialitate financiară, 12 U.S.C. §§ 3401–3422. Astfel, instanțele din Statele Unite apără împotriva solicitărilor neadecvate de reglementare și oferă supravegherea independentă a acțiunilor agenției federale.

În cele din urmă, orice competență legală pe care o au autoritățile administrative de a confisca fizic evidențe de la o companie din Statele Unite ale Americii în urma unei percheziții administrative trebuie să îndeplinească cerințele celui de al patrulea amendament, A se vedea See/Orașul Seattle, 387 U.S. 541 (1967).

Concluzie

Toate activitățile de aplicare a legii și de reglementare din Statele Unite ale Americii trebuie să respecte legislația aplicabilă, inclusiv Constituția SUA, legile, normele și reglementările relevante. Aceste activități trebuie să fie în conformitate cu politicile aplicabile, inclusiv orice orientări ale procurorului general care reglementează activitățile de aplicare a legii federale. Cadrul juridic descris mai sus limitează capacitatea agențiilor de reglementare și de aplicare a legii din SUA să obțină informații de la companii din Statele Unite – indiferent dacă informațiile se referă la cetățeni americani sau cetățeni ai unor țări străine – și, în plus, permite reexaminarea judiciară a tuturor solicitărilor de date ale autorităților publice în conformitate cu aceste mecanisme.

Cu stimă,

Bruce C. Swartz

Procuror general adjunct și Consilier pentru afaceri internaționale