DECIZIA DE PUNERE ÎN APLICARE (UE) 2023/1795 A COMISIEI

din 10 iulie 2023

de constatare, în conformitate cu Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului, a nivelului adecvat de protecție a datelor cu caracter personal asigurat de Cadrul UE-SUA privind confidențialitatea datelor

[notificată cu numărul C(2043) 4745]

(Text cu relevanță pentru SEE)

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) ([1]), în special articolul 45 alineatul (3),

întrucât:

1. INTRODUCERE

(1) Regulamentul (UE) 2016/679 ([2]) stabilește normele pentru transferul de date cu caracter personal de la operatori sau persoane împuternicite de operatori din Uniune către țări terțe și organizații internaționale, în măsura în care astfel de transferuri intră în domeniul său de aplicare. Normele privind transferurile internaționale de date sunt prevăzute în capitolul V din regulamentul respectiv. Deși fluxul de date cu caracter personal către și dinspre țări situate în afara Uniunii Europene este esențial pentru dezvoltarea comerțului transfrontalier și a cooperării internaționale, nivelul de protecție conferit datelor cu caracter personal din Uniune nu trebuie să fie subminat de transferurile către țări terțe sau organizații internaționale ([3]).

(2) În temeiul articolului 45 alineatul (3) din Regulamentul (UE) 2016/679, Comisia poate decide, printr-un act de punere în aplicare, că o țară terță, un teritoriu sau unul sau mai multe sectoare specificate dintr-o țară terță asigură un nivel de protecție adecvat. În astfel de condiții, transferurile de date cu caracter personal către o țară terță pot avea loc fără a fi necesar să se obțină autorizări suplimentare, astfel cum se prevede la articolul 45 alineatul (1) și în considerentul 103 din Regulamentul (UE) 2016/679.

(3) În conformitate cu articolul 45 alineatul (2) din Regulamentul (UE) 2016/679, adoptarea unei decizii privind caracterul adecvat al nivelului de protecție trebuie să se bazeze pe o analiză cuprinzătoare a ordinii juridice a țării terțe, în ceea ce privește atât normele aplicabile importatorilor de date, cât și limitările și garanțiile referitoare la accesul autorităților publice la datele cu caracter personal. În evaluarea sa, Comisia trebuie să stabilească dacă țara terță în cauză garantează un nivel de protecție „echivalent în esență” cu cel asigurat în cadrul Uniunii [considerentul 104 din Regulamentul (UE) 2016/679]. Această situație trebuie evaluată în raport cu legislația Uniunii, în special cu Regulamentul (UE) 2016/679, precum și cu jurisprudența Curții de Justiție a Uniunii Europene („Curtea de Justiție”) ([4]).

([1]) JO L 119, 4.5.2016, p. 1.
([2]) Pentru a facilita consultarea, în anexa VIII este inclusă o listă a abrevierilor utilizate în prezenta decizie.
([3]) A se vedea considerentul 101 din Regulamentul (UE) 2016/679.
([4]) A se vedea, cel mai recent, cauza C-311/18, Facebook Ireland și Schrems („Hotărârea Schrems II”), ECLI:EU:C:2020:559.

(4) Astfel cum a clarificat Curtea de Justiție în hotărârea sa din 6 octombrie 2015 în cauza C-362/14, Maximillian Schrems/Data Protection Commissioner ([5]) („Hotărârea Schrems"), acest lucru nu impune constatarea unui nivel de protecție identic. În special, mijloacele la care țara terță în cauză recurge pentru protecția datelor cu caracter personal pot fi diferite de cele puse în aplicare în Uniune, cu condiția ca acestea să se dovedească în practică efective în scopul de a asigura un nivel de protecție adecvat ([6]). Prin urmare, standardul caracterului adecvat nu necesită o reproducere punct cu punct a normelor Uniunii. Mai curând, testul constă în faptul dacă, prin fondul drepturilor la viață privată și punerea în aplicare, supravegherea și exercitarea efectivă a acestora, sistemul străin în cauză, în ansamblul său, oferă nivelul ridicat de protecție necesar ([7]). În plus, potrivit hotărârii respective, atunci când aplică acest standard, Comisia ar trebui să evalueze în special dacă respectivul cadru juridic al țării terțe în cauză prevede norme menite să limiteze ingerințele în drepturile fundamentale ale persoanelor ale căror date sunt transferate din Uniune, ingerințe pe care entități de stat din această țară ar fi autorizate să le practice atunci când urmăresc obiective legitime precum securitatea națională și oferă o protecție juridică eficientă împotriva ingerințelor de această natură ([8]). Criteriile de referință privind caracterul adecvat al nivelului de protecție ale Comitetului european pentru protecția datelor, care urmăresc să ofere clarificări suplimentare cu privire la acest standard, includ, de asemenea, orientări în acest sens ([9]).

(5) Standardul aplicabil în ceea ce privește o astfel de ingerință în drepturile fundamentale la viață privată și la protecția datelor a fost clarificat suplimentar de Curtea de Justiție în hotărârea sa din 16 iulie 2020 în cauza C-311/18, Data Protection Commissioner/Facebook Ireland Limited și Maximillian Schrems („Hotărârea Schrems II"), care a declarat ca fiind nevalidă Decizia de punere în aplicare (UE) 2016/1250 a Comisiei ([10]) privind un cadru transatlantic anterior aferent fluxurilor de date, respectiv Scutul de confidențialitate UE-SUA. Curtea de Justiție a considerat că limitările protecției datelor cu caracter personal care decurg din reglementarea internă a Statelor Unite ale Americii privind accesul și utilizarea de către autoritățile publice americane a unor date transferate din Uniune către Statele Unite în scopuri legate de securitatea națională nu sunt circumscrise astfel încât să îndeplinească cerințe în esență echivalente cu cele prevăzute în dreptul Uniunii în ceea ce privește necesitatea și proporționalitatea acestor ingerințe în dreptul la protecția datelor ([11]). De asemenea, Curtea de Justiție a considerat că nu se furnizează nicio cale de atac în fața unui organ care oferă persoanelor ale căror date sunt transferate către Statele Unite garanții în esență echivalente cu cele prevăzute la articolul 47 din cartă privind dreptul la o cale de atac eficientă ([12]).

(6) În urma pronunțării Hotărârii Schrems II, Comisia a inițiat discuții cu guvernul SUA pentru a se ajunge la o eventuală nouă decizie privind caracterul adecvat al nivelului de protecție care să îndeplinească respectivele cerințe prevăzute la articolul 45 alineatul (2) din Regulamentul (UE) 2016/679, astfel cum au fost interpretate de Curtea de Justiție. Ca urmare a acestor discuții, la 7 octombrie 2022, Statele Unite ale Americii au adoptat Ordinul executiv nr. 14086 – „Enhancing Safeguards for US Signals Intelligence Activities" (Consolidarea garanțiilor pentru activitățile de colectare de informații de tip SIGINT desfășurate de Statele Unite ale Americii) (OE nr. 14086), care este completat de un regulament privind Curtea de Reexaminare a Protecției Datelor (*Data Protection Review Court*), emis de procurorul general al SUA („Regulamentul PG") ([13]). În plus, cadrul care se aplică entităților comerciale care prelucrează date transferate din Uniune în temeiul prezentei decizii – „Cadrul UE-SUA privind confidențialitatea datelor" („CCD UE-SUA" sau „CCD") – a fost actualizat.

(7) Comisia a analizat cu atenție legislația și practica din SUA, inclusiv OE nr. 14086 și Regulamentul PG. Pe baza constatărilor prezentate în considerentele 9-200, Comisia concluzionează că Statele Unite ale Americii asigură un nivel adecvat de protecție a datelor cu caracter personal transferate în temeiul CCD UE-SUA de la un operator sau o persoană împuternicită de operator din Uniune ([14]) către organizații certificate din Statele Unite ale Americii.

([5]) Cauza C-362/14, Maximillian Schrems/Data Protection Commissioner („Hotărârea Schrems"), ECLI:EU:C:2015:650, punctul 73.

([6]) Hotărârea Schrems, punctul 74.

([7]) A se vedea secțiunea 3.1. din Comunicarea Comisiei către Parlamentul European și Consiliu – Schimbul de date cu caracter personal și protecția acestora într-o lume globalizată, COM(2017) 7, 10.1.2017, p. 6.

([8]) Hotărârea Schrems, punctele 88-89.

([9]) Comitetul european pentru protecția datelor, Criterii de referință privind caracterul adecvat al nivelului de protecție, WP 254 rev. 01., disponibile la următoarea adresă: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

([10]) 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 (JO L 207, 1.8.2016, p. 1.)

([11]) Hotărârea Schrems II, punctul 185.

([12]) Hotărârea Schrems II, punctul 197.

([13]) Titlul 28 partea 302 din CFR – Codul regulamentelor federale (*Code of Federal Regulations*).

([14]) 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 care fac parte din SEE, și anume Islanda, Liechtenstein și Norvegia. Decizia Comitetului mixt care încorporează Regulamentul (UE) 2016/679 în anexa XI la Acordul privind SEE a fost adoptată de Comitetul mixt al SEE la 6 iulie 2018 și a intrat în vigoare la 20 iulie 2018. Regulamentul este, prin urmare, reglementat de acordul respectiv. În sensul deciziei, trimiterile la UE și la statele membre ale UE ar trebui, prin urmare, să fie înțelese ca incluzând și statele SEE.

(8) Prezenta decizie are drept efect posibilitatea ca transferurile de date cu caracter personal de la operatorii și persoanele împuternicite de operatori din Uniune ([15]) către organizații certificate din Statele Unite ale Americii să aibă loc fără a fi necesară obținerea unei autorizări suplimentare. Aceasta nu aduce atingere aplicării directe a Regulamentului (UE) 2016/679 pentru astfel de organizații în cazul în care sunt îndeplinite condițiile privind domeniul de aplicare teritorial al regulamentului respectiv, astfel cum se prevede la articolul 3.

2. CADRUL UE-SUA PRIVIND CONFIDENȚIALITATEA DATELOR

2.1 Domeniul de aplicare personal și material

2.1.1 *Organizații certificate*

(9) CCD UE-SUA se bazează pe un sistem de certificare 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 ([16]). Pentru a fi eligibilă pentru certificare în temeiul CCD UE-SUA, o organizație trebuie să facă obiectul competențelor de investigare și de asigurare a respectării legii ale Comisiei Federale pentru Comerț (FTC) (*Federal Trade Commission*) sau ale Departamentului Transporturilor al SUA (DoT) (*Department of Transportation*) ([17]). Principiile se aplică imediat după certificare. Astfel cum se explică mai detaliat în considerentele 48-52, organizațiile CCD UE-SUA trebuie să își recertifice anual adeziunea la aceste principii ([18]).

2.1.2 *Definiția datelor cu caracter personal și conceptele de „operator" și „agent"*

(10) Protecția conferită de CCD UE-SUA se aplică oricăror date cu caracter personal transferate din Uniune către organizații din SUA care și-au certificat adeziunea la principii față de DoC, cu excepția datelor colectate în vederea publicării, a difuzării sau a comunicării publice prin alte forme a materialelor jurnalistice și a informațiilor din materiale publicate anterior și diseminate din arhive mass-media ([19]). Prin urmare, astfel de informații nu pot fi transferate în baza CCD UE-SUA.

(11) Principiile definesc datele cu caracter personal/informațiile cu caracter personal în același mod precum Regulamentul (UE) 2016/679, și anume drept „informații referitoare la o persoană identificată sau identificabilă care intră în domeniul de aplicare al RGPD, primite de o organizație din Statele Unite din Uniunea Europeană și înregistrate sub orice formă" ([20]). În consecință, acestea vizează, de asemenea, datele pseudonimizate (sau „codificate") provenite cercetare (inclusiv în cazul în care codul de acces nu este comunicat organizației destinatare din SUA) ([21]). În mod similar, noțiunea de „prelucrare" este definită ca „orice operațiune sau set de operațiuni care se efectuează asupra datelor cu caracter personal, cu sau fără utilizarea de mijloace automatizate, precum colectarea, înregistrarea, organizarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea sau diseminarea, ștergerea sau distrugerea" ([22]).

(12) CCD UE-SUA se aplică organizațiilor din SUA care se califică drept operatori (și anume o persoană sau o organizație care, singură sau împreună cu alte persoane, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal) ([23]) sau persoane împuternicite de operatori (și anume agenți care acționează în numele unui operator) ([24]). Persoanele împuternicite de operatori din SUA trebuie să fie obligate prin contract să acționeze numai la

([15]) Prezenta decizie nu aduce atingere cerințelor Regulamentului (UE) 2016/679 care se aplică entităților (operatorilor și persoanelor împuternicite de operatori) din Uniune care transferă datele, de exemplu, în ceea ce privește limitarea scopului, reducerea la minimum a datelor, transparența și securitatea datelor [a se vedea, de asemenea, articolul 44 din Regulamentul (UE) 2016/679].

([16]) A se vedea în acest sens punctul 81 din Hotărârea Schrems, în care Curtea de Justiție a confirmat că un sistem de autocertificare poate asigura un nivel de protecție adecvat.

([17]) Anexa I secțiunea I punctul 2. FTC are o competență extinsă asupra activităților comerciale, cu unele excepții, de exemplu în ceea ce privește activitățile bancare, companiile aeriene, activitățile de asigurare și activitățile de transport comune desfășurate de furnizorii de servicii de telecomunicații [deși hotărârea Curții de Apel pentru al Nouălea Circuit din Statele Unite (U.S. Court of Appeals for the Ninth Circuit) din 26 februarie 2018 în cauza FTC/AT&T a confirmat faptul că FTC are competență asupra activităților de transport care nu sunt comune, desfășurate de aceste entități]. A se vedea, de asemenea, anexa IV nota de subsol 2. DOT are competența de a impune respectarea normelor de către companiile aeriene și agenții de bilete (pentru transportul aerian); a se vedea anexa V secțiunea A.

([18]) Anexa I secțiunea III punctul 6.

([19]) Anexa I secțiunea III punctul 2.

([20]) Anexa I secțiunea I punctul 8 litera (a).

([21]) Anexa I secțiunea III punctul 14 litera (g).

([22]) Anexa I secțiunea I punctul 8 litera (b).

([23]) Anexa I secțiunea I punctul 8 litera (c).

([24]) A se vedea, de exemplu, anexa I secțiunea II punctul 2 litera (b), precum și secțiunea II punctul 3 litera (b) și punctul 7 litera (d), care clarifică faptul că agenții acționează în numele unui operator, sub rezerva instrucțiunilor acestuia din urmă și în temeiul unor obligații contractuale specifice.

instrucțiunile operatorului din UE și să îi furnizeze asistență acestuia pentru a le răspunde persoanelor care își exercită drepturile în conformitate cu principiile ([25]). În plus, în cazul subcontractării serviciilor de prelucrare a datelor, o persoană împuternicită de operator trebuie să încheie cu subcontractantul un contract care să asigure același nivel de protecție în conformitate cu principiile și să ia măsuri pentru a asigura punerea în aplicare corespunzătoare a acestuia ([26]).

2.2 **Principiile Cadrului UE-SUA privind confidențialitatea datelor**

2.2.1 ***Limitarea scopului și opțiunea***

(13) Datele cu caracter personal ar trebui prelucrate în mod legal și echitabil. Acestea ar trebui colectate într-un scop anume și utilizate ulterior numai în măsura în care acest lucru nu este incompatibil cu scopul prelucrării.

(14) În temeiul CCD UE-SUA, acest lucru este asigurat prin intermediul unor principii diferite. În primul rând, în temeiul *principiului integrității datelor și al limitării scopului*, la fel ca în temeiul articolului 5 alineatul (1) litera (b) din Regulamentul (UE) 2016/679, o organizație nu poate prelucra date cu caracter personal într-un mod incompatibil cu scopul în care acestea au fost colectate inițial sau cu scopul aprobat ulterior de persoana vizată ([27]).

(15) În al doilea rând, înainte de a utiliza date cu caracter personal într-un scop nou (modificat) care diferă în mod semnificativ de scopul inițial, dar rămâne, totuși, compatibil cu acesta sau de a le divulga unei părți terțe, organizația trebuie să ofere persoanelor vizate posibilitatea de a se opune unei astfel de operațiuni (de a o refuza), în conformitate cu *principiul opțiunii* ([28]), printr-un mecanism clar, vizibil și ușor accesibil. Este important de remarcat că acest principiu nu înlocuiește interdicția explicită privind prelucrarea incompatibilă ([29]).

([25]) Anexa I secțiunea III punctul 10 litera (a). A se vedea, de asemenea, orientările elaborate de DoC, în consultare cu Comitetul european pentru protecția datelor, în temeiul Scutului de confidențialitate, care au clarificat obligațiile persoanelor împuternicite de operatori din SUA care primesc date cu caracter personal din Uniune în temeiul cadrului. Întrucât aceste norme nu s-au schimbat, aceste orientări/FAQ rămân relevante în temeiul CCD UE-SUA (https://www.privacyshield.gov/article?id=Processing-FAQs).

([26]) Anexa I secțiunea II punctul 3 litera (b).

([27]) Anexa I secțiunea II punctul 5 litera (a). Scopurile compatibile pot include activitățile de audit, prevenirea fraudei sau alte scopuri care sunt conforme cu așteptările unei persoane rezonabile, având în vedere contextul în care sunt colectate datele respective (a se vedea nota de subsol 6 din anexa I).

([28]) Anexa I secțiunea II punctul 2 litera (a). Acest lucru nu este valabil în cazul în care o organizație furnizează date cu caracter personal unei persoane împuternicite de operator care acționează în numele său și în conformitate cu instrucțiunile sale [anexa I secțiunea II punctul 2 litera (b)]. Astfel, în acest caz, organizația trebuie să dispună de un contract și să asigure respectarea *principiului responsabilității pentru transferurile ulterioare*, astfel cum este descris în detaliu în considerentul 43. În plus, principiul *opțiunii* (precum și principiul *notificării*) poate fi restricționat atunci când datele cu caracter personal sunt prelucrate în contextul unui proces de diligență (realizat în cadrul unei potențiale fuziuni sau preluări) sau al auditurilor, în măsura în care și atât timp cât este necesar pentru a îndeplini cerințe legale sau de interes public sau în măsura în care și atât timp cât aplicarea acestor principii ar aduce atingere intereselor legitime ale organizației în contextul specific al procesului de diligență sau al auditurilor (anexa I secțiunea III punctul 4). Principiul suplimentar 15 [anexa I secțiunea III punctul 15 literele (a) și (b)] prevede, de asemenea, o excepție de la aplicarea principiului *opțiunii* (precum și de la aplicarea principiilor *notificării* și *responsabilității pentru transferurile ulterioare*) pentru datele cu caracter personal din surse aflate la dispoziția publicului (cu excepția cazului în care exportatorul de date din UE indică faptul că informațiile fac obiectul unor restricții care impun aplicarea principiilor respective) sau pentru datele cu caracter personal colectate din registre care pot fi consultate de publicul larg (atât timp cât acestea nu sunt asociate cu informații care nu au caracter public și sunt respectate toate condițiile de consultare). În mod similar, principiul suplimentar 14 [anexa I secțiunea III punctul 14 litera (f)] prevede o excepție de la aplicarea principiului *opțiunii* (precum și de la aplicarea principiilor *notificării* și *responsabilității pentru transferurile ulterioare*) pentru prelucrarea datelor cu caracter personal de către o societatea farmaceutică sau o societate producătoare de dispozitive medicale pentru activitățile de monitorizare a siguranței și a eficacității produselor, în măsura în care adeziunea la principii contravine respectării cerințelor de reglementare.

([29]) Acest lucru este valabil pentru toate transferurile de date în temeiul CCD UE-SUA, inclusiv în cazul în care acestea vizează date colectate în contextul unui raport de muncă. Astfel, deși o organizație certificată din SUA poate, în principiu, să utilizeze date privind resursele umane în scopuri diferite, care nu au legătură cu un raport de muncă (de exemplu, pentru anumite comunicări cu caracter publicitar), aceasta trebuie să respecte interdicția privind prelucrarea incompatibilă și, în plus, poate face acest lucru numai în conformitate cu principiile *notificării* și *opțiunii*. În mod excepțional, o organizație poate utiliza date cu caracter personal pentru un scop compatibil suplimentar fără a realiza *notificarea* și fără a oferi *posibilitatea exprimării opțiunii*, dar numai în măsura și pe durata necesară pentru a evita afectarea capacității organizației de a lua decizii de promovare, numire sau alte decizii similare privind raporturile de muncă [a se vedea anexa I secțiunea III punctul 9 litera (b) subpunctul (iv)]. Interdicția impusă organizației din SUA privind sancționarea angajatului pentru exercitarea unei astfel de opțiuni, inclusiv orice restrângere a oportunităților profesionale, va oferi asigurarea că, în pofida raportului de subordonare și a dependenței inerente, angajatul nu va fi supus niciunei presiuni și poate exercita, astfel, o veritabilă libertate de alegere. A se vedea anexa I secțiunea III punctul 9 litera (b) subpunctul (i).

2.2.2 ***Prelucrarea de categorii speciale de date cu caracter personal***

(16) În cazul în care sunt prelucrate „categorii speciale” de date, ar trebui să existe garanții specifice.

(17) În conformitate cu *principiul opțiunii*, se aplică garanții specifice prelucrării „informațiilor sensibile”, și anume a datelor privind dosarul medical sau starea de sănătate a unei persoane, originea rasială sau etnică, opiniile politice, credințele religioase sau convingerile filosofice, apartenența sindicală, viața sexuală a persoanei respective sau a oricăror alte informații primite de la o parte terță care sunt identificate și tratate de partea respectivă ca fiind sensibile ([30]). Aceasta înseamnă că orice date care sunt considerate sensibile în temeiul legislației Uniunii privind protecția datelor (inclusiv datele privind orientarea sexuală, datele genetice și datele biometrice) vor fi tratate ca informații sensibile în temeiul CCD UE-SUA de către organizațiile certificate.

(18) Ca regulă generală, organizațiile trebuie să obțină consimțământul explicit al persoanelor (și anume acordul acestora) pentru a utiliza informații sensibile în alte scopuri decât cele în care au fost colectate inițial acestea sau cele aprobate ulterior de către persoana respectivă (prin acordul exprimat) sau pentru a le divulga unor părți terțe ([31]).

(19) Un astfel de consimțământ nu trebuie obținut în circumstanțe limitate similare excepțiilor comparabile prevăzute în temeiul legislației Uniunii privind protecția datelor, de exemplu, în cazul în care prelucrarea de date sensibile este în interesul vital al unei persoane, este necesară pentru stabilirea unui drept în instanță sau este necesară în vederea acordării îngrijirii medicale sau a stabilirii unui diagnostic ([32]).

2.2.3 ***Acuratețea, reducerea la minimum și securitatea datelor***

(20) Datele ar trebui să fie exacte și, dacă este necesar, actualizate. De asemenea, acestea ar trebui să fie adecvate, relevante și neexcesive în raport cu scopurile în care sunt prelucrate și, în principiu, păstrate pe o perioadă care nu depășește perioada necesară atingerii scopurilor în care sunt prelucrate datele cu caracter personal.

(21) În conformitate cu *principiul integrității datelor și al limitării scopului* ([33]), datele cu caracter personal trebuie limitate la ceea ce este pertinent în scopul prelucrării. În plus, în măsura în care acest lucru este necesar în scopul prelucrării, organizațiile trebuie să ia măsuri rezonabile pentru a asigura fiabilitatea datelor cu caracter personal în raport cu utilizarea preconizată, precum și acuratețea, exhaustivitatea și actualitatea acestora.

(22) În plus, informațiile cu caracter personal pot fi păstrate într-o formă care identifică o persoană sau permite identificarea sa (așadar, sub formă de date cu caracter personal) ([34]) numai atât timp cât aceasta servește atingerii scopului (scopurilor) în care au fost colectate inițial informațiile sau a scopului (scopurilor) aprobat(e) ulterior de persoana în cauză în temeiul *principiului opțiunii*. Această obligație nu împiedică organizațiile să continue să prelucreze informații cu caracter personal pe perioade mai lungi, însă numai pe perioada și în măsura în care o astfel de prelucrare servește în mod rezonabil atingerii unuia dintre următoarele scopuri specifice similare excepțiilor comparabile prevăzute în legislația Uniunii privind protecția datelor legate de: arhivarea în interes public, jurnalism, literatură și artă, cercetarea științifică și istorică și analiza statistică ([35]). În cazul în care datele cu caracter personal sunt păstrate în unul dintre aceste scopuri, prelucrarea lor face obiectul garanțiilor prevăzute de principii ([36]).

(23) De asemenea, datele cu caracter personal ar trebui prelucrate într-un mod care să le asigure securitatea, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale. În acest scop, operatorii și persoanele împuternicite de operatori ar trebui să ia măsurile tehnice sau organizatorice adecvate pentru a proteja datele cu caracter personal împotriva eventualelor amenințări. Aceste măsuri ar trebui evaluate luând în considerare stadiul actual al tehnologiei, costurile aferente și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscurile la adresa drepturilor persoanelor.

([30]) Anexa I secțiunea II punctul 2 litera (c).
([31]) Anexa I secțiunea II punctul 2 litera (c).
([32]) Anexa I secțiunea III punctul 1.
([33]) Anexa I secțiunea II punctul 5.
([34]) A se vedea nota de subsol 7 din anexa I, care clarifică faptul că o persoană este considerată „identificabilă” atât timp cât o organizație sau o parte terță ar putea identifica persoana respectivă în mod rezonabil, ținând seama de mijloacele de identificare ce pot fi utilizate în mod rezonabil (luând în considerare, printre altele, costul și intervalul de timp necesare pentru identificare și tehnologia disponibilă la momentul prelucrării).
([35]) Anexa I secțiunea II punctul 5 litera (b).
([36]) *Ibidem*.

(24) În temeiul CCD UE-SUA, acest lucru este asigurat de *principiul securității*, care impune, în mod similar celor prevăzute la articolul 32 din Regulamentul (UE) 2016/679, să se adopte măsuri de securitate rezonabile și adecvate, ținând seama de riscurile implicate în prelucrarea datelor și de natura acestora ([37]).

2.2.4 ***Transparența***

(25) Persoanele vizate ar trebui să fie informate cu privire la principalele caracteristici ale prelucrării datelor cu caracter personal ale acestora.

(26) Acest lucru este asigurat prin *principiul notificării* ([38]), care, în mod similar cerințelor de transparență prevăzute în Regulamentul (UE) 2016/679, impune organizațiilor să informeze persoanele vizate, printre altele, cu privire la (i) participarea organizației la CCD, (ii) tipul de date colectate, (iii) scopul prelucrării, (iv) tipul sau identitatea părților terțe cărora le pot fi divulgate datele cu caracter personal și scopurile divulgării respective, (v) drepturile lor individuale, (vi) modul de contactare a organizației și (vii) modalitățile de recurs disponibile.

(27) Această notificare trebuie formulată într-un limbaj clar și lizibil și trebuie comunicată persoanelor în cauză atunci când acestora li se solicită pentru prima dată să furnizeze datele cu caracter personal sau cât mai curând posibil după aceasta, dar, în orice caz, înainte ca datele să fie folosite într-un scop care diferă în mod semnificativ de cel în care au fost colectate (dar care este compatibil cu acesta) sau înainte să fie divulgate unei părți terțe ([39]).

(28) În plus, organizațiile trebuie să își facă publice politicile de confidențialitate care reflectă principiile (sau, în cazul datelor privind resursele umane, să le pună la dispoziția persoanelor în cauză) și să furnizeze linkuri către site-ul web al DoC (cu detalii suplimentare privind certificarea, drepturile persoanelor vizate și mecanismele de recurs disponibile), către lista organizațiilor participante la Cadrul privind confidențialitatea datelor („lista CCD") și către site-ul web al unui furnizor corespunzător de servicii de soluționare alternativă a litigiilor ([40]).

2.2.5 ***Drepturi individuale***

(29) Persoanele vizate ar trebui să aibă anumite drepturi care pot fi impuse operatorului sau persoanei împuternicite de operator, în special dreptul de acces la date, dreptul de a se opune prelucrării și dreptul la rectificarea și ștergerea datelor.

(30) *Principiul accesului* ([41]) aferent CCD UE-SUA oferă persoanelor astfel de drepturi. În special, fără necesitatea unei justificări în acest sens, persoanele vizate au dreptul să obțină din partea unei organizații confirmarea că aceasta prelucrează date cu caracter personal care le privesc, să li se comunice datele respective și să obțină informații cu privire la scopul prelucrării, categoriile de date cu caracter personal care sunt prelucrate și (categoriile de) destinatari cărora le sunt divulgate datele ([42]). Organizațiile au obligația de a răspunde cererilor de acces într-un termen rezonabil ([43]). O organizație poate stabili limite

([37]) Anexa I secțiunea II punctul 4 litera (a). În plus, în ceea ce privește datele privind resursele umane, CCD UE-SUA impune angajatorilor 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 [anexa I secțiunea III punctul 9 litera (b) subpunctul (iii)].

([38]) Anexa I secțiunea II punctul 1.

([39]) Anexa I secțiunea II punctul 1 litera (b). Principiul suplimentar 14 [enunțat în anexa I secțiunea III punctul 14 literele (b) și (c)] stabilește dispoziții specifice pentru prelucrarea datelor cu caracter personal în contextul cercetării medicale și al studiilor clinice. În special, acest principiu permite organizațiilor să prelucreze datele aferente unui studiu clinic chiar și după ce o persoană se retrage din acesta, dacă acest lucru a fost specificat în notificarea furnizată atunci când persoana respectivă a convenit să participe la studiu. În mod similar, în situația în care o organizație CCD UE-SUA primește date cu caracter personal în scopuri de cercetare în domeniul sănătății, aceasta le poate utiliza numai pentru o nouă activitate de cercetare, în conformitate cu principiul *notificării* și al *opțiunii*. În acest caz, notificarea adresată persoanei în cauză, ar trebui, în principiu, să ofere informații cu privire la orice utilizare specifică viitoare a datelor (de exemplu, în studii conexe). În cazul în care nu este posibil să se includă de la început toate utilizările viitoare ale datelor (deoarece o nouă utilizare în scopuri de cercetare ar putea rezulta din noi perspective sau evoluții medicale/de cercetare), trebuie inclusă o explicație a faptului că datele pot fi utilizate în activități viitoare neprevăzute de cercetare medicală și farmaceutică. În cazul în care această utilizare ulterioară a datelor nu este conformă cu scopurile de cercetare generale în care au fost colectate datele (și anume dacă noile scopuri diferă în mod semnificativ de scopul inițial, dar sunt totuși compatibile cu acesta, a se vedea considerentele 14-15), trebuie obținut un nou consimțământ (și anume un nou acord). A se vedea, de asemenea, restricțiile/excepțiile specifice de la principiul *notificării* descrise în nota de subsol 28.

([40]) Anexa I secțiunea III punctul 6 litera (d).

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

([42]) Anexa I secțiunea III punctul 8 litera (a) subpunctele (i)-(ii).

([43]) Anexa I secțiunea III punctul 8 litera (i).

rezonabile ale numărului de cereri de acces depuse de o anumită persoană într-o perioadă de timp dată la care va răspunde și poate percepe o taxă care să nu fie excesivă, de exemplu, în situația în care cererile sunt în mod evident excesive, în special ca urmare a caracterului lor repetitiv ([44]).

(31) Dreptul de acces poate fi restricționat numai în împrejurări excepționale similare celor prevăzute de legislația Uniunii privind protecția datelor, în special în cazul în care ar fi încălcate drepturile legitime ale terților, în cazul în care dificultatea sau costurile ocazionate de acordarea dreptului de acces ar fi disproporționată (disproporționate) în raport cu riscurile la adresa vieții private a persoanei în circumstanțele respective (deși costurile și dificultatea aferente acordării accesului nu au un rol decisiv în stabilirea caracterului rezonabil al accesului), în măsura în care divulgarea acestora poate aduce atingere unor importante interese publice, cum ar fi securitate națională, apărarea sau siguranța publică, în cazul în care informațiile respective conțin informații comerciale confidențiale sau informațiile sunt prelucrate exclusiv în scopuri statistice sau de cercetare ([45]). Orice refuz sau limitare a dreptului trebuie să fie necesar(ă) și justificat(ă) în mod corespunzător, organizației revenindu-i sarcina de a demonstra că aceste cerințe sunt îndeplinite ([46]). La efectuarea aprecierii respective, organizația trebuie să țină seama în special de interesele individului ([47]). În situațiile în care este posibilă separarea informațiilor de alte date cărora li se aplică o restricție, organizația trebuie să omită informațiile protejate și să divulge restul informațiilor ([48]).

(32) De asemenea, persoanele vizate au dreptul de a obține rectificarea sau modificarea datelor inexacte și de a obține ștergerea datelor care au fost prelucrate cu încălcarea principiilor ([49]). În plus, astfel cum se explică în considerentul 15, persoanele au dreptul de a se opune prelucrării datelor lor în scopuri care diferă în mod semnificativ de cele în care au fost colectate datele (dar care sunt compatibile cu acestea) și divulgării datelor lor către părți terțe, respectiv de a refuza o astfel de prelucrare și divulgare. Atunci când datele cu caracter personal sunt utilizate în scopuri de marketing direct, persoanele au dreptul general de a renunța în orice moment la prelucrarea acestora ([50]).

(33) Principiile nu abordează în mod specific deciziile care afectează persoana vizată bazate exclusiv pe prelucrarea automată a datelor cu caracter personal. Cu toate acestea, în ceea ce privește datele cu caracter personal care au fost colectate în Uniune, orice decizie bazată pe prelucrarea automată va fi luată, de regulă, de către operatorul din Uniune (care are o relație directă cu persoana vizată în cauză) și, prin urmare, intră sub incidența directă a Regulamentului (UE) 2016/679 ([51]). Această situație include scenarii de transfer în care prelucrarea este efectuată de un operator economic din străinătate (de exemplu, din SUA) care acționează ca agent (persoană împuternicită de operator) în numele operatorului din Uniune (sau în calitate de subcontractant care acționează în numele persoanei împuternicite de operator din Uniune, care a primit datele de la un operator din Uniune care le-a colectat), care, pe această bază, ia decizia respectivă.

(34) Acest lucru a fost confirmat de un studiu comandat de Comisie în 2018 în contextul celei de a doua revizuiri anuale a funcționării Scutului de confidențialitate ([52]), care a concluzionat că, la momentul respectiv, nu existau dovezi care să sugereze că, în mod normal, organizațiile care au aderat la Scutul de confidențialitate desfășurau un proces decizional automatizat pe baza datelor cu caracter personal transferate în temeiul Scutului de confidențialitate.

([44]) Anexa I secțiunea III punctul 8 litera (f) subpunctele (i)-(ii) și litera (g).
([45]) Anexa I secțiunea III punctul 4, punctul 8 literele (b), (c) și (e), punctul 14 literele (e) și (f) și punctul 15 litera (d).
([46]) Anexa I secțiunea III punctul 8 litera (e) subpunctul (ii). Organizația trebuie să informeze persoana în cauză cu privire la motivele refuzului/restricției și să furnizeze un punct de contact pentru solicitări de informații suplimentare – secțiunea III punctul 8 litera (a) subpunctul (iii).
([47]) Anexa I secțiunea III punctul 8 litera (a) subpunctele (ii)-(iii).
([48]) Anexa I secțiunea III punctul 8 litera (a) subpunctul (i).
([49]) Anexa I secțiunea II punctul 6 și secțiunea III punctul 8 litera (a) subpunctul (i).
([50]) Anexa I secțiunea III punctele 8 și 12.
([51]) În schimb, în cazul excepțional în care organizația din SUA are o relație directă cu persoana vizată din Uniune, aceasta va fi, de regulă, o consecință a faptului că aceasta s-a adresat persoanei din Uniune prin oferirea de bunuri sau servicii ori prin monitorizarea comportamentului său. În acest scenariu, organizația din SUA va intra sub incidența Regulamentului (UE) 2016/679 [articolul 3 alineatul (2)] și, prin urmare, trebuie să respecte în mod direct legislația Uniunii privind protecția datelor.
([52]) SWD(2018) 497 final, punctul 4.1.5. Studiul s-a axat pe (i) măsura în care organizațiile din SUA care au aderat la Scutul de confidențialitate iau decizii care afectează persoanele bazate pe prelucrarea automată a datelor cu caracter personal transferate de la întreprinderi din UE în temeiul Scutului de confidențialitate și (ii) garanțiile acordate persoanelor pe care le prevede legislația federală din SUA pentru acest tip de situații și condițiile de aplicare a acestor garanții.

(35) În orice caz, în domeniile în care întreprinderile recurg, cel mai probabil, la prelucrarea automată a datelor cu caracter personal pentru a lua decizii care afectează persoanele (de exemplu, creditare, oferte de credite ipotecare, ocuparea forței de muncă, locuințe și asigurări), legislația SUA oferă măsuri specifice de protecție împotriva deciziilor nefavorabile ([53]). Aceste acte legislative 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. În domeniul creditelor de consum, Legea privind raportarea echitabilă a creditelor (*Fair Credit Reporting Act*) (FCRA) și Legea privind egalitatea de șanse în materie de credit (*Equal Credit Opportunity Act*) (ECOA) conțin garanții care oferă consumatorilor, într-o anumită formă, dreptul la explicații și dreptul de a contesta decizia. Aceste acte legislative sunt relevante într-o gamă largă de domenii, inclusiv în domeniul creditării, al ocupării forței de muncă, al locuințelor și al asigurărilor. În plus, anumite legi împotriva discriminării, cum ar fi titlul VII din Legea privind drepturile civile (*Civil Rights Act*) și Legea privind egalitatea de șanse în materie de locuințe (*Fair Housing Act*), oferă protecție persoanelor în ceea ce privește modelele utilizate în procesul decizional automatizat care ar putea conduce la discriminare pe baza anumitor caracteristici și acordă persoanelor dreptul de a contesta astfel de decizii, inclusiv deciziile automatizate. În ceea ce privește informațiile în materie de sănătate, Legea privind portabilitatea și răspunderea în materie de asigurări de sănătate (*Health Insurance Portability and Accountability Act*) (HIPAA) creează anumite drepturi similare celor prevăzute în Regulamentul (UE) 2016/679 în ceea ce privește accesul la informațiile cu caracter personal privind sănătatea. În plus, orientările din partea autorităților SUA impun furnizorilor de servicii medicale să primească informații care să le permită să informeze persoanele cu privire la sistemele aferente proceselor decizionale automatizate din sectorul medical ([54]).

(36) Prin urmare, aceste norme oferă măsuri de protecție similare celor prevăzute în legislația Uniunii privind protecția datelor în situația improbabilă a luării unor decizii automatizate de către o organizație CCD UE-SUA.

2.2.6 ***Restricții privind transferurile ulterioare de date***

(37) Nivelul de protecție conferit datelor cu caracter personal transferate din Uniune către organizații din Statele Unite ale Americii nu trebuie să fie subminat de transferul ulterior al acestor date către un destinatar din Statele Unite ale Americii sau dintr-o altă țară terță.

(38) În temeiul *principiului responsabilității pentru transferurile ulterioare* ([55]), se aplică norme speciale pentru așa-numitele „transferuri ulterioare", și anume pentru transferurile de date cu caracter personal de la o organizație CCD UE-SUA către o parte terță care este operator sau persoana împuternicită de operator, indiferent dacă aceasta din urmă este situată în Statele Unite ale Americii sau într-o țară terță față de Statele Unite ale Americii (și față de Uniune). Orice transfer ulterior poate avea loc (i) numai în scopuri limitate și specificate, (ii) pe baza unui contract încheiat între organizația CCD UE-SUA și partea terță ([56]) (sau a unui acord asemănător în cadrul unui grup de întreprinderi ([57])) și (iii) numai în cazul în care contractul respectiv îi impune părții terțe în cauză să asigure același nivel de protecție precum cel garantat de principii.

(39) Această obligație de a oferi același nivel de protecție precum cel garantat de principii, coroborată cu *principiul integrității datelor și al limitării scopului* înseamnă, în special, că partea terță poate prelucra doar informațiile cu caracter personal transmise în scopuri care nu sunt incompatibile cu scopurile în care au fost colectate inițial informațiile sau cu scopurile aprobate ulterior de persoana în cauză (în conformitate cu *principiul opțiunii*).

([53]) A se vedea, de exemplu, Legea privind egalitatea de șanse în materie de credit [titlul 15 articolul 1691 și următoarele din U.S.C. – Codul legislației SUA (*US Code*)] sau Legea privind raportarea echitabilă a creditelor (titlul 15 articolul 1681 și următoarele din U.S.C.) sau Legea privind egalitatea de șanse în materie de locuințe (titlul 42 articolul 3601 și următoarele din U.S.C.). În plus, Statele Unite ale Americii au aderat la principiile Organizației pentru Cooperare și Dezvoltare Economică privind inteligența artificială, care includ, printre altele, principii privind transparența, caracterul explicabil, securitatea și responsabilitatea.

([54]) A se vedea, de exemplu, orientările disponibile la 2042-What personal health information do individuals have a right under HIPAA to access from their health care providers and health plans? | HHS.gov (2042-Ce informații cu caracter personal în materie de sănătate au dreptul, în temeiul HIPAA, să acceseze persoanele la nivelul furnizorilor lor de asistență medicală și al planurilor lor de sănătate?).

([55]) A se vedea anexa I secțiunea II punctul 3 și principiul suplimentar „Contracte obligatorii pentru transferurile ulterioare" (anexa I secțiunea III punctul 10).

([56]) Ca excepție de la acest principiu general, o organizație poate transfera ulterior datele cu caracter personal ale unui număr mic de angajați fără a încheia un contract cu destinatarul acestora pentru necesități operaționale ocazionale în contextul unui raport de muncă, de exemplu, pentru rezervarea unui bilet de avion sau a unei camere de hotel sau pentru contractarea unei asigurări. Cu toate acestea, și în acest caz, organizația trebuie să respecte în continuare principiul *notificării* și al *opțiunii* [a se vedea anexa I secțiunea III punctul 9 litera (e)].

([57]) A se vedea principiul suplimentar „Contracte obligatorii pentru transferurile ulterioare" [anexa I secțiunea III punctul 10 litera (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 certificată 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.

(40) *Principiul responsabilității pentru transferurile ulterioare* ar trebui, de asemenea, coroborat cu *principiul notificării* și, în cazul unui transfer ulterior către un operator terț ([58]), cu *principiul opțiunii*, potrivit căruia persoanele vizate trebuie să fie informate, printre altele, cu privire la tipul/identitatea oricărui destinatar terț, la scopul transferului ulterior și la opțiunile oferite, acestea putându-se opune transferului ulterior respectiv (putându-l refuza) sau, în cazul datelor sensibile, trebuind să își dea „consimțământului explicit” (acordul) în ceea ce privește transferul ulterior respectiv.

(41) Obligația de a oferi același nivel de protecție precum 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 destinatarul terț inițial transferă el însuși datele respective către un alt destinatar terț, de exemplu, în scopuri de subcontractare a serviciilor de prelucrare a datelor.

(42) În toate cazurile, contractul cu destinatarul terț trebuie să prevadă că acesta din urmă va transmite o notificare organizației CCD UE-SUA dacă ajunge la concluzia că nu mai poate îndeplini această obligație. În cazul în care se ajunge la o astfel de concluzie, prelucrarea de către partea terță respectivă trebuie să înceteze sau trebuie luate alte măsuri rezonabile și adecvate pentru a remedia situația ([59]).

(43) În cazul unui transfer ulterior către un agent terț (și anume o persoană împuternicită de operator), se aplică măsuri de protecție suplimentare. În acest caz, organizația din SUA trebuie să se asigure că agentul acționează numai pe baza instrucțiunilor sale și 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 ([60]). DoC poate solicita organizației respective să furnizeze un rezumat sau o copie reprezentativă a dispozițiilor privind confidențialitatea incluse în contract ([61]). În cazul în care apar probleme legate de conformitate de-a lungul lanțului de (sub)contractare a serviciilor de prelucrare, organizația care acționează în calitate de operator de date cu caracter personal va fi, în principiu, organizația responsabilă, astfel cum prevede *principiul recursului, al punerii în aplicare și al răspunderii*, cu excepția situației în care dovedește că nu este responsabilă pentru fapta care a provocat prejudiciul ([62]).

2.2.7 ***Responsabilitatea***

(44) Conform principiului responsabilității, entităților care prelucrează date li se solicită să pună în aplicare măsuri tehnice și organizatorice adecvate pentru a-și respecta în mod efectiv obligațiile în materie de protecție a datelor și pentru a putea demonstra această conformitate, în special autorității de supraveghere competente.

(45) Odată ce o organizație a decis în mod voluntar să se certifice ([63]) în temeiul CCD UE-SUA, respectarea efectivă a principiilor este obligatorie și executorie. În temeiul *principiului recursului, al punerii în aplicare și al răspunderii* ([64]), organizațiile CCD UE-SUA trebuie să ofere mecanisme eficace pentru a asigura respectarea principiilor. De asemenea, organizațiile trebuie să ia măsuri pentru a verifica ([65]) dacă politicile lor de confidențialitate sunt conforme cu principiile și sunt respectate efectiv. Acest lucru se poate realiza fie prin intermediul unui sistem de autoevaluare, care trebuie să includă proceduri interne care garantează 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 evaluări externe ale conformității, metode care pot include auditul, verificările aleatorii sau utilizarea instrumentelor tehnologice.

([58]) Persoanele nu vor dispune de dreptul de refuz în cazul în care datele cu caracter personal sunt transferate unei părți terțe 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 SUA va fi răspunzătoare pentru garantarea măsurilor de protecție acordate în temeiul principiilor prin exercitarea competențelor sale de a da instrucțiuni.

([59]) Situația diferă în funcție de calitatea părții terțe, respectiv de operator sau persoană împuternicită de 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 a doua ipoteză, sarcina de a lua aceste măsuri îi revine organizației CCD UE-SUA, ea controlând prelucrarea și dând instrucțiunile pe baza cărora agentul își desfășoară activitatea. A se vedea anexa I secțiunea II punctul 3.

([60]) Anexa I secțiunea II punctul 3 litera (b).

([61]) *Ibidem*.

([62]) Anexa I secțiunea II punctul 7 litera (d).

([63]) A se vedea, de asemenea, principiul suplimentar „Autocertificarea” (anexa I secțiunea III punctul 6).

([64]) A se vedea, de asemenea, principiul suplimentar „Soluționarea litigiilor și punerea în aplicare a deciziilor” (anexa I secțiunea III punctul 11).

([65]) A se vedea, de asemenea, principiul suplimentar „Verificarea” (anexa I secțiunea III punctul 7).

(46) În plus, organizațiile trebuie să păstreze evidențe privind punerea în aplicare a practicilor lor aferente CCD UE-SUA și să le pună la dispoziție, la cerere, organismului independent de soluționare a litigiilor sau autorității competente de aplicare a legii în contextul unei investigații sau al unei plângeri referitoare la o situație de neconformitate ([66]).

2.3 **Gestionarea, supravegherea și asigurarea respectării legii**

(47) CCD UE-SUA va fi gestionat de DoC. Cadrul prevede mecanisme de supraveghere și de asigurare a respectării legii, menite să verifice și să asigure faptul că organizațiile CCD UE-SUA respectă principiile și că orice încălcare este remediată. Aceste mecanisme sunt prezentate în cadrul principiilor (anexa I) și al angajamentelor asumate de DoC (anexa III), de FTC (anexa IV) și de DoT (anexa V).

2.3.1 ***(Re)certificarea***

(48) Pentru a se certifica în temeiul CCD UE-SUA (sau pentru a se recertifica anual), organizațiile trebuie să își declare în mod public angajamentul de a respecta principiile, să își pună la dispoziție politicile de confidențialitate și să le pună pe deplin în aplicare ([67]). În cadrul cererii lor de (re)certificare, organizațiile trebuie să transmită DoC informații privind, printre altele, numele organizației relevante, o descriere a scopurilor în care organizația va prelucra datele cu caracter personal, datele cu caracter personal care vor face obiectul certificării, precum și metoda de verificare aleasă, mecanismul independent de recurs relevant și organismul statutar care are competența de a asigura respectarea principiilor ([68]).

(49) Organizațiile pot primi date cu caracter personal în baza CCD UE-SUA de la data la care sunt incluse pe lista CCD de către DoC. Pentru a asigura securitatea juridică și pentru a evita „declarațiile false", organizațiilor care se certifică pentru prima dată nu le este permis să facă publică adeziunea acestora la principii înainte ca DoC să fi stabilit că respectiva cerere de certificare a organizației este completă și să fi adăugat organizația pe lista CCD ([69]). Pentru a avea în continuare dreptul să beneficieze de CCD UE-SUA pentru a primi date cu caracter personal din Uniune, astfel de organizații trebuie să își recertifice anual participarea la cadru. Atunci când o organizație părăsește CCD UE-SUA, indiferent de motiv, aceasta trebuie să elimine toate declarațiile care implică faptul că organizația participă în continuare la cadru ([70]).

(50) Astfel cum se reflectă în angajamentele prevăzute în anexa III, DoC va verifica dacă organizațiile îndeplinesc toate cerințele de certificare și dacă au instituit o politică (publică) de confidențialitate care să conțină informațiile necesare în temeiul *principiului notificării* ([71]). Pe baza experienței acumulate în procesul de (re)certificare în temeiul Scutului de confidențialitate, DoC va efectua o serie de verificări, inclusiv pentru a stabili dacă politicile de confidențialitate ale organizațiilor conțin un hyperlink către formularul de plângere corect de pe site-ul web al mecanismului relevant de soluționare a litigiilor și, atunci când mai multe entități și filiale ale unei organizații sunt incluse într-o cerere de certificare, dacă politicile de confidențialitate ale fiecăreia dintre aceste entități îndeplinesc cerințele de certificare și dacă sunt ușor accesibile persoanelor vizate ([72]). În plus, atunci când este necesar, DoC va efectua verificări încrucișate cu FTC și DoT pentru a stabili dacă organizațiile se supun autorității organismului de supraveghere identificat în cererile lor de (re)certificare și va colabora cu organisme de soluționare alternativă a litigiilor pentru a stabili dacă organizațiile sunt înregistrate în ceea ce privește mecanismul independent de recurs identificat în cererea lor de (re)certificare ([73]).

([66]) Anexa I secțiunea III punctul 7.
([67]) Anexa I secțiunea I punctul 2.
([68]) Anexa I secțiunea III punctul 6 litera (b) și anexa III – a se vedea secțiunea „Verificarea cerințelor de autocertificare".
([69]) Nota de subsol 12 din anexa I.
([70]) Anexa I secțiunea III punctul 6 litera (h).
([71]) Anexa I secțiunea III punctul 6 litera (a) și nota de subsol 12, precum și anexa III – a se vedea secțiunea „Verificarea cerințelor de autocertificare".
([72]) Anexa III – secțiunea „Verificarea cerințelor de autocertificare".
([73]) În mod similar, DoC va colabora cu partea terță care va servi drept custode al fondurilor colectate prin intermediul taxei pentru comitetul APD (a se vedea considerentul 73) pentru a verifica dacă organizațiile care aleg APD ca mecanism independent de recurs au plătit taxa pentru anul relevant. A se vedea anexa III – secțiunea „Verificarea cerințelor de autocertificare".

(51) DoC va informa organizațiile că, pentru a finaliza (re)certificarea, acestea trebuie să abordeze toate problemele identificate în cursul revizuirii sale. În cazul în care o organizație nu răspunde într-un interval de timp stabilit de DoC (de exemplu, în ceea ce privește recertificarea, se așteaptă ca procesul să fie finalizat în termen de 45 de zile) ([74]) sau în cazul în care nu își finalizează certificarea, se va considera că s-a renunțat la cererea respectivă. În acest caz, orice declarație falsă cu privire la participarea la CCD UE-SUA sau la respectarea acestuia poate face obiectul unei măsuri de asigurare a respectării legii luate de FTC sau DoT ([75]).

(52) Pentru a asigura aplicarea corespunzătoare a CCD 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. Pentru a asigura o astfel de transparență la „punctul de intrare", DoC s-a angajat să mențină și să pună la dispoziția publicului o listă a organizațiilor care și-au certificat adeziunea la principii și care intră sub jurisdicția a cel puțin uneia dintre autoritățile de aplicare a legii enumerate în anexele IV și V la prezenta decizie ([76]). DoC va actualiza lista pe baza cererii de recertificare depuse anual de o organizație și ori de câte ori o organizație se retrage sau este eliminată din CCD UE-SUA. În plus, pentru a garanta transparența și la „punctul de ieșire", DoC va menține și va pune la dispoziția publicului un registru al organizațiilor care au fost eliminate de pe listă, în fiecare caz identificând motivul aflat la baza unei astfel de măsuri ([77]). În cele din urmă, acesta va furniza un link către pagina web a FTC aferentă CCD UE-SUA, unde se vor regăsi măsurile de asigurare a respectării legii adoptate de FTC în temeiul cadrului ([78]).

2.3.2 ***Monitorizarea conformității***

(53) DoC va monitoriza în permanență respectarea efectivă a principiilor de către organizațiile CCD UE-SUA prin diferite mecanisme ([79]). În special, acesta va efectua „controale prin sondaj" asupra unor organizații selectate aleatoriu, precum și controale prin sondaj ad-hoc asupra unor organizații specifice atunci când sunt identificate posibile probleme de conformitate (de exemplu, aspecte sesizate DoC de către părți terțe) pentru a verifica dacă (i) punctul (punctele) de contact pentru gestionarea plângerilor și a cererilor persoanelor vizate este (sunt) disponibil(e) și oferă răspunsuri la acestea, (ii) politica de confidențialitate a organizației este ușor accesibilă, atât pe site-ul său web, cât și prin intermediul unui hyperlink existent pe site-ul web al DoC, (iii) politica de confidențialitate a organizației continuă să respecte cerințele de certificare și (iv) mecanismul independent de soluționare a litigiilor ales de organizații este disponibil pentru gestionarea plângerilor ([80]).

(54) În cazul în care există dovezi credibile că o organizație nu își respectă angajamentele asumate în temeiul CCD UE-SUA (inclusiv în cazul în care DoC primește plângeri sau organizația nu răspunde în mod satisfăcător la solicitările de informații înaintate de DoC), DoC va solicita organizației să completeze și să transmită un chestionar detaliat ([81]). În cazul în care o organizație nu răspunde în mod satisfăcător și în timp util la chestionarul respectiv, se va transmite o sesizare în acest sens autorității relevante (FTC sau DoT) pentru impunerea unor eventuale măsuri de asigurare a respectării legii ([82]). În cadrul activităților sale de monitorizare a conformității în temeiul Scutului de

([74]) Nota de subsol 2 din anexa III.

([75]) A se vedea anexa III – secțiunea „Verificarea cerințelor de autocertificare".

([76]) Informații privind gestionarea listei CCD se regăsesc în anexa III (a se vedea introducerea secțiunii „Gestionarea și supravegherea programului aferent Cadrului privind confidențialitatea datelor de către Departamentul Comerțului") și în anexa I [secțiunea I punctul 3, secțiunea I punctul 4, secțiunea III punctul 6 litera (d) și secțiunea III punctul 11 litera (g)].

([77]) Anexa III – a se vedea introducerea secțiunii „Gestionarea și supravegherea programului aferent Cadrului privind confidențialitatea datelor de către Departamentul Comerțului".

([78]) A se vedea anexa III – secțiunea „Adaptarea site-ului web destinat Cadrului privind confidențialitatea datelor la publicul vizat".

([79]) A se vedea anexa III – secțiunea „Efectuarea de evaluări periodice *ex officio* ale conformității și de evaluări ale programului aferent Cadrului privind confidențialitatea datelor".

([80]) În cadrul activităților sale de monitorizare, DoC poate utiliza diferite instrumente, inclusiv să verifice dacă există linkuri inactive către politicile de confidențialitate sau să monitorizeze în mod activ știrile pentru a identifica relatări care oferă dovezi credibile de neconformitate.

([81]) A se vedea anexa III – secțiunea „Efectuarea de evaluări periodice *ex officio* ale conformității și de evaluări ale programului aferent Cadrului privind confidențialitatea datelor".

([82]) A se vedea anexa III – secțiunea „Efectuarea de evaluări periodice *ex officio* ale conformității și de evaluări ale programului aferent Cadrului privind confidențialitatea datelor".

confidențialitate, DoC a efectuat periodic controalele prin sondaj menționate în considerentul 53 și a monitorizat în permanență relatările publice, ceea ce i-a permis să identifice, să abordeze și să soluționeze problemele de conformitate ([83]). Organizațiile care încalcă în mod sistematic principiile vor fi eliminate de pe lista CCD și trebuie să returneze sau să șteargă datele cu caracter personal primite în temeiul cadrului ([84]).

(55) În alte cazuri de eliminare, precum retragerea voluntară sau lipsa recertificării, organizația fie trebuie să șteargă sau să returneze datele, fie poate să le păstreze, cu condiția să declare anual DoC angajamentul de a continua să aplice principiile sau să ofere o protecție adecvată a datelor cu caracter personal prin alte mijloace autorizate (de exemplu, aplicând un contract care să reflecte pe deplin cerințele clauzelor contractuale standard relevante aprobate de către Comisie) ([85]). În acest caz, o organizație trebuie, de asemenea, să identifice un punct de contact în cadrul organizației pentru toate întrebările legate de CCD UE-SUA.

2.3.3 ***Identificarea și abordarea declarațiilor false de participare***

(56) DoC va monitoriza orice declarații false de participare la CCD UE-SUA sau utilizarea necorespunzătoare a mărcii de certificare aferente CCD UE-SUA, atât din oficiu, cât și pe baza plângerilor primite (de exemplu, de la APD) ([86]). În special, DoC va verifica în permanență dacă organizațiile care (i) se retrag din CCD UE-SUA, (ii) nu finalizează procesul de recertificare anuală (și anume fie au început, dar nu au finalizat procesul de recertificare anuală în timp util, fie nici măcar nu au început procesul de recertificare anuală), (iii) sunt eliminate ca participant, în special pentru o „încălcare sistematică" sau (iv) nu finalizează o certificare inițială (și anume au început, dar nu au finalizat procesul de certificare inițială în timp util) elimină din orice politică de confidențialitate relevantă publicată trimiterile la CCD UE-SUA care implică faptul că organizația participă activ la cadru ([87]). De asemenea, DoC va efectua căutări pe internet pentru a identifica trimiteri la CCD UE-SUA în politicile de confidențialitate ale organizațiilor, inclusiv pentru a identifica declarațiile false ale organizațiilor care nu au participat niciodată la CCD UE-SUA ([88]).

(57) În cazul în care constată că trimiterile la CCD UE-SUA nu au fost eliminate sau sunt utilizate în mod necorespunzător, DoC va informa organizația în cauză cu privire la o posibilă sesizare a FTC/DoT ([89]). În cazul în care o organizație nu răspunde în mod satisfăcător, DoC va sesiza agenția relevantă în vederea impunerii unor eventuale măsuri de asigurare a respectării legii ([90]). Orice declarație falsă adresată publicului larg de către o organizație cu privire la adeziunea la principii sub forma unor afirmații sau practici înșelătoare poate fi sancționată de către FTC, DoT sau alte autorități relevante de aplicare a legii din SUA. Declarațiile false adresate DoC pot fi sancționate în temeiul Legii privind declarațiile false (*False Statements Act*) (titlul 18 articolul 1001din U.S.C.)

([83]) În cursul celei de a doua revizuiri anuale a Scutului de confidențialitate, DoC a comunicat că a efectuat controale prin sondaj asupra a 100 de organizații și a trimis chestionare de conformitate în 21 de cazuri (după care problemele detectate au fost remediate); a se vedea documentul de lucru al serviciilor Comisiei SWD(2018) 497 final, p. 9. În mod similar, în cursul celei de a treia revizuiri anuale a Scutului de confidențialitate, DoC a raportat că a detectat trei incidente prin monitorizarea relatărilor publice și a început să efectueze controale prin sondaj a 30 de societăți în fiecare lună, această practică ducând la acțiuni de monitorizare prin intermediul chestionarelor de conformitate în 28 % din cazuri (după care problemele detectate au fost imediat remediate sau, în trei cazuri, au fost soluționate în urma unei scrisori de avertizare); a se vedea documentul de lucru al serviciilor Comisiei SWD(2019) 495 final, p. 8.

([84]) Anexa I secțiunea III punctul 11 litera (g). O situație de încălcare sistematică survine, în special, atunci când o organizație refuză să se supună unei decizii definitive a oricărei autorități de autoreglementare în materie de protecție a vieții private, a oricărei autorități independente de soluționare a litigiilor sau a oricărei autorități de aplicare a legii.

([85]) Anexa I secțiunea III punctul 6 litera (f).

([86]) Anexa III – secțiunea „Identificarea și abordarea declarațiilor false de participare".

([87]) *Ibidem*.

([88]) *Ibidem*.

([89]) *Ibidem*.

([90]) În temeiul Scutului de confidențialitate, DoC a raportat, în cursul celei de a treia revizuiri anuale a cadrului, că a identificat 669 de cazuri de declarații false de participare (între octombrie 2018 și octombrie 2019), dintre care majoritatea au fost soluționate după scrisoarea de avertizare a DoC, 143 de cazuri fiind înaintate FTC (a se vedea considerentul 62 de mai jos). A se vedea documentul de lucru al serviciilor Comisiei SWD(2019) 495 final, p. 10.

2.3.4 ***Asigurarea respectării legii***

(58) Pentru a asigura în practică un nivel adecvat de protecție a datelor, ar trebui instituită o autoritate de supraveghere independentă, care să aibă competența de a monitoriza și de a asigura respectarea normelor de protecție a datelor.

(59) Organizațiile CCD UE-SUA trebuie să se afle sub jurisdicția autorităților competente din SUA – FTC și DoT – care dispun de competențele necesare de investigare și de asigurare a respectării legii pentru a asigura respectarea efectivă a principiilor ([91]).

(60) FTC este o autoritate independentă compusă din cinci comisari, care sunt numiți de președinte, cu avizul și acordul Senatului ([92]). Comisarii sunt numiți pentru un mandat de șapte ani și pot fi revocați din funcție numai de către președinte pentru ineficiență, neglijență sau practici ilicite în serviciu. FTC nu poate include mai mult de trei comisari din cadrul aceluiași partid politic și, în timpul mandatului lor, comisarii nu pot să desfășoare alte activități comerciale, profesionale sau salariale.

(61) FTC poate investiga respectarea principiilor, precum și declarațiile false de adeziune la principii sau de participare la CCD UE-SUA emise de către organizații care fie nu se mai află pe lista CCD, fie nu s-au certificat niciodată ([93]). FTC poate asigura conformitatea prin solicitarea unor ordine judecătorești federale sau administrative (inclusiv a unor „ordonanțe prin consimțământ" obținute prin intermediul tranzacțiilor) ([94]) cu caracter preliminar sau definitiv sau de stabilire a altor măsuri reparatorii și va monitoriza în mod sistematic respectarea acestor ordine ([95]). În cazul în care organizațiile nu respectă aceste ordine, FTC poate solicita sancțiuni civile și alte măsuri reparatorii, inclusiv pentru orice prejudiciu cauzat de comportamentul ilicit. Fiecare ordonanță prin consimțământ adresată unei organizații CCD UE-SUA va include dispoziții de autoraportare ([96]), iar organizațiile vor trebui să facă publice toate secțiunile relevante cu privire la CCD UE-SUA din orice raport de conformitate sau de evaluare transmis către FTC. În sfârșit, FTC va menține o listă online a organizațiilor care fac obiectul unor ordine ale FTC sau al unor ordine judecătorești în cazuri care vizează CCD UE-SUA ([97]).

(62) În ceea ce privește Scutul de confidențialitate, FTC a luat măsuri de asigurare a respectării legii în aproximativ 22 de cazuri, atât în ceea ce privește încălcarea cerințelor specifice ale cadrului (de exemplu, nedeclararea în fața DoC a faptului că organizația a continuat să aplice măsurile de protecție prevăzute de Scutul de confidențialitate după ce a părăsit cadrul, neverificarea, printr-o autoevaluare sau printr-o evaluare externă a conformității, dacă organizația a respectat cadrul) ([98]), cât și în ceea ce privește declarațiile false de participare la cadrul respectiv (de exemplu, ale organizațiilor care nu au finalizat etapele necesare pentru a obține certificarea sau au permis expirarea certificării lor, însă care au dat declarații false cu privire la participarea în continuare la cadru) ([99]). Această măsură de asigurare a respectării legii a rezultat, printre altele, din utilizarea proactivă a citațiilor administrative pentru a obține materiale de la anumiți participanți la Scutul de confidențialitate cu scopul de a verifica dacă există încălcări de fond ale obligațiilor asumate în temeiul Scutului de confidențialitate ([100]).

([91]) O organizație CCD UE-SUA 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 poate fi sancționată în temeiul secțiunii 5 din Legea privind FTC (*FTC Act*), care interzice practicile neloiale și frauduloase în domeniul comerțului sau care afectează comerțul (titlul 15 articolul 45 din U.S.C.) și al titlului 49 articolul 41712 din U.S.C., care interzice unui transportator sau unui agent de bilete să desfășoare orice practică neloială sau frauduloasă în cadrul activității de transport aerian sau pentru vânzarea de servicii de transport aerian.

([92]) Titlul 15 articolul 41 din U.S.C.

([93]) Anexa IV.

([94]) 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 poate obliga organizațiile să prezinte înscrisuri și să furnizeze declarații ale martorilor (a se vedea secțiunea 20 din Legea privind FTC) și poate apela la sistemul judiciar pentru a executa aceste ordine într-o situație de neconformitate.

([95]) A se vedea anexa IV – secțiunea „Solicitarea și monitorizarea ordinelor".

([96]) Ordinele FTC sau ordinele judecătorești pot impune societăților să pună în aplicare programe de protecție a vieții private și să pună periodic la dispoziția FTC rapoarte de conformitate sau evaluări independente externe ale programelor respective.

([97]) Anexa IV – secțiunea „Solicitarea și monitorizarea ordinelor".

([98]) Documentul de lucru al serviciilor Comisiei SWD(2019) 495 final, p. 11.

([99]) A se vedea cazurile menționate pe site-ul web al FTC, disponibil la adresa https://www.ftc.gov/business-guidance/privacy-security/privacy-shield. A se vedea, de asemenea, documentul de lucru al serviciilor Comisiei SWD(2017) 344 final, p. 17, documentul de lucru al serviciilor Comisiei SWD(2018) 497 final, p. 12, și documentul de lucru al serviciilor Comisiei SWD(2019) 495 final, p. 11.

([100]) A se vedea, de exemplu, Prepared Remarks of Chairman Joseph Simons at the Second Privacy Shield Annual Review (ftc.gov) (Observațiile președintelui Joseph Simons cu ocazia celei de a doua revizuiri anuale a Scutului de confidențialitate).

(63) La un nivel mai general, FTC a luat, în ultimii ani, măsuri de asigurare a respectării legii într-o serie de cazuri privind respectarea cerințelor specifice în materie de protecție a datelor care sunt, de asemenea, prevăzute în CCD UE-SUA, de exemplu în ceea ce privește principiul limitării scopului și al păstrării datelor ([101]), principiul reducerii la minimum a datelor ([102]), principiul securității datelor ([103]) și principiul acurateței datelor ([104]).

(64) DoT dispune de competențe exclusive de reglementare a practicilor 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 de bilete la vânzarea serviciilor de transport aerian. Funcționarii DoT urmăresc mai întâi să ajungă la o înțelegere și, dacă acest lucru nu este posibil, pot iniția proceduri de asigurare a respectării legii care implică o audiere probatorie în fața unui judecător de drept administrativ al DoT, care are competența de a emite ordine de încetare și de a impune sancțiuni civile ([105]). Judecătorii de drept administrativ beneficiază de o serie măsuri de protecție în temeiul Legii privind procedura administrativă (*Administrative Procedure Act*) (APA), care vizează asigurarea independenței și a imparțialității acestora. De exemplu, aceștia pot fi revocați din funcție numai din motive întemeiate, iar cazurile le sunt repartizate prin rotație. În plus, nu pot îndeplini sarcini incompatibile cu îndatoririle și responsabilitățile lor în calitate de judecători de drept administrativ, nu fac obiectul supravegherii de către echipa de anchetă a autorității de care aparțin (în acest caz, DoT) și trebuie să își îndeplinească funcția de judecată/de asigurare a respectării legii în mod imparțial ([106]). DoT s-a angajat să monitorizeze ordinele de asigurare a respectării legii și să se asigure că ordinele aferente cazurilor care vizează CCD UE-SUA sunt disponibile pe site-ul său web ([107]).

2.4 **Căi de atac**

(65) Pentru a asigura o protecție adecvată și, în special, pentru asigurarea respectării drepturilor individuale, persoanei vizate ar trebui să i se pună la dispoziție căi de atac administrative și judiciare efective.

(66) CCD UE-SUA, prin *principiul recursului, al punerii în aplicare și al răspunderii*, impune organizațiilor să ofere modalități de recurs persoanelor afectate de nerespectarea cadrului și, prin urmare, posibilitatea ca persoanele vizate din UE să depună plângeri privind nerespectarea cadrului de către organizațiile CCD UE-SUA, precum și ca aceste plângeri să fie soluționate, dacă este cazul, printr-o decizie care prevede o cale de atac eficientă ([108]). Ca parte a certificării acestora, organizațiile trebuie să îndeplinească cerințele acestui principiu, punând la dispoziție mecanisme independente de recurs eficiente și ușor accesibile, care să permită investigarea și soluționarea în mod rapid a litigiilor și a plângerilor înaintate de orice persoană, fără ca aceasta să implice costuri pentru persoana în cauză ([109]).

([101]) A se vedea, de exemplu, ordinul FTC în cauza Drizly, LLC, prin care se impune, printre altele, societății (1) să distrugă toate datele cu caracter personal pe care le-a colectat și care nu sunt necesare pentru a furniza produse sau servicii consumatorilor, (2) să se abțină de la colectarea sau stocarea de informații cu caracter personal, cu excepția cazului în care această acțiune este necesară în scopuri specifice prezentate într-un calendar de păstrare.

([102]) A se vedea, de exemplu, ordinul FTC în cauza CafePress (24 martie 2022), care impune, printre altele, reducerea la minimum a volumului de date colectate.

([103]) A se vedea, de exemplu, măsurile FTC de asigurare a respectării legii în cauzele Drizzly, LLC și CafePress, în care aceasta a solicitat societăților în cauză să instituie un program de securitate dedicat sau măsuri de securitate specifice. În plus, în ceea ce privește încălcarea securității datelor, a se vedea, de asemenea, ordinul FTC din 27 ianuarie 2023 în cauza Chegg, acordul încheiat cu Equifax în 2019 (https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach).

([104]) A se vedea, de exemplu, cauza RealPage, Inc (16 octombrie 2018), în care FTC a luat măsuri de asigurare a respectării legii în temeiul FCRA împotriva unei societăți de verificare a chiriașilor care a furnizat rapoarte de verificare a antecedentelor persoanelor către proprietarii de bunuri imobile și către societățile de administrare a bunurilor imobile, pe baza informațiilor provenite din istoricul închirierilor, a informațiilor din registrele publice (inclusiv istoricul infracțiunilor și al evacuărilor) și a informațiilor privind creditele, care au fost utilizate ca factor de stabilire a eligibilității pentru locuințe. FTC a constatat că societatea nu a luat măsuri rezonabile pentru a asigura acuratețea informațiilor pe care le-a furnizat pe baza instrumentului său decizional automatizat.

([105]) A se vedea anexa V – secțiunea „Practici de asigurare a respectării legii”.

([106]) A se vedea titlul 5 articolul 3105, articolul 7521 litera (a), articolul 554 litera (d) și articolul 556 litera (b) punctul 3 din U.S.C.

([107]) Anexa V – a se vedea secțiunea „Monitorizarea și publicarea ordinelor de asigurare a respectării legii privind încălcările CCD UE-SUA”.

([108]) Anexa I secțiunea II punctul 7.

([109]) Anexa I secțiunea III punctul 11.

(67) Organizațiile pot opta pentru mecanisme independente de recurs fie în Uniune, fie în Statele Unite ale Americii. Astfel cum se explică mai detaliat în considerentul 73, acest lucru include posibilitatea ca acestea să își asume în mod voluntar angajamentul de a coopera cu APD din UE. În cazul în care organizațiile prelucrează date privind resursele umane, un astfel de angajament de cooperare cu APD din UE este obligatoriu. Alte opțiuni includ sistemul independent de soluționare alternativă a litigiilor sau programe privind protecția vieții private elaborate de sectorul privat care integrează principiile în regulile lor. Acestea din urmă trebuie să includă mecanisme eficiente de asigurare a respectării legii, în conformitate cu cerințele *principiului recursului, al punerii în aplicare și al răspunderii*.

(68) Prin urmare, CCD UE-SUA oferă persoanelor vizate o serie de posibilități de a-și exercita drepturile, de a înainta plângeri privind nerespectarea cadrului de către organizațiile CCD UE-SUA, precum și de a beneficia de soluționarea acestor plângeri, dacă este cazul, printr-o decizie care să prevadă o cale de atac eficientă. Persoanele pot înainta plângeri direct unei organizații, unui organism independent de soluționare a litigiilor desemnat de către organizație, precum și APD naționale, DoC sau FTC. În cazul în care plângerile acestora nu au fost soluționate în baza niciunuia dintre aceste mecanisme de recurs sau de asigurare a respectării legii, persoanele au, de asemenea, dreptul de a recurge la procedura de arbitraj obligatoriu (anexa I la anexa I la prezenta decizie). Cu excepția cazului în care se apelează la o comisie de arbitraj, situație care impune ca anumite căi de atac să fie epuizate înainte de sesizarea acesteia, 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 ordine.

(69) În primul rând, persoanele vizate din Uniune pot înainta plângeri care vizează nerespectarea principiilor prin contact direct cu organizațiile CCD UE-SUA în cauză ([110]). Pentru a facilita soluționarea, organizația trebuie să instituie un mecanism eficient de recurs pentru a gestiona 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 în legătură cu orice sediu relevant din Uniune care poate răspunde la solicitările de informații sau la plângeri), precum și cu privire la organismul independent de soluționare a litigiilor desemnat (a se vedea considerentul 70). La primirea unei plângeri direct de la persoana în cauză sau prin intermediul DoC în urma sesizării acestuia de către o APD, organizația trebuie să furnizeze un răspuns persoanei vizate din Uniune în termen de 45 de zile ([111]). În mod similar, organizațiile trebuie să răspundă cu promptitudine la solicitările de informații și la alte solicitări din partea DoC sau a unei APD ([112]) (în cazul în care organizația și-a asumat angajamentul de a coopera cu APD) legate de adeziunea acestora la principii.

(70) În al doilea rând, persoanele pot înainta plângeri direct organismului independent de soluționare a litigiilor (fie în Statele Unite, fie în Uniune) desemnat de organizație să investigheze și să soluționeze plângeri individuale (cu excepția cazului în care acestea sunt în mod evident nefondate sau abuzive) și să asigure persoanei în cauză căi de atac corespunzătoare care să nu presupună costuri pentru aceasta ([113]). Sancțiunile și măsurile reparatorii impuse de un astfel de organism trebuie să fie suficient de severe pentru a asigura respectarea principiilor de către organizații și ar trebui să prevadă o inversare sau o corectare de către organizație a efectelor neconformității respective și, în funcție de circumstanțe, încheierea prelucrării ulterioare a datelor cu caracter personal în cauză și/sau ștergerea acestora, precum și publicarea neconformităților constatate ([114]). Organismele independente de soluționare a litigiilor desemnate de o organizație trebuie să includă pe site-urile lor web publice informații relevante cu privire la CCD UE-SUA și serviciile pe care le furnizează în temeiul acestuia ([115]). În fiecare an, acestea trebuie să publice un raport anual care să furnizeze statistici agregate privind aceste servicii ([116]).

([110]) Anexa I secțiunea III punctul 11 litera (d) subpunctul (i).
([111]) Anexa I secțiunea III punctul 11 litera (d) subpunctul (i).
([112]) Aceasta este autoritatea de gestionare desemnată de comitetul APD prevăzut în principiul suplimentar privind „Rolul autorităților pentru protecția datelor") (anexa I secțiunea III punctul 5).
([113]) Anexa I secțiunea III punctul 11 litera (d).
([114]) Anexa I secțiunea II punctul 7 și secțiunea III punctul 11 litera (e).
([115]) Anexa I secțiunea III punctul 11 litera (d) subpunctul (ii).
([116]) Raportul anual trebuie să conțină: (1) numărul total de plângeri legate de CCD UE-SUA primite în cursul anului de raportare, (2) tipurile de plângeri primite, (3) măsurile cu privire la calitatea procesului de soluționare a litigiilor, cum ar fi perioada de timp necesară pentru soluționarea plângerilor și (4) rezultatele plângerilor primite, în special numărul și tipul de măsuri reparatorii sau sancțiuni impuse.

(71) În cadrul procedurilor de evaluare a conformității desfășurate de DoC, acesta poate verifica dacă organizațiile CCD UE-SUA și-au înregistrat efectiv participarea la mecanismele independente de recurs la care susțin că sunt înregistrate ([117]). Atât organizațiile, cât și mecanismele independente de recurs competente trebuie să răspundă cu promptitudine la solicitările de informații și cererile formulate de DoC referitoare la CCD UE-SUA. DoC va colabora cu mecanismele independente de recurs pentru a verifica dacă acestea includ pe site-urile lor web informații privind principiile și serviciile pe care le furnizează în temeiul CCD UE-SUA, precum și dacă publică rapoarte anuale ([118]).

(72) În cazurile în care organizația nu respectă hotărârea pronunțată de un organism de soluționare a litigiilor sau de autoreglementare, acesta din urmă trebuie să notifice neconformitatea respectivă DoC și FTC (sau altei autorități din SUA cu competențe de investigare a respectivei neconformități) sau unei instanțe competente ([119]). În cazul în care o organizație refuză să se supună unei decizii definitive luate de un organism de autoreglementare în materie de protecție a vieții private, de un organism independent de soluționare a litigiilor sau de un organism guvernamental ori în cazul în care un astfel de organism constată că o organizație încalcă frecvent principiile, se poate considera că este vorba de o încălcare sistematică, care va avea drept consecință radierea de pe lista CCD a organizației respective de către DoC, însă numai după ce acesta acordă organizației respective un preaviz de 30 de zile și posibilitatea de a răspunde ([120]). În cazul în care, după radierea de pe listă, organizația continuă să pretindă că deține certificarea în temeiul CCD UE-SUA, DoC va sesiza în acest sens FTC sau o altă agenție de aplicare a legii ([121]).

(73) În al treilea rând, persoanele pot înainta, de asemenea, plângeri la o APD națională din Uniune, care poate face uz de competențele sale de investigare și de remediere în temeiul Regulamentului (UE) 2016/679. Organizațiile sunt obligate să coopereze în cadrul investigației și al soluționării plângerii de către o APD fie în cazul în care plângerea se referă la prelucrarea datelor privind resursele umane colectate în contextul unui raport de muncă, fie în cazul în care organizația respectivă s-a oferit în mod voluntar să fie supravegheată de către APD ([122]). În special, organizațiile trebuie să răspundă la solicitările de informații, să se conformeze avizului emis de APD, inclusiv în ceea ce privește măsurile reparatorii sau compensatorii, și să trimită APD confirmarea scrisă că au fost întreprinse astfel de acțiuni ([123]). În cazurile de nerespectare a avizului emis de APD, APD va sesiza DoC (care poate elimina organizații de pe lista CCD UE-SUA) sau, pentru eventuale măsuri de asigurare a respectării legii, FTC sau DoT (lipsa cooperării cu autoritățile pentru protecția datelor sau nerespectarea principiilor poate face obiectul unor acțiuni în temeiul legislației SUA) ([124]).

(74) Pentru a facilita cooperarea în vederea unei gestionări eficace a plângerilor, atât DoC, cât și FTC au instituit un punct de contact specific care este responsabil de asigurarea legăturii directe cu APD ([125]). Punctele de contact respective oferă asistență în ceea ce privește anchetele APD cu privire la respectarea principiilor de către o organizație.

(75) Avizul APD ([126]) se emite după ce ambele părți implicate în litigiu au avut posibilitatea rezonabilă de a-și prezenta observațiile și de a aduce toate elementele de probă pe care doresc să le prezinte. Comitetul poate transmite avizul cât mai repede posibil, însă respectând garanțiile procedurale și, ca regulă generală, în termen de 60 de zile după primirea unei plângeri ([127]). 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 își poate notifica intenția fie de a sesiza FTC în această privință (sau o altă autoritate de aplicare a legii competentă din SUA), fie de a concluziona că

([117]) Anexa I – secțiunea „Verificarea cerințelor de autocertificare”.

([118]) A se vedea anexa III – secțiunea „Facilitarea cooperării cu organismele de soluționare alternativă a litigiilor care oferă servicii legate de principii”. A se vedea, de asemenea, anexa I secțiunea III punctul 11 litera (d) subpunctele (ii)-(iii).

([119]) A se vedea anexa I secțiunea III punctul 11 litera (e).

([120]) A se vedea anexa I secțiunea III punctul 11 litera (g), în special subpunctele (ii) și (iii).

([121]) A se vedea anexa III – secțiunea „Identificarea și abordarea declarațiilor false de participare”.

([122]) Anexa I secțiunea II punctul 7 litera (b).

([123]) Anexa I secțiunea III punctul 5.

([124]) Anexa I secțiunea III punctul 5 litera (c) subpunctul (ii).

([125]) Anexa III (a se vedea secțiunea „Facilitarea cooperării cu APD”) și anexa IV (a se vedea secțiunile „Gestionarea cu prioritate a sesizărilor și realizarea investigațiilor” și „Cooperarea cu APD din UE în scopuri de asigurare a respectării legii”).

([126]) Regulamentul de procedură al comitetului informal al APD ar trebui să fie stabilit de APD pe baza competenței lor de a-și organiza activitatea și de a coopera.

([127]) Anexa I secțiunea III punctul 5 litera (c) subpunctul (i).

angajamentul de cooperare a fost grav încălcat. În primul caz, acest lucru poate conduce la măsuri de asigurare a respectării legii în temeiul secțiunii 5 din Legea FTC (sau o lege similară) ([128]). În al doilea caz, comitetul informează DoC, care va considera că refuzul organizației de a se conforma avizului comitetului APD constituie o încălcare sistematică, ceea ce va conduce la eliminarea organizației de pe lista CCD.

(76) În cazul în care APD 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.

(77) 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 al unei organizații. În aceste cazuri, APD poate înainta aceste plângeri fie DoC, fie FTC. Pentru a facilita și a consolida cooperarea în ceea ce privește plângerile individuale și nerespectarea cadrului de către organizațiile CCD UE-SUA, DoC va stabili un punct de contact specific, care să acționeze ca punct de legătură și să ofere asistență în cadrul anchetelor APD cu privire la respectarea principiilor de către o organizație ([129]). FTC s-a angajat, de asemenea, să ofere un punct de contact specific ([130]).

(78) În al patrulea rând, DoC s-a angajat să primească și să examineze plângerile legate de nerespectarea principiilor de către o organizație, precum și să depună toate eforturile în vederea soluționării acestora ([131]). În acest scop, DoC prevede proceduri speciale pentru transmiterea de către APD a plângerilor către un punct de contact specific, urmărirea acestora și contactarea organizațiilor pentru a facilita soluționarea ([132]). Pentru a accelera prelucrarea plângerilor individuale, punctul de contact ia legătura direct cu APD în cauză cu privire la aspectele legate de conformitate și, în special, o informează cu privire la stadiul plângerilor în termen de cel mult 90 de zile de la sesizare ([133]). Acest lucru le permite persoanelor vizate să înainteze plângeri legate de nerespectarea cadrului de către organizațiile CCD UE-SUA direct la APD națională a acestora, plângerile urmând să fie direcționate către DoC, în calitate de autoritate care gestionează CCD UE-SUA.

(79) În cazul în care, în baza verificărilor *ex officio*, a plângerilor sau a oricăror altor informații, DoC concluzionează că o organizație a încălcat în mod sistematic principiile, acesta poate elimina organizația respectivă de pe lista CCD ([134]). Refuzul unei organizații de a se supune unei decizii definitive a oricărui organism de autoreglementare în materie de protecție a vieții private, organism independent de soluționare a litigiilor sau organism guvernamental, inclusiv a unei APD, va fi considerat o încălcare sistematică ([135]).

(80) În al cincilea rând, o organizație CCD UE-SUA trebuie să se afle sub jurisdicția autorităților competente din SUA, în special FTC ([136]), care dispun de competențele necesare de investigare și de asigurare a respectării legii pentru a asigura respectarea efectivă a principiilor. FTC acordă prioritate sesizărilor privind nerespectarea principiilor primite de la organisme independente de soluționare a litigiilor sau de la organisme de autoreglementare, DoC și APD (care acționează din proprie inițiativă sau în urma unei plângeri) pentru a stabili dacă s-a încălcat secțiunea 5 din Legea FTC ([137]). 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, aceasta poate accepta plângeri direct de la persoanele în cauză și poate demara investigații privind CCD UE-SUA din proprie inițiativă, în special în cadrul unei investigații mai ample a unor aspecte legate de protecția vieții private.

([128]) Anexa I secțiunea III punctul 5 litera (c) subpunctul (ii).
([129]) A se vedea anexa III – secțiunea „Facilitarea cooperării cu APD”.
([130]) A se vedea anexa IV – secțiunile „Gestionarea cu prioritate a sesizărilor și realizarea investigațiilor” și „Cooperarea cu APD din UE în scopuri de asigurare a respectării legii”.
([131]) Anexa III – a se vedea, de exemplu, secțiunea „Facilitarea cooperării cu APD”.
([132]) Anexa I secțiunea II punctul 7 litera (e) și anexa III secțiunea „Facilitarea cooperării cu APD”.
([133]) *Ibidem*.
([134]) Anexa I secțiunea III punctul 11 litera (g).
([135]) Anexa I secțiunea III punctul 11 litera (g).
([136]) O organizație CCD UE-SUA 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 poate fi sancționată în temeiul secțiunii 5 din Legea privind FTC, care interzice practicile neloiale și frauduloase în domeniul comerțului sau care afectează comerțul.
([137]) A se vedea, de asemenea, angajamentele similare asumate de DoT – anexa V.

(81) În al șaselea rând, ca mecanism de recurs „de ultimă instanță”, în cazul în care niciuna dintre celelalte modalități de recurs disponibile nu a soluționat în mod satisfăcător o plângere, persoana vizată din Uniune poate recurge la procedura de arbitraj obligatoriu desfășurată de „comisia de arbitraj pentru Cadrul privind confidențialitatea datelor” („comisia de arbitraj CCD UE-SUA”) ([138]). Organizațiile trebuie să informeze persoanele cu privire la posibilitatea acestora de a recurge la o procedură de arbitraj obligatoriu, fiind obligate să răspundă atunci când o persoană a apelat la această opțiune transmițând o notificare în acest sens organizației în cauză ([139]).

(82) Această comisie de arbitraj CCD UE-SUA este formată dintr-un grup de cel puțin zece arbitri care vor fi desemnați de către DoC și Comisia Europeană 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 selectează din acest grup o comisie de arbitraj formată din unul sau trei ([140]) arbitri.

(83) Pentru desfășurarea procedurilor de arbitraj, DoC a selectat Centrul Internațional pentru Soluționarea Litigiilor (*International Centre for Dispute Resolution*) (ICDR), divizia internațională a Asociației Americane de Arbitraj (*American Arbitration Association*) (AAA). Procedurile desfășurate înaintea comisiei de arbitraj CCD UE-SUA vor fi reglementate de un set de norme de arbitraj convenite și un cod de conduită pentru arbitrii desemnați. Site-ul web al ICDR-AAA oferă persoanelor informații clare și concise cu privire la mecanismul de arbitraj și la procedura de depunere a cererilor de arbitraj.

(84) Normele de arbitraj convenite de DoC și Comisie completează CCD UE-SUA, care conține mai multe dispoziții ce vor spori posibilitățile de acces ale persoanelor vizate din Uniune 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 comisiei de arbitraj; (ii) deși arbitrajul va avea loc în Statele Unite, persoanele vizate din Uniune pot alege să participe prin teleconferință sau videoconferință, servicii care trebuie furnizate cu titlu gratuit persoanei în cauză; (iii) deși limba folosită în cadrul procedurii de arbitraj va fi limba engleză, în urma unei cereri motivate, serviciile de interpretare în cadrul ședinței de arbitraj și de traducere vor fi furnizate, în principiu, cu titlu gratuit persoanei vizate; (iv) în sfârșit, deși fiecare parte trebuie să suporte onorariul propriului avocat, în cazul în care este reprezentată de un avocat în fața comisiei de arbitraj, DoC va menține un fond alimentat din contribuțiile anuale ale organizațiilor CCD UE-SUA, care acoperă costurile procedurii de arbitraj până la o anumită valoare maximă, ce urmează să fie stabilită de către autoritățile din SUA în consultare cu Comisia ([141]).

(85) Comisia de arbitraj CCD UE-SUA are competența de a impune măsuri nemonetare, echitabile și personalizate ([142]) necesare pentru remedierea cazurilor de nerespectare a principiilor. Deși comisia de arbitraj va ține seama de alte măsuri reparatorii deja obținute prin alte mecanisme ale CCD UE-SUA la formularea soluției sale, persoanele pot, totuși, să recurgă la arbitraj dacă acestea consideră că respectivele măsuri sunt insuficiente. Acest lucru le va permite persoanelor vizate din Uniune să recurgă la procedura de arbitraj în toate cazurile în care, prin acțiunea sau lipsa de acțiune a acestora, organizațiile CCD UE-SUA, mecanismele independente de recurs sau autoritățile competente din SUA (de exemplu, FTC) nu au soluționat în mod satisfăcător plângerile înaintate. Nu se poate recurge la procedura de arbitraj dacă o APD deține competența legală de a soluționa plângerea în cauză cu privire la o organizație CCD UE-SUA, și anume în cazurile în care organizația respectivă fie este obligată să coopereze și să se conformeze avizului emis de APD în ceea ce privește prelucrarea datelor privind resursele umane colectate în contextul unui raport de muncă, fie s-a angajat voluntar să facă acest lucru. Persoanele în cauză pot pune în aplicare hotărârea arbitrală în instanțele din SUA în temeiul Legii federale privind arbitrajul (Federal Arbitration Act), asigurându-se astfel o cale de atac în cazul în care o organizație nu se conformează.

([138]) A se vedea anexa I la anexa I – „Modelul de arbitraj”.
([139]) A se vedea anexa I secțiunea II punctul 1 litera (a) subpunctul (xi) și secțiunea II punctul 7 litera (c).
([140]) Numărul de arbitri din comisia de arbitraj va trebui convenit de părți.
([141]) Anexa I anexa I secțiunea G punctul 6.
([142]) Persoanele nu pot solicita despăgubiri în cadrul procedurii de arbitraj, dar, în schimb, recurgerea la procedura de arbitraj nu exclude posibilitatea de a solicita despăgubiri în instanțele de drept comun din SUA.

(86) În al șaptelea rând, în cazul în care o organizație nu își îndeplinește angajamentul de a respecta principiile și politica de confidențialitate publicată, pot fi disponibile alte căi de atac judiciare în temeiul legislației SUA, inclusiv pentru a obține despăgubiri pentru prejudiciile suferite. De exemplu, persoanele au la dispoziție, în anumite condiții, căi de atac judiciare (putând obține inclusiv despăgubiri pentru prejudiciile suferite) în temeiul legislației la nivel de stat în materie de protecție a consumatorilor în cazurile de declarații false frauduloase sau de acte sau practici neloiale sau frauduloase ([143]) și în temeiul dreptului răspunderii civile (în special în cazul delictelor de violare a intimității ([144]), de uzurpare prin utilizarea numelui sau a imaginii ([145]) și de publicare a unor fapte cu caracter privat ([146])).

(87) Împreună, diferitele căi de atac descrise mai sus asigură faptul că fiecare plângere privind nerespectarea CCD UE-SUA de către organizațiile certificate va fi soluționată și remediată în mod eficace.

3. ACCESAREA ȘI UTILIZAREA DE CĂTRE AUTORITĂȚILE PUBLICE DIN STATELE UNITE ALE AMERICII A DATELOR CU CARACTER PERSONAL TRANSFERATE DIN UNIUNEA EUROPEANĂ

(88) Comisia a evaluat, de asemenea, limitările și garanțiile, inclusiv mecanismele de supraveghere și mecanismele individuale de recurs prevăzute în legislația Statelor Unite ale Americii în ceea ce privește colectarea și utilizarea ulterioară, din motive de interes public, de către autoritățile publice din SUA a datelor cu caracter personal transferate operatorilor și persoanelor împuternicite de operatori, în special în scopul asigurării respectării dreptului penal și în scopuri legate de securitatea națională („accesul autorităților") ([147]). Pentru a evalua dacă respectivele condiții de acces al autorităților la datele transferate către Statele Unite ale Americii în temeiul prezentei decizii îndeplinesc criteriul „echivalenței esențiale" în temeiul articolului 45 alineatul (1) din Regulamentul (UE) 2016/679, astfel cum a fost interpretat de Curtea de Justiție în lumina Cartei drepturilor fundamentale, Comisia a luat în considerare mai multe criterii.

(89) În special, orice restrângere a dreptului la protecția datelor cu caracter personal trebuie să fie prevăzută de lege și temeiul juridic care permite ingerința în acest drept trebuie să definească el însuși întinderea restrângerii exercitării dreptului vizat ([148]). În plus, pentru a îndeplini cerința proporționalității potrivit căreia derogările de la protecția datelor cu caracter personal și restrângerile acesteia trebuie să fie efectuate în limitele strictului necesar într-o societate democratică pentru a îndeplini obiective specifice de interes general echivalente cu cele recunoscute de Uniune, acest temei juridic trebuie să prevadă norme clare și precise care să reglementeze conținutul și aplicarea măsurilor respective și să impună o serie de cerințe minime, astfel încât persoanele ale căror date au fost transferate să dispună de garanții suficiente care să permită protejarea în mod eficient a datelor lor cu caracter personal împotriva riscurilor de abuz ([149]). În plus, aceste norme și garanții trebuie să fie obligatorii din punct de vedere

([143]) A se vedea, de exemplu, legislația la nivel de stat în materie de protecție a consumatorilor din California [Codul civil din California (*Cal. Civ. Code*) – articolele 1750-1785 – Legea privind căile de atac disponibile consumatorilor (West) – *(West) Consumers Legal Remedies Act*]; Districtul Columbia [Codul Districtului Columbia (*D.C. Code*) – articolele 28-3901]; Florida [Codul legislativ al Floridei (*Fla. Stat.*) – articolele 501.201-501.213 – Legea privind practicile comerciale frauduloase și neloiale (*Deceptive and Unfair Trade Practices Act*)]; Illinois [titlul 815 din Codul legislativ compilat al statului Illinois (*Ill. Comp. Stat.*) – articolele 505/1-505/12 – Legea privind frauda și practicile comerciale frauduloase la adresa consumatorilor (*Consumer Fraud and Deceptive Business Practices Act*)]; Pennsylvania [titlul 73 din Codul legislativ adnotat din Pennsylvania (Pa. Stat. Ann.) – articolele 201-1-201-9.3 – Legea privind practicile comerciale neloiale și protecția consumatorilor (West) – (*West*) *Unfair Trade Practices and Consumer Protection Law*].

([144]) Și anume în cazul unei ingerințe intenționate în activitățile sau preocupările private ale unei persoane, într-un mod care ar fi extrem de ofensator pentru o persoană rezonabilă (Al doilea tratat în materia răspunderii civile – articolul 652 litera (b) [*Restatement (2nd) of Torts*]).

([145]) Acest delict intervine în mod obișnuit în cazul uzurpării prin utilizarea numelui sau a imaginii unei persoane pentru a face publicitate unei activități comerciale sau unui produs sau în scopuri comerciale similare (a se vedea Al doilea tratat în materia răspunderii civile – articolul 652C).

([146]) Și anume atunci când informațiile privind viața privată a unei persoane sunt făcute publice, iar acest lucru este extrem de ofensator pentru o persoană rezonabilă și informațiile respective nu vizează o preocupare legitimă a publicului [a se vedea Al doilea tratat în materia răspunderii civile – articolul 652D].

([147]) Acest lucru este relevant și în lumina anexei I secțiunii I punctul 5. În conformitate cu această secțiune și în mod similar cu RGPD, respectarea cerințelor în materie de protecție a datelor și a drepturilor care fac parte din principiile privind protecția vieții private poate fi supusă unor limitări. Cu toate acestea, astfel de limitări nu sunt absolute, ci pot fi invocate doar în mai multe condiții, de exemplu în măsura necesară pentru a respecta o hotărâre judecătorească sau pentru a îndeplini cerințe de interes public, de asigurare a respectării legii sau de securitate națională. În acest context și din motive de claritate, această secțiune se referă, de asemenea, la condițiile stabilite în OE nr. 14086 care sunt evaluate, printre altele, în considerentele 127-141.

([148]) A se vedea Hotărârea Schrems II, punctele 174-175 și jurisprudența citată. A se vedea, de asemenea, în ceea ce privește accesul autorităților publice ale statelor membre, cauza C-623/17, Privacy International, ECLI:EU:C:2020:790, punctul 65 și cauzele conexate C-511/18, C-512/18 și C-520/18, La Quadrature du Net și alții, ECLI:EU:C:2020:791, punctul 175.

([149]) A se vedea Hotărârea Schrems II, punctele 176 și 181, precum și jurisprudența citată. A se vedea, de asemenea, în ceea ce privește accesul autorităților publice ale statelor membre, cauzele Privacy International, punctul 68 și La Quadrature du Net și alții, punctul 132.

juridic și opozabile din perspectiva persoanelor ([150]). În special, persoanele vizate trebuie să dispună de posibilitatea de a exercita căi legale în fața unei instanțe judecătorești independente și imparțiale pentru a avea acces la date cu caracter personal care le privesc sau pentru a obține rectificarea sau ștergerea unor astfel de date ([151]).

3.1 **Accesarea și utilizarea datelor de către autoritățile publice din SUA în scopul asigurării respectării dreptului penal**

(90) Referitor la ingerințele privind datele cu caracter personal transferate în temeiul CCD UE-SUA în scopuri legate de asigurarea respectării dreptului penal, legislația Statelor Unite ale Americii impune o serie de limitări privind accesarea și utilizarea datelor cu caracter personal și prevede mecanisme de supraveghere și de recurs în concordanță cu cerințele menționate în considerentul 89 din prezenta decizie. Condițiile în care poate avea loc o astfel de accesare și garanțiile aplicabile utilizării acestor competențe sunt evaluate în detaliu în secțiunile următoare. În acest sens, guvernul SUA [prin intermediul Departamentului de Justiție – DoJ (*Department of Justice*)] a oferit, de asemenea, asigurări cu privire la limitările și garanțiile aplicabile (anexa VI la prezenta decizie).

3.1.1 ***Temeiuri juridice, limitări și garanții***

3.1.1.1 *Limitări și garanții în ceea ce privește colectarea datelor cu caracter personal în scopul asigurării respectării dreptului penal*

(91) Datele cu caracter personal prelucrate de organizații certificate din SUA care ar urma să fie transferate din Uniune în temeiul CCD UE-SUA pot fi accesate în scopul asigurării respectării dreptului penal de către procurorii federali și agenții federali de investigații din SUA în cadrul unor proceduri diferite, astfel cum se explică mai detaliat în considerentele 92-99. Aceste proceduri se aplică în același mod atunci când se obțin informații de la orice organizație din SUA, fără a ține cont de cetățenia sau locul de reședință al persoanelor vizate în cauză ([152]).

(92) În primul rând, la cererea unui agent federal de aplicare a legii sau a unui avocat al guvernului, un judecător poate emite un mandat de percheziție sau punere sub sechestru (inclusiv a informațiilor stocate electronic) ([153]). Un astfel de mandat poate fi emis numai dacă există „o cauză probabilă" ([154]) pentru posibilitatea de identificare, în locul specificat în mandat, a unor „bunuri care pot fi puse sub sechestru" (dovada unei infracțiuni, obiecte deținute ilegal sau bunuri concepute sau destinate utilizării ori utilizate pentru comiterea unei infracțiuni). Mandatul trebuie să identifice bunul sau obiectul care urmează să fie pus sub sechestru și să desemneze judecătorul căruia trebuie să îi

([150]) A se vedea hotărârea Schrems II, punctele 181-182.

([151]) A se vedea hotărârea Schrems I, punctul 95 și Hotărârea Schrems II, punctul 194. În acest sens, CJUE a subliniat în special faptul că respectarea articolului 47 din Carta drepturilor fundamentale, care garantează dreptul la o cale de atac eficientă în fața unei instanțe judecătorești independente și imparțiale, „participă de asemenea la nivelul de protecție impus în cadrul Uniunii [și] trebuie să fie constatată de Comisie înainte ca aceasta să adopte o decizie privind caracterul adecvat al nivelului de protecție în temeiul articolului 45 alineatul (1) din [Regulamentul (UE) 2016/679]" (Hotărârea Schrems II, punctul 186).

([152]) A se vedea anexa VI. A se vedea, de exemplu, în legătură cu Legea privind interceptarea comunicațiilor (*Wiretap Act*), Legea privind comunicațiile stocate (Stored Communications Act) și Legea privind interceptarea (*Pen Register Act*) (menționate mai detaliat în considerentele 95-98), Suzlon Energy Ltd/Microsoft Corp., 671 F.3d 726, 729 (al nouălea circuit, 2011).

([153]) Norma 41 din Codul federal de procedură penală (*Federal Rules of Criminal Procedure*). Într-o hotărâre din 2018, Curtea Supremă a SUA a confirmat că autoritățile de aplicare a legii necesită un mandat de percheziție sau o renunțare la prezentarea unui mandat pentru a avea acces la istoricul de localizare al celulelor, care oferă o imagine de ansamblu cuprinzătoare asupra deplasărilor unui utilizator și că utilizatorul se poate aștepta în mod rezonabil la respectarea vieții private în ceea ce privește aceste informații [Timothy Ivory Carpenter/Statele Unite ale Americii, nr. 16-402, 585 U.S. (2018)]. Prin urmare, astfel de date nu pot fi obținute, în general, de la o societate de servicii celulare în temeiul unui ordin judecătoresc plecându-se de la motive rezonabile pentru a se considera că informațiile sunt relevante și semnificative pentru o investigare în curs, ci este necesar să se demonstreze existența unei cauze probabile atunci când se utilizează un mandat.

([154]) Potrivit Curții Supreme, „cauza probabilă" este un standard „practic, netehnic" care se bazează pe „considerațiile factuale și practice din viața de zi cu zi în conformitate cu care acționează persoanele rezonabile și prudente […]" [Illinois/Gates, 462 U.S 213, 232 (1983)]. În ceea ce privește mandatele de percheziție, există o cauză probabilă atunci când există o probabilitate justă ca o percheziție să conducă la descoperirea unor elemente de probă privind comiterea unei infracțiuni (id).

fie returnat mandatul. O persoană care face obiectul unei percheziții sau ale cărei bunuri fac obiectul unei percheziții poate solicita invalidarea elementelor de probă obținute sau rezultate în urma unei percheziții ilegale în cazul în care se aduc astfel de probe împotriva persoanei respective în cursul unui proces penal ([155]). În cazul în care un deținător de date (de exemplu, o societate) este obligat să divulge date în temeiul unui mandat, acesta poate contesta în special cerința de divulgare a datelor ca fiind nejustificat de împovărătoare ([156]).

(93) În al doilea rând, un mare juriu (o divizie de anchetă a instanței convocată de un judecător sau de un magistrat) poate emite o citație în contextul investigațiilor privind anumite infracțiuni grave ([157]), de obicei la cererea unui procuror federal, pentru a solicita unei persoane să prezinte sau să pună la dispoziție documente comerciale, informații stocate electronic sau alte elemente tangibile. În plus, diferite legi autorizează utilizarea unor citații administrative pentru a prezenta sau a pune la dispoziție documente comerciale, informații stocate electronic sau alte elemente tangibile în investigații care implică fraudarea serviciilor de sănătate, abuzuri împotriva copiilor, protecția Serviciului Secret, cazuri care implică substanțe controlate și investigații ale inspectorului general ([158]). În ambele cazuri, informațiile trebuie să fie relevante pentru investigație și citația nu poate fi nerezonabilă, și anume excesiv de cuprinzătoare, abuzivă sau împovărătoare (putând fi contestată de persoana pe care o vizează din aceste motive) ([159]).

(94) Condiții foarte similare se aplică în cazul citațiilor administrative emise pentru a obține acces la datele deținute de societăți din SUA în scopuri civile sau de reglementare („interes public"). Autoritatea agențiilor cu responsabilități civile și de reglementare de a emite aceste citații administrative trebuie să fie stabilită prin lege. Utilizarea unei citații administrative face obiectul unui „test privind caracterul rezonabil", care impune ca investigația să fie efectuată în conformitate cu un scop legitim, ca informațiile solicitate în temeiul citației să fie relevante pentru scopul respectiv, ca agenția să nu dispună deja de informațiile pe care le solicită prin citație și ca măsurile administrative necesare pentru emiterea citației să fi fost urmate ([160]). Jurisprudența Curții Supreme a clarificat, de asemenea, necesitatea de a asigura un echilibru între importanța interesului public în ceea ce privește informațiile solicitate și importanța intereselor personale și organizaționale în materie de confidențialitate ([161]). Cu toate că utilizarea unei citații administrative nu este supusă unei autorizări judiciare prealabile, aceasta ajunge să fie supusă controlului jurisdicțional în cazul contestării de către destinatar pe baza motivelor menționate mai sus sau în cazul în care agenția emitentă dorește să aplice citația în instanță ([162]). Pe lângă aceste limitări generale, din statut pot rezulta cerințe specifice (mai stricte) ([163]).

([155]) Mapp/Ohio, 367 U.S. 643 (1961).

([156]) A se vedea cauza cu privire la o cerere înaintată de Statele Unite ale Americii, 610 F.2d 1148, 1157 (al treilea circuit 1979) (în care s-a statuat că, „pentru respectarea garanțiilor procedurale, este necesar să aibă loc o audiere cu privire la caracterul împovărător al unei măsuri înainte de a obliga o societate de telefonie să furnizeze" asistență în baza unui mandat de percheziție) și cauza cu privire la o cerere a Statelor Unite ale Americii, 616 F.2d 1122 (al nouălea circuit 1980).

([157]) Al cincilea amendament la Constituția SUA impune punerea sub acuzare de către un mare juriu pentru orice „infracțiune capitală sau infracțiune gravă de altă natură". Marele juriu este format din 16 până la 23 de membri și stabilește dacă există o cauză probabilă pentru a se considera că s-a comis o infracțiune. Pentru a ajunge la această concluzie, marile jurii sunt învestite cu competențe de investigare care le permit să emită citații.

([158]) A se vedea anexa VI.

([159]) Norma 17 din Codul federal de procedură penală.

([160]) Statele Unite ale Americii/Powell, 379 U.S. 48 (1964).

([161]) Oklahoma Press Publishing Co./Walling, 327 U.S. 186 (1946).

([162]) Curtea Supremă a clarificat faptul că, în cazul contestării unei citații administrative, o instanță trebuie să analizeze dacă (1) investigația are un scop autorizat în mod legal, (2) competența de citare în cauză îi aparține Congresului și (3) „documentele solicitate sunt relevante pentru anchetă". Curtea a menționat, de asemenea, că o cerere de citație administrativă trebuie să fie „rezonabilă", și anume să impună „specificarea documentelor care trebuie prezentate în mod adecvat, dar nu excesiv, în scopul anchetei relevante", inclusiv „particularitatea în ceea ce privește «descrierea spațiului care urmează să fie percheziționat, persoanele care urmează să fie arestate sau obiectele care urmează să fie confiscate»".

([163]) De exemplu, Legea privind dreptul la confidențialitatea informațiilor financiare conferă unei autorități guvernamentale competența de a obține evidențe financiare deținute de o instituție financiară în temeiul unei citații administrative numai în cazul în care (1) există motive să se considere că evidențele solicitate sunt relevante pentru o anchetă legitimă de asigurare a respectării legii și (2) clientului i s-a furnizat o copie a citației sau a somației, împreună cu o notificare care precizează, cu specificitate rezonabilă, natura anchetei (titlul 12 articolul 3405 din U.S.C.). Un alt exemplu este Legea privind raportarea echitabilă a creditelor, care interzice agențiilor de raportare a consumatorilor să divulge rapoartele consumatorilor ca răspuns la cererile de citație administrativă (și le permite să răspundă doar cererilor de citație ale marelui juriu sau ordinelor judecătorești, titlul 15 articolul 1681 și următoarele din U.S.C.). În ceea ce privește accesul la informațiile privind comunicațiile, se aplică cerințele specifice prevăzute în Legea privind comunicațiile stocate, inclusiv în ceea ce privește posibilitatea de a utiliza citații administrative (a se vedea considerentele 96-97 pentru o prezentare detaliată).

(95) În al treilea rând, mai multe temeiuri juridice le permit autorităților de aplicare a dreptului penal să obțină acces la datele privind comunicațiile. O instanță poate emite un ordin de autorizare a colectării în timp real a unor informații care nu vizează conținutul privind apelarea, rutarea, adresarea și transmiterea semnalelor cu privire la un număr de telefon sau un o adresă de e-mail [prin utilizarea unui dispozitiv de interceptare (*pen register*) sau a unui dispozitiv de capturare și trasabilitate (*trap and trace*)], în cazul în care constată că autoritatea a certificat faptul că informațiile care ar putea fi obținute sunt relevante pentru o investigare în curs ([164]). Ordinul trebuie, printre altele, să precizeze identitatea suspectului, dacă este cunoscută, atributele comunicațiilor cărora li se aplică și o precizare a infracțiunii la care se referă informațiile care urmează să fie colectate. Utilizarea unui dispozitiv de interceptare sau a unui dispozitiv de capturare și trasabilitate poate fi autorizată pentru o perioadă maximă de șaizeci de zile, care poate fi prelungită numai printr-un nou ordin judecătoresc.

(96) În plus, accesarea în scopuri de asigurare a respectării dreptului penal a informațiilor privind abonații, traficul și conținutul stocat al comunicațiilor deținute de furnizorii de servicii de internet, societățile de telefonie sau alți furnizori de servicii terți pot fi obținute în temeiul Legii privind comunicațiilor stocate ([165]). Pentru a obține conținutul stocat al comunicațiilor electronice, autoritățile de aplicare a dreptului penal trebuie, în principiu, să obțină un mandat din partea unui judecător în temeiul unei cauze probabile pentru a se considera că acel cont conține elemente de probă privind comiterea unei infracțiuni ([166]). Pentru informațiile de înregistrare ale abonaților, adresele IP și marcajele temporale asociate, precum și informațiile privind facturarea, autoritățile de aplicare a dreptului penal pot utiliza o citație. Pentru majoritatea celorlalte informații stocate care nu vizează conținutul, cum ar fi antetul mesajelor electronice fără includerea câmpului care conține subiectul, o autoritate de aplicare a dreptului penal trebuie să obțină un ordin judecătoresc, care va fi emis dacă judecătorul este convins că există motive rezonabile pentru a se considera că informațiile solicitate sunt relevante și semnificative pentru o investigare în curs.

(97) Furnizorii care primesc solicitări în temeiul Legii privind comunicațiile stocate pot notifica în mod voluntar clientul sau abonatul ale cărui informații sunt solicitate, cu excepția cazului în care autoritatea de aplicare a dreptului penal competentă obține un ordin de protecție care interzice o astfel de notificare ([167]). Un astfel de ordin de protecție este un ordin judecătoresc prin care se impune unui furnizor de servicii de comunicații electronice sau de servicii informatice la distanță căruia i se adresează un mandat, o citație sau un ordin judecătoresc să nu notifice nicio altă persoană cu privire la existența mandatului, a citației sau a ordinului judecătoresc, atât timp cât instanța consideră necesar. Ordinele de protecție se emit în cazul în care o instanță constată că există motive pentru a se considera că notificarea ar pune în pericol în mod semnificativ o investigație sau ar întârzia în mod nejustificat un proces, de exemplu, deoarece ar duce la punerea în pericol a vieții sau a siguranței fizice a unei persoane, la sustragerea de la urmărirea penală, la intimidarea potențialilor martori etc. Un memorandum al procurorului general adjunct (care este obligatoriu pentru toți procurorii și agenții DoJ) impune procurorilor să se pronunțe în detaliu cu privire la necesitatea unui ordin de protecție și să furnizeze o justificare instanței cu privire la modul în care sunt îndeplinite criteriile legale pentru obținerea unui ordin de protecție în cazul respectiv ([168]). Memorandumul impune, de asemenea, ca solicitările ordinelor de protecție să nu urmărească, în general, să amâne transmiterea notificării cu mai mult de un an. În cazul în care, în circumstanțe excepționale, ar putea fi necesare ordine cu o durată mai lungă, acestea pot fi solicitate numai cu acordul scris al unui supraveghetor desemnat de procurorul SUA sau de procurorul general adjunct corespunzător. În plus, la încheierea unei investigații, procurorul trebuie să evalueze imediat dacă există un temei pentru menținerea oricăror ordine de protecție în curs și, în cazul în care nu există un astfel de temei, să pună capăt ordinului de protecție și să se asigure că furnizorul de servicii este informat cu privire la aceasta ([169]).

([164]) Titlul 18 articolul 3123 din U.S.C.

([165]) Titlul 18 articolele 2701-2713 din U.S.C.

([166]) Titlul 18 articolul 2701 literele (a)-(b) punctul 1 partea A din U.S.C. În cazul în care abonatul sau clientul în cauză este informat (fie în prealabil, fie, în anumite circumstanțe, printr-o notificare transmisă cu întârziere), informațiile care vizează conținutul stocate pentru o perioadă mai mare de 180 de zile pot fi obținute, de asemenea, pe baza unei citații administrative sau a unei citații emise de un mare juriu [titlul 18 articolul 2701 litera (b) punctul 1 partea B din U.S.C.] sau a unui ordin judecătoresc [în cazul în care există motive întemeiate pentru a se considera că informațiile sunt relevante și semnificative pentru o investigare în curs [titlul 18 articolul 2701 litera (d) din U.S.C.]. Cu toate acestea, în conformitate cu o hotărâre a unei instanțe federale de apel, anchetatorii guvernamentali obțin, în general, mandate de percheziție din partea judecătorilor pentru a colecta conținutul comunicațiilor private sau datele stocate de la un furnizor de servicii de comunicații comerciale. Statele Unite ale Americii/Warshak, 631 F.3d 266 (al șaselea circuit 2010).

([167]) Titlul 18 articolul 2705 litera (b) din U.S.C.

([168]) A se vedea memorandumul emis de procurorul general adjunct Rod Rosenstein la 19 octombrie 2017 referitor la o politică mai restrictivă privind solicitările de ordine de protecție (sau de nedivulgare), disponibil la adresa: https://www.justice.gov/criminal-ccips/page/file/1005791/download.

([169]) Memorandumul emis de procurorul general adjunct Lisa Moncao la 27 mai 2022 referitor la o politică suplimentară privind solicitările de ordine de protecție în temeiul titlului 18 articolul 2705 litera (b) din U.S.C.

(98) De asemenea, autoritățile de aplicare a dreptului penal pot intercepta în timp real comunicații telefonice, orale sau electronice în baza unui ordin judecătoresc prin care un judecător constată, printre altele, că există o cauză probabilă pentru a se considera că interceptarea convorbirilor telefonice sau interceptarea comunicațiilor electronice va face dovada unei infracțiuni federale sau va dezvălui locul în care se află un fugar care se sustrage de la urmărirea penală ([170]).

(99) Mai multe politici și orientări ale Departamentului de Justiție oferă măsuri de protecție suplimentare, inclusiv Orientările procurorului general cu privire la operațiunile interne ale FBI (AGG-DOM), care, printre altele, impun ca Biroul Federal de Investigații (FBI) să utilizeze metodele de investigație cel mai puțin intruzive fezabile, ținând seama de efectul asupra vieții private și a libertăților civile ([171]).

(100) Potrivit declarațiilor guvernului SUA, se aplică nivelurile de protecție similare sau mai ridicate menționate mai sus pentru investigațiile în scopul asigurării respectării legii la nivel de stat (cu privire la investigațiile desfășurate în temeiul legislației la nivel de stat) ([172]). În special, dispozițiile constituționale, precum și legile și jurisprudența la nivel de stat reafirmă nivelurile de protecție menționate mai sus împotriva percheziților și sechestrelor nerezonabile, impunând emiterea unui mandat de percheziție ([173]). În mod similar nivelurilor de protecție acordate la nivel federal, mandatele de percheziție pot fi emise numai la prezentarea unei suspiciuni rezonabile și trebuie să descrie spațiul care urmează să fie percheziționat și persoanele care urmează să fie arestate sau obiectele care urmează să fie confiscate ([174]).

([170]) Titlul 18 articolele 2510-2522 din U.S.C.

([171]) *Attorney General's Guidelines for Domestic Federal Bureau of Investigation (FBI) Operations* [Orientările procurorului general cu privire la operațiunile interne ale Biroului Federal de Investigații (FBI)] (septembrie 2008), disponibil la adresa http://www.justice.gov/archive/opa/docs/guidelines.pdf. Norme și politici suplimentare care impun limitări asupra activităților de investigare ale procurorilor federali sunt stabilite în *United States Attorneys' Manual* (Manualul procurorilor americani), disponibil la adresa http://www.justice.gov/usam/united-states-attorneys-manual. Pentru orice abatere de la aceste orientări, trebuie să se obțină aprobarea prealabilă din partea directorului, a directorului adjunct sau directorului executiv adjunct al FBI desemnat de director, cu excepția cazului în care o astfel de aprobare nu poate fi obținută ținând seama de caracterul imediat sau gravitatea unei amenințări la adresa siguranței persoanelor sau a bunurilor ori la adresa securității naționale (caz în care directorul sau o altă persoană autorizată trebuie notificată cât mai curând posibil). În cazul nerespectării orientărilor, FBI trebuie să notifice DoJ în acest sens, care, la rândul său, informează procurorul general și procurorul general adjunct.

([172]) A se vedea nota de subsol 2 din anexa VI. A se vedea, de exemplu, cauzele Arnold/City of Cleveland, 67 Ohio St.3d 35, 616 N.E.2d 163, 169 (1993) („În domeniul drepturilor individuale și al libertăților civile, Constituția Statelor Unite, atunci când se aplică statelor, prevede un prag sub care hotărârile instanțelor de stat nu pot coborî"); Cooper/California, 386 U.S. 58, 62, 87 S.Ct. 788, 17 L.Ed.2d 730 (1967) („Hotărârea noastră, desigur, nu afectează competența statului de a impune standarde pentru percheziții și confiscări mai ridicate decât cele impuse de Constituția federală, în cazul în care alege să facă acest lucru."); Petersen/City of Mesa, 63 P.3d 309, 312 (Ariz. Ct. App. 2003) („Deși Constituția Arizonei poate impune standarde mai stricte privind percheziții și confiscările decât Constituția federală, instanțele din Arizona nu pot oferi mai puțină protecție decât cea oferită de cel de al patrulea amendament").

([173]) Majoritatea statelor au reprodus în constituțiile lor măsurile de protecție prevăzute în cel de al patrulea amendament. A se vedea Constituția Statului Alabama, articolul I punctul 5; Constituția Statului Alaska, articolul I punctul 14; 1; Constituția Statului Arkansas, articolul II punctul 15; Constituția Statului California, articolul I punctul 13; Constituția Statului Colorado, articolul II punctul 7; Constituția Statului Connecticut, articolul I punctul 7; Constituția Statului Delaware, articolul I punctul 6; Constituția Statului Florida, articolul I punctul 12; Constituția Statului Georgia, articolul I punctul I alineatul XIII; Constituția Statului Hawai, articolul I punctul 7; Constituția Statului Idaho, articolul I punctul 17; Constituția Statului Illinois, articolul I punctul 6; Constituția Statului Indiana, articolul I punctul 11; Constituția Statului Iowa, articolul I punctul 8; Constituția Statului Kansas, Declarația drepturilor punctul 15; Constituția Statului Kentucky, punctul 10; Constituția Statului Louisiana, articolul I punctul 5; Constituția Statului Maine, articolul I punctul 5; Constituția Statului Massachusetts, Declarația privind drepturile, articolul 14; Constituția Statului Michigan, articolul I punctul 11; Constituția Statului Minnesota, articolul I punctul 10; Constituția Statului Mississippi, articolul III punctul 23; Constituția Statului Missouri, articolul I punctul 15; Constituția Statului Montana, articolul II punctul 11; Constituția Statului Nebraska, articolul I punctul 7; Constituția Statului Nevada, articolul I punctul 18; Constituția Statului New Hampshire, punctul 1 articolul 19; Constituția Statului N.J., articolul II punctul 7; Constituția Statului New Mexico, articolul II punctul 10; Constituția Statului New York, articolul I punctul 12; Constituția Statului Dakota de Nord, articolul I punctul 8; Constituția Statului Ohio, articolul I punctul 14; Constituția Statului Oklahoma, articolul II punctul 30; Constituția Statului Oregon, articolul I punctul 9; Constituția Statului Pennsylvania, articolul I punctul 8; Constituția Statului Rhode Island, articolul I punctul 6; Constituția Statului Carolina de Sud, articolul I punctul 10; Constituția Statului Dakota de Sud, articolul VI punctul 11; Constituția Statului Tennessee, articolul I punctul 7; Constituția Statului Texas, articolul I punctul 9; Constituția Statului Utah, articolul I punctul 14; Constituția Statului Vermont, capitolul I articolul 11; Constituția Statului Virginia de Vest, articolul III punctul 6; Constituția Statului Wisconsin, articolul I punctul 11; Constituția Statului Wyoming, articolul I punctul 4. Altele (de exemplu, Maryland, Carolina de Nord și Virginia) au consacrat în constituțiile lor un limbaj specific privind mandatele care a fost interpretat pe cale judiciară pentru a oferi o protecție similară sau superioară celei oferite de cel de al patrulea amendament [a se vedea Declarația privind drepturile din Maryland, articolul 26; Constituția Statului Carolina de Nord, articolul I punctul 20; Constituția Statului Virginia, articolul I punctul 10 și jurisprudența relevantă, de exemplu Hamel/Statul, 943 A.2d 686, 701 (Md. Ct. Spec. App. 2008; Statul/Johnson, 861 S.E.2d 474, 483 (N.C. 2021) și Lowe/Commonwealth, 337 S.E.2d 273, 274 (Va. 1985)]. În cele din urmă, Arizona și Washington au dispoziții constituționale care protejează viața privată la un nivel mai general (Constituția Statului Arizona, articolul 2 punctul 8; Constituția Statului Washington, articolul I punctul 7), care au fost interpretate de instanțe ca oferind mai multe măsuri de protecție decât cea oferită de cel de al patrulea amendament [a se vedea, de exemplu, Statul/Bolt, 689 P.2d 519, 523 (Ariz. 1984), Statul/Ault, 759 P.2d 1320, 1324 (Ariz. 1988), Statul/Myrick, 102 Wn.2d 506, 511, 688 P.2d 151, 155 (1984), Statul/Young, 123 Wn.2d 173, 178, 867 P.2d 593, 598 (1994)].

([174]) A se vedea, de exemplu, articolul 1524,3 litera (b) din Codul penal al Californiei; normele 3.6-3.13 din Codul de procedură penală din Alabama; Secțiunea 10.79.035; Codul revizuit al Statului Washington; Capitolul 5 secțiunea 19.2-59, titlul 19.2 Procedura penală, Codul Statului Virginia.

3.1.1.2 *Utilizarea ulterioară a informațiilor colectate*

(101) În ceea ce privește utilizarea ulterioară a datelor colectate de autoritățile federale de aplicare a dreptului penal, diverse legi, orientări și standarde impun garanții specifice. Cu excepția instrumentelor specifice aplicabile activităților FBI (AGG-DOM și Ghidul FBI privind investigațiile și operațiunile interne), cerințele descrise în prezenta secțiune se aplică, în general, utilizării ulterioare a datelor de către orice autoritate federală, inclusiv a datelor accesate în scopuri civile sau de reglementare. Aceasta include cerințele care decurg din memorandumurile/regulamentele Biroului pentru Administrare și Buget, din Legea federală privind modernizarea gestionării securității informațiilor (Federal Information Security Management Modernization Act), din Legea privind guvernarea electronică (E-Government Act) și din Legea privind registrele federale (Federal Records Act).

(102) În conformitatea cu competența conferită de Legea Clinger-Cohen (*Clinger-Cohen Act*) (P.L. 104-106, Diviziunea E) și de Legea privind securitatea informatică din 1987 (*Computer Security Act*) (P.L. 100-235) Biroul pentru Administrare și Buget (*Office of Management and Budget*) (OMB) a emis Circulara nr. A-130 pentru a stabili orientări generale obligatorii, aplicabile tuturor agențiilor federale (inclusiv autorităților de aplicare a legii) atunci când prelucrează informații de identificare personală ([175]). În special, circulara impune tuturor agențiilor federale să „limiteze crearea, colectarea, utilizarea, prelucrarea, stocarea, gestionarea, diseminarea și divulgarea informațiilor de identificare personală la cele care sunt autorizate din punct de vedere legal, sunt relevante și sunt considerate în mod rezonabil necesare pentru îndeplinirea corespunzătoare a funcțiilor de agenție autorizată” ([176]). În plus, în măsura în care este rezonabil din punct de vedere practic, agențiile federale trebuie să se asigure că informațiile de identificare personală sunt exacte, relevante, oportune și complete și sunt reduse la minimul necesar pentru îndeplinirea corespunzătoare a funcțiilor unei agenții. La un nivel mai general, agențiile federale trebuie să instituie un program cuprinzător privind protecția vieții private pentru a asigura respectarea cerințelor aplicabile în materie de protecție a vieții private, să elaboreze și să evalueze politici de confidențialitate, precum și să gestioneze riscurile la adresa confidențialității, să mențină proceduri de detectare, documentare și raportare a incidentelor legate de respectarea vieții private, să dezvolte programe de sensibilizare cu privire la viața privată și de formare pentru angajați și contractanți și să instituie politici și proceduri pentru a se asigura că personalul este tras la răspundere în ceea ce privește respectarea cerințelor în materie de protecție a vieții private și a politicilor de confidențialitate ([177]).

(103) În plus, Legea privind guvernarea electronică (*E-Government Act*) ([178]) impune tuturor agențiilor federale (inclusiv autorităților de aplicare a dreptului penal) să instituie măsuri de protecție a securității informațiilor, care să fie proporționale cu riscul și amploarea prejudiciului care ar rezulta din accesul, utilizarea, divulgarea, perturbarea, modificarea sau distrugerea neautorizată a acestora, să aibă un responsabil-șef cu informațiile pentru a asigura respectarea cerințele de securitate a informațiilor și să realizeze o evaluare anuală independentă (de exemplu, prin intermediul unui inspector general, a se vedea considerentul 109) a programului și a practicilor lor de securitate a informațiilor ([179]). În mod similar, Legea privind registrele federale (*Federal Records Act*) (FRA) ([180]) și reglementările suplimentare ([181]) impun ca informațiile deținute de agențiile federale să facă obiectul unor garanții care să asigure integritatea fizică a informațiilor și protecția acestora împotriva accesului neautorizat.

(104) În temeiul competenței statutare federale, inclusiv al Legii federale privind modernizarea securității informațiilor din 2014 (*Federal Information Security Modernisation Act*), OMB și Institutul Național pentru Standarde și Tehnologie (*National Institute of Standards and Technology*) (NIST) au elaborat standarde care sunt obligatorii pentru agențiile federale (inclusiv pentru autoritățile de aplicare a dreptului penal) și care precizează în detaliu cerințele minime de securitate a informațiilor care trebuie instituite, inclusiv controale de acces, asigurarea sensibilizării și a formării, planificarea de contingență, răspunsul la incidente, instrumentele de audit și de responsabilitate, asigurarea integrității sistemului și a informațiilor, efectuarea de evaluări ale riscurilor la adresa vieții private și a securității etc. ([182]) În plus, în conformitate cu orientările OMB, toate agențiile federale (inclusiv autoritățile de aplicare a

([175]) Și anume „informații care pot fi utilizate pentru a distinge sau a stabili identitatea unei persoane, fie singure, fie în combinație cu alte informații care sunt legate sau pot fi legate de o anumită persoană”, a se vedea Circulara nr. A-130 a OMB, p. 33 (definiția „informațiilor de identificare personală”).

([176]) Circulara nr. A-130 a OMB – *Managing Information as a Strategic Resource* (Gestionarea informațiilor ca resursă strategică), apendicele II, *Responsibilities for Managing Personally Identifiable Information* (Responsabilități pentru gestionarea informațiilor de identificare personală), volumul 81 al Registrului Federal – p. 49 689 (28 iulie 2016), p. 17.

([177]) Apendicele II, punctul 5 literele (a)-(h).

([178]) Titlul 44 capitolul 36 din U.S.C.

([179]) Titlul 44 articolele 3544-3545 din U.S.C.

([180]) FAC, titlul 44 articolul 3105 din U.S.C.

([181]) Titlul 36 articolul 1228,150 și următoarele, articolul 1228,228 și apendicele A din Codul regulamentelor federale (*Code of Federal Regulations*).

([182]) A se vedea, de exemplu, Circulara nr. A-130 a OMB; NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* (Controale asupra securității și a confidențialității pentru sisteme informatice și organizații) (10 decembrie 2020) și *NIST Federal Information Processing Standards 200: Minimum Security Requirements for Federal Information and Information Systems* (Standardele federale de prelucrare a informațiilor aferente NIST 200: cerințe minime de securitate pentru informațiile și sistemele informatice federale).

dreptului penal) trebuie să mențină și să pună în aplicare un plan de gestionare a încălcărilor securității datelor, inclusiv în ceea ce privește răspunsul la astfel de încălcări și evaluarea riscurilor de prejudiciu ([183]).

(105) În ceea ce privește păstrarea datelor, FRA ([184]) impune agențiilor federale din SUA (inclusiv autorităților de aplicare a dreptului penal) să stabilească perioade de păstrare a evidențelor lor (după care aceste evidențe trebuie eliminate), care trebuie aprobate de Administrația Arhivelor și a Registrelor Naționale (*National Archives and Record Administration*) ([185]). Durata acestei perioade de păstrare este stabilită în funcție de diferiți factori, cum ar fi tipul de investigație, dacă elementele de probă sunt în continuare relevante pentru aceasta etc. În ceea ce privește FBI, AGG-DOM prevede că FBI trebuie să dispună de un astfel de plan de păstrare a evidențelor și să mențină un sistem care să poată recupera rapid stadiul și temeiul investigațiilor.

(106) În sfârșit, Circulara nr. A-130 a OMB conține, de asemenea, anumite cerințe privind diseminarea informațiilor de identificare personală. În principiu, diseminarea și divulgarea informațiilor de identificare personală trebuie să se limiteze la cele care sunt autorizate din punct de vedere legal, sunt relevante și sunt considerate în mod rezonabil necesare pentru îndeplinirea corespunzătoare a funcțiilor unei agenții ([186]). Atunci când fac schimb de informații de identificare personală cu alte entități guvernamentale, agențiile federale din SUA trebuie să impună, după caz, anumite condiții (inclusiv instituirea unor controale specifice asupra securității și a confidențialității) care să reglementeze prelucrarea informațiilor prin acorduri scrise (inclusiv contracte, acorduri privind utilizarea datelor, acorduri privind schimbul de informații și memorandumuri de înțelegere) ([187]). În ceea ce privește temeiurile în baza cărora pot fi diseminate informațiile, AGG-DOM și Ghidul FBI privind investigațiile și operațiunile interne ([188]), de exemplu, prevăd că FBI poate fi obligat prin lege să facă acest lucru (de exemplu, în temeiul unui acord internațional) sau că acesta este autorizat să disemineze informații în anumite circumstanțe, de exemplu, altor agenții din SUA, în cazul în care divulgarea este compatibilă cu scopul pentru care au fost colectate informațiile și este legată de responsabilitățile acestora; comisiilor din cadrul Congresului; agențiilor străine, în cazul în care informațiile au legătură cu responsabilitățile lor, iar diseminarea este în concordanță cu interesele Statelor Unite ale Americii; diseminarea este necesară în special pentru a proteja siguranța sau securitatea persoanelor sau a bunurilor sau pentru a proteja împotriva unei infracțiuni sau a unei amenințări la adresa securității naționale ori pentru a preveni o astfel de infracțiune, iar divulgarea este compatibilă cu scopul pentru care au fost colectate informațiile ([189]).

3.1.2 ***Supraveghere***

(107) Activitățile agențiilor federale de aplicare a dreptului penal fac obiectul supravegherii de către diferite organisme ([190]). Astfel cum se explică în considerentele 92-99, în majoritatea cazurilor, aceasta include o supraveghere prealabilă de către sistemul judiciar, care trebuie să autorizeze măsurile individuale de colectare înainte ca acestea să poată fi utilizate. În plus, alte organisme supraveghează diferite etape ale activităților desfășurate de autoritățile de aplicare a dreptului penal, inclusiv colectarea și prelucrarea datelor cu caracter personal. Împreună, aceste organisme judiciare și nejudiciare asigură faptul că autoritățile de aplicare a legii fac obiectul unei supravegheri independente.

([183]) Memorandumul nr. 17-12, „Preparing for and Responding to a Breach of Personally Identifiable Information" (Pregătirea pentru o încălcare a securității informațiilor de identificare personală și răspunsul la aceasta), disponibil la adresa https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf și Circulara nr. A-130 a OMB. De exemplu, procedurile de răspuns la cazurile de încălcare a securității datelor ale Departamentului de Justiție, *a se vedea* https://www.justice.gov/file/4336/download.

([184]) FRA, titlul 44 articolul 3101 și următoarele din U.S.C.

([185]) Administrația Arhivelor și a Registrelor Naționale deține competența de a evalua practicile de gestionare a evidențelor agențiilor și poate stabili dacă păstrarea în continuare a anumitor evidențe este justificată [titlul 44 articolul 2904 litera (c) și articolul 2906 din U.S.C.].

([186]) Secțiunea 5.f.1. litera (d) din Circulara nr. A-130 a OMB.

([187]) Punctul 3 litera (d) din apendicele I la Circulara nr. A-130 a OMB.

([188]) A se vedea, de asemenea, secțiunea 14 din Ghidul FBI privind investigațiile și operațiunile interne (Domestic Investigations and Operations Guide – DIOG).

([189]) AGG-DOM, secțiunea VI punctele B și C; secțiunea 14 din Ghidul FBI privind investigațiile și operațiunile interne (*Domestic Investigations and Operations Guide* – DIOG).

([190]) Mecanismele menționate în prezenta secțiune se aplică, de asemenea, colectării și utilizării datelor de către autoritățile federale în scopuri civile și de reglementare. Agențiile federale civile și de reglementare sunt supuse controlului inspectorilor lor generali și supravegherii din partea Congresului, inclusiv din partea Biroului pentru Responsabilitate Guvernamentală (Government Accountability Office), agenția de audit și de investigare a Congresului. Cu excepția cazului în care agenția are un responsabil desemnat pentru protecția vieții private și a libertăților civile – o funcție care se regăsește, de regulă, în cadrul unor agenții precum Departamentul de Justiție și Departamentul pentru Securitate Internă (DHS) ca urmare a responsabilităților lor în materie de aplicare a legii și de securitate națională – aceste atribuții revin înaltului funcționar al agenției pentru protecția vieții private (Senior Agency Official for Privacy – SAOP). Toate agențiile federale sunt obligate prin lege să desemneze un SAOP, care are responsabilitatea de a asigura respectarea de către agenție a legislației privind protecția vieții private și de a supraveghea aspectele conexe. A se vedea, de exemplu, OMB M-16-24, Rolul și desemnarea înalților funcționari ai agenției pentru protecția vieții private (2016).

(108) În primul rând, responsabilii pentru protecția vieții private și a libertăților civile există în cadrul mai multor departamente cu responsabilități în materie de asigurare a respectării dreptului penal ([191]). Deși competențele specifice ale acestor responsabili pot varia într-o anumită măsură în funcție de statutul care îi autorizează, acestea cuprind, de regulă, supravegherea procedurilor pentru a se asigura că departamentul/agenția în cauză 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/s-au încălcat dreptul la viață privată sau libertățile civile. Șefii fiecărui departament sau a fiecărei agenții trebuie să se asigure că responsabilii pentru protecția vieții private și a libertăților civile dispun de materialele și resursele necesare pentru a-și îndeplini mandatul, că au acces la orice material și personal necesar pentru îndeplinirea funcțiilor lor și că sunt informați și consultați cu privire la modificările de politică propuse ([192]). Responsabilii pentru protecția vieții private și a libertăților civile raportează periodic Congresului, inclusiv cu privire la numărul și natura plângerilor primite de către departament/agenție, punând la dispoziție și un rezumat al deciziilor luate în legătură cu astfel de plângeri, cu privire la evaluările și anchetele întreprinse și la impactul activităților desfășurate de aceștia ([193]).

(109) În al doilea rând, un inspector general independent supraveghează activitățile Departamentului de Justiție, inclusiv ale FBI ([194]). Inspectorii generali sunt independenți din punct de vedere legal ([195]) și sunt responsabili pentru efectuarea de investigații, audituri și inspecții independente ale programelor și operațiunilor departamentului. Aceștia au acces la toate evidențele, rapoartele, auditurile, analizele, documentele, dosarele, recomandările sau alte materiale relevante, dacă este necesar, prin intermediul unei citații și pot lua declarații ale martorilor ([196]). Deși inspectorii generali emit recomandări referitoare la măsuri de remediere fără caracter obligatoriu, în general, rapoartele lor, inclusiv cu privire la acțiunile subsecvente (sau lipsa acestora) ([197]) sunt făcute publice și transmise Congresului, care poate să își exercite, pe această bază, funcția de supraveghere (a se vedea considerentul 111) ([198]).

([191]) A se vedea titlul 42 articolul 2000ee-1 din U.S.C. Printre acestea se numără, de exemplu, Departamentul de Justiție, Departamentul pentru Securitate Internă (*Department of Homeland Security*) (DHS) și FBI. În plus, în cadrul DHS, un responsabil-șef pentru protecția vieții private are ca atribuții menținerea și consolidarea măsurilor de protecție a vieții private și promovarea transparenței în cadrul departamentului (titlul 6 articolul 142, secțiunea 222 din U.S.C.). Toate sistemele, tehnologiile, formularele și programele DHS care colectează date cu caracter personal sau au un impact asupra vieții private fac obiectul supravegherii de către responsabilul-șef pentru protecția vieții private, care are acces la toate evidențele, rapoartele, auditurile, analizele, documentele, dosarele, recomandările și alte materiale aflate la dispoziția departamentului și, dacă este necesar, prin intermediul unei citații. Responsabilul pentru protecția vieții private trebuie să raporteze anual Congresului cu privire la activitățile departamentului care afectează viața privată, inclusiv plângerile privind încălcarea vieții private.

([192]) Titlul 42 articolul 2000ee-1 litera (d) din U.S.C.

([193]) A se vedea titlul 42 articolul 2000ee-1 litera (f) punctele 1-2 din U.S.C. De exemplu, raportul responsabilului-șef pentru protecția vieții private și a libertăților civile din cadrul DoJ și al Biroului pentru protecția vieții private și a libertăților civile (*Office of Privacy and Civil Liberties*) pentru perioada octombrie 2020-martie 2021 arată că au fost efectuate 389 de evaluări asupra protecției vieții private, inclusiv a sistemelor informatice și a altor programe (https://www.justice.gov/d9/pages/attachments/2021/05/10/2021-4-21opclsection803reportfy20sa1_final.pdf).

([194]) În mod similar, în baza legii privind securitatea internă (*Homeland Security Act*) din 2002, s-a înființat un Birou al Inspectorului General (*Office of Inspector General*) în cadrul Departamentului de Securitate Internă.

([195]) Inspectorii generali au un mandat sigur și pot fi revocați din funcție doar de către președinte, care trebuie să comunice Congresului în scris motivele care justifică o astfel de măsură.

([196]) A se vedea articolul 6 din Legea privind inspectorii generali din 1978.

([197]) A se vedea în acest sens, de exemplu, prezentarea generală elaborată de Biroul Inspectorului General al DoJ cu privire la recomandările formulate de acesta și măsura în care acestea au fost puse în aplicare prin acțiuni subsecvente ale departamentelor și agențiilor, https://oig.justice.gov/sites/default/files/reports/22-043.pdf.

([198]) A se vedea articolul 4 alineatul (5) și articolul 5 din Legea privind inspectorii generali din 1978. De exemplu, Biroul Inspectorului General din cadrul Departamentului de Justiție a publicat recent raportul său semestrial adresat Congresului (1 octombrie 2021-31 martie 2022, https://oig.justice.gov/node/23596), care oferă o prezentare generală a auditurilor, a evaluărilor, a inspecțiilor, a analizelor speciale și a investigațiilor privind programele și operațiunile DoJ. Aceste activități au inclus o investigație asupra unui fost contractant cu privire la divulgarea ilegală a materialului obținut în urma supravegherii electronice (interceptarea comunicațiilor unei persoane) în cadrul unei investigații în curs, care a condus la condamnarea contractantului respectiv. Biroul Inspectorului General a efectuat, de asemenea, o investigație asupra programelor și practicilor de securitate a informațiilor ale agențiilor DoJ, care a inclus testarea eficacității politicilor, a procedurilor și a practicilor în materie de securitate a informațiilor ale unui subset reprezentativ din sistemele agențiilor.

(110) În al treilea rând, în măsura în care desfășoară activități de combatere a terorismului, departamentele cu responsabilități în materie de asigurare a respectării dreptului penal fac obiectul supravegherii de către Comitetul de supraveghere în materie de protecție a vieții private și a libertăților civile (*Privacy and Civil Liberties Oversight Board* – PCLOB), o agenție independentă din cadrul ramurii executive, reprezentând un consiliu bipartizan format din cinci membri numiți de președinte pentru un mandat fix de șase ani, cu aprobarea Senatului ([199]). În conformitate cu statutul său de constituire, PCLOB are responsabilități în domeniul politicilor de combatere a terorismului și al punerii în aplicare a acestora în vederea protejării vieții private și a libertăților civile. În cadrul evaluării efectuate, acesta poate avea acces la toate evidențele, rapoartele, auditurile, analizele, documentele, dosarele și recomandările, inclusiv la informații clasificate, poate desfășura interviuri și audia martori ([200]). Comitetul primește rapoarte de la responsabilii pentru protecția vieții private și a libertăților civile din mai multe departamente/agenții federale ([201]), poate emite recomandări pentru autoritățile guvernamentale și de aplicare a legii și prezintă rapoarte periodice către comisiile Congresului și către Președinte ([202]). Rapoartele comitetului, inclusiv cele adresate Congresului, trebuie puse la dispoziția publicului în cea mai mare măsură posibilă ([203]).

(111) În sfârșit, activitățile de aplicare a dreptului penal fac obiectul supravegherii de către comisii specifice din cadrul Congresului SUA (comisiile judiciare ale Camerei Reprezentanților și Senatului). Comisiile judiciare exercită o supraveghere periodică în diferite moduri, în special prin audieri, investigații, analize și rapoarte ([204]).

3.1.3 *Căi de atac*

(112) După cum s-a indicat, autoritățile de aplicare a dreptului penal trebuie, în majoritatea cazurilor, să obțină o autorizație judiciară prealabilă pentru a colecta date cu caracter personal. Deși acest lucru nu este necesar pentru citațiile administrative, acestea se limitează la situații specifice și vor face obiectul unui control jurisdicțional independent, cel puțin în cazul în care guvernul urmărește executarea în instanță. În special, persoanele vizate de citații administrative le pot contesta în instanță pe motiv că nu sunt rezonabile, și anume sunt excesiv de cuprinzătoare, abuzive sau împovărătoare ([205]).

(113) Persoanele pot, în primul rând, să depună cereri sau plângeri la autoritățile de aplicare a dreptului penal cu privire la prelucrarea datelor lor cu caracter personal. Aceasta include posibilitatea de a solicita accesul la datele cu caracter personal și corectarea acestora ([206]). În ceea ce privește activitățile legate de combaterea terorismului, persoanele pot depune, de asemenea, o plângere la responsabilii pentru protecția vieții private și a libertăților civile (sau la alți funcționari responsabili pentru protecția vieții private) din cadrul autorităților de aplicare a legii ([207]).

(114) În plus, legislația SUA pune la dispoziția persoanelor 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 ([208]). Aceste căi de atac prevăzute, printre altele, în special de Legea privind procedura administrativă (APA), de Legea privind libertatea de informare (*Freedom of Information Act*) (FOIA) și de Legea privind confidențialitatea comunicațiilor electronice (*Electronic Communications Privacy Act*) (ECPA) stau la dispoziția tuturor persoanelor, indiferent de cetățenia lor, sub rezerva condițiilor aplicabile.

([199]) Membrii comitetului trebuie selectați exclusiv pe baza calificărilor lor profesionale, a realizărilor, a statutului public, a competențelor deținute în domeniul libertăților civile și al vieții private, precum și pe baza experienței lor relevante, fără a se ține seama de afilierea lor politică. Comitetul nu poate avea, în nicio circumstanță, mai mult de trei membri care aparțin aceluiași partid politic. Pe durata mandatului în cadrul comitetului, o persoană care a fost numită membru al acestuia nu poate fi funcționar ales, funcționar sau angajat al guvernului federal, putând deține doar calitatea de membru al comitetului. A se vedea titlul 42 articolul 2000ee litera (h) din U.S.C.

([200]) Titlul 42 articolul 2000ee litera (g) din U.S.C.

([201]) A se vedea titlul 42 articolul 2000ee-1 litera (f) punctul 1 partea A subpunctul (iii) din U.S.C. Printre acestea se numără cel puțin Departamentul de Justiție, Departamentul Apărării, Departamentul pentru Securitate Internă, precum și orice alt departament, agenție sau element al ramurii executive desemnate de PCLOB drept adecvate ca arie de acoperire.

([202]) Titlul 42 articolul 2000ee litera (e) din U.S.C.

([203]) Titlul 42 articolul 2000ee litera (f) din U.S.C.

([204]) De exemplu, comisiile organizează audieri tematice [a se vedea, de exemplu, o audiere recentă a comisiei judiciare a Camerei Reprezentanților pe tema „raziilor digitale” (*digital dragnets*) – https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983], precum și audieri de supraveghere periodice, de exemplu a FBI și DoJ – a se vedea https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation; https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 și https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899.

([205]) A se vedea anexa VI.

([206]) Secțiunea 3 literele (a) și (f) din apendicele II la Circulara nr. A-130 a OMB, care impune agențiilor federale să asigure accesul și corectarea corespunzătoare la cererea persoanelor și să stabilească proceduri pentru primirea și soluționarea plângerilor și a cererilor legate de protecția vieții private.

([207]) A se vedea titlul 42 articolul 2000ee-1 din U.S.C în ceea ce privește, de exemplu, DoJ și Departamentul pentru Securitate Internă. A se vedea, de asemenea, Memorandumul M-16-24 al OMB, *Rolul și desemnarea înalților funcționari ai agenției pentru protecția vieții private*.

([208]) Mecanismele de recurs menționate în prezenta secțiune se aplică, de asemenea, colectării și utilizării datelor de către autoritățile federale în scopuri civile și de reglementare.

(115) În general, în temeiul dispozițiilor referitoare la controlul jurisdicțional din APA ([209]), „o persoană care este victima unui abuz juridic în urma acțiunilor agenției sau este afectată ori lezată într-un alt mod în urma acțiunilor agenției" are dreptul la un control jurisdicțional al acestora ([210]). Acest lucru include posibilitatea de a solicita instanței „să declare ilegale sau să anuleze acțiunile, 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" ([211]).

(116) Mai precis, titlul II din ECPA ([212]) prevede un sistem de drepturi legale în materie de protecție a vieții private și, prin urmare, reglementează accesul autorităților de aplicare a legii la conținutul comunicațiilor telefonice, orale sau electronice stocate de furnizori de servicii terți ([213]). Acesta incriminează accesul ilegal (și anume care nu a fost autorizat de o instanță sau care nu a fost permis în alt mod) la aceste comunicații și permite persoanelor afectate să intenteze o acțiune civilă într-o instanță federală din SUA pentru a solicita daune compensatorii și punitive, precum și măsuri reparatorii echitabile sau o hotărâre declarativă împotriva unui funcționar guvernamental care a săvârșit cu intenție astfel de acte ilicite sau împotriva Statelor Unite ale Americii.

(117) În plus, mai multe alte legi acordă persoanelor dreptul de a introduce acțiuni împotriva unei autorități publice sau a unui funcționar public din SUA cu privire la prelucrarea datelor lor cu caracter personal, precum Legea privind interceptarea comunicațiilor ([214]), Legea privind fraudele și abuzurile informatice (*Computer Fraud and Abuse Act*) ([215]), Legea federală privind acțiunile în răspundere civilă (*Federal Torts Claim Act*) ([216]), Legea privind dreptul la confidențialitatea informațiilor financiare (*Right to Financial Privacy Act*) ([217]) și Legea privind raportarea echitabilă a creditelor ([218]).

([209]) Titlul 5 articolul 702 din U.S.C.

([210]) În general, doar acțiunile „finale" ale agenției și nu „acțiunile preliminare, procedurale sau intermediare" ale acesteia fac obiectul unui control jurisdicțional. A se vedea titlul 5 articolul 704 din U.S.C.

([211]) Titlul 5 articolul 706 alineatul (2) partea A din U.S.C.

([212]) Titlul 18 articolele 2701-2712 din U.S.C.

([213]) 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 și (ii) servicii informatice la distanță, cum ar fi serviciile informatice de stocare sau de prelucrare.

([214]) Titlul 18 articolul 2510 și următoarele din U.S.C. În temeiul Legii privind interceptarea comunicațiilor (titlul 18 articolul 2520 din U. S.C), o persoană ale cărei comunicații telefonice, orale sau electronice sunt interceptate, divulgate sau utilizate în mod intenționat poate introduce o acțiune civilă pe motive de încălcare a acestei legi, inclusiv, în anumite circumstanțe, împotriva unei funcționar guvernamental sau împotriva Statelor Unite ale Americii. Pentru colectarea de informații care nu vizează conținutul (de exemplu, adresa IP, mesaje electronice trimise/primite), a se vedea, de asemenea, secțiunea consacrată dispozitivelor de interceptare și de capturare și trasabilitate de la titlul 18 (titlul 18 articolele 3121-3127 din U.S.C. și, pentru acțiunile civile, articolul 2707).

([215]) Titlul 18 articolul 1030 din U.S.C. 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 care aparține autorităților SUA sau orice alt calculator, inclusiv, în anumite circumstanțe, împotriva unui funcționar guvernamental.

([216]) Titlul 28 articolul 2671 și următoarele din U.S.C. În temeiul Legii federale privind acțiunile în răspundere civilă, o persoană poate introduce o acțiune în justiție, în anumite condiții, împotriva Statelor Unite ale Americii cu privire la „neglijența sau culpa ori omisiunea oricărui angajat guvernamental care a acționat în domeniul de aplicare al mandatului sau al contractului său de muncă."

([217]) Titlul 12 articolul 3401 și următoarele din U.S.C. În conformitate cu Legea privind dreptul la confidențialitatea informațiilor financiare, 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 autorităților la evidențe financiare protejate este, în general, interzis, cu excepția cazului în care acestea adresează cererea sub rezerva unei citații sau a unui mandat de percheziție legal 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.

([218]) Titlul 15 articolele 1681-1681x din U.S.C. În temeiul Legii privind raportarea echitabilă a creditelor, o persoană poate introduce o acțiune în justiție împotriva oricărei persoane care nu respectă cerințele (în special necesitatea unei autorizații legale) în ceea ce privește colectarea, diseminarea și utilizarea rapoartelor privind creditele de consum sau, în anumite condiții, împotriva unei agenții guvernamentale.

(118) De asemenea, în temeiul FOIA ([219]) și al titlului 5 articolul 552 din U.S.C., orice persoană are dreptul de a obține accesul la evidențele agențiilor federale, inclusiv în cazul în care acestea conțin datele cu caracter personal ale persoanei respective. După epuizarea căilor de atac administrative, orice persoană fizică poate invoca acest drept de acces în instanță, cu excepția cazului în care aceste evidențe sunt protejate împotriva divulgării publice printr-o derogare sau o excepție specială care vizează asigurarea respectării legii ([220]). În acest caz, instanța va evalua dacă se aplică vreo excepție sau dacă aceasta a fost invocată în mod legal de către autoritatea publică relevantă.

3.2 **Accesarea și utilizarea datelor de către autoritățile publice din SUA în scopuri legate de securitatea națională**

(119) Legislația Statelor Unite ale Americii conține diverse limitări și garanții în ceea ce privește accesarea și utilizarea datelor cu caracter personal în scopuri legate de securitatea națională și prevede mecanisme de supraveghere și de recurs care sunt în concordanță cu cerințele menționate în considerentul 89 din prezenta decizie. Condițiile în care pot fi accesate datele și garanțiile aplicabile utilizării acestor competențe sunt evaluate în detaliu în secțiunile următoare.

3.2.1 ***Temeiuri juridice, limitări și garanții***

3.2.1.1 *Cadrul juridic aplicabil*

(120) Datele cu caracter personal transferate din Uniune către organizațiile CCD UE-SUA pot fi colectate de autoritățile SUA în scopuri legate de securitatea națională în baza unor instrumente juridice diferite, sub rezerva îndeplinirii unor condiții și garanții specifice.

(121) Odată ce organizații din Statele Unite ale Americii au primit date cu caracter personal, serviciile de informații din SUA pot solicita accesul la aceste date numai în scopuri legate de securitatea națională, astfel cum este autorizat prin lege, în special în temeiul Legii privind supravegherea activităților străine de spionaj (*Foreign Intelligence Surveillance Act*) (FISA) sau al dispozițiilor legale care autorizează accesul prin intermediul scrisorilor privind securitatea națională (NSL) ([221]). FISA conține mai multe temeiuri juridice care pot fi utilizate pentru a colecta (și prelucra ulterior) datele cu caracter personal ale persoanelor vizate din Uniune transferate în temeiul CCD UE-SUA (secțiunea 105 din FISA ([222]), secțiunea 302 din FISA ([223]), secțiunea 402 din FISA ([224]), secțiunea 501 din FISA ([225]) și secțiunea 702 din FISA ([226])), după cum se menționează mai detaliat în considerentele 142-152.

([219]) Titlul 5 articolul 552 din U.S.C.

([220]) Aceste excepții sunt, totuși, limitate. De exemplu, în conformitate cu titlul 5 articolul 552 litera (b) punctul 7 din U.S.C., drepturile prevăzute de FOIA sunt excluse în cazul „evidențelor sau al informațiilor compilate în scopul asigurării respectării legii, însă numai în măsura în care prezentarea unor astfel de evidențe sau informații care vizează asigurarea respectării legii (A) ar putea în mod rezonabil să interfereze cu procedurile de asigurare a respectării legii, (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 a unei agenții sau autorități statale, locale sau străine sau a oricărei instituții private care furnizează informații în mod confidențial și, în cazul unor evidențe sau al unor informații compilate de o autoritate de aplicare a dreptului penal în cursul unei investigări sau de către o agenție care desfășoară o investigație legală de securitate națională, a informațiilor furnizate de o sursă confidențială, (E) ar dezvălui tehnici și proceduri referitoare la investigații care vizează asigurarea respectării legii sau urmăriri penale sau ar divulga orientările referitoare la investigații care vizează asigurarea respectării legii sau urmăriri penale, în cazul în care o astfel de divulgare ar putea conduce în mod rezonabil la riscul eludării legii sau (F) s-ar putea prevedea 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 evidențe [a căror prezentare ar putea în mod rezonabil să interfereze cu procedurile de asigurare a respectării legii] și (A) investigarea sau procedura respectivă implică o posibilă încălcare a dreptului penal și (B) există motive să se creadă că (i) persoana care face obiectul investigației sau al procedurii respective nu are cunoștință de desfășurarea acesteia și (ii) divulgarea existenței evidențelor respective ar putea în mod rezonabil să interfereze cu procedura de asigurare a respectării legii, agenția poate trata evidențele respective, numai atât timp cât această împrejurare continuă, ca nefăcând obiectul cerințelor prezentei secțiuni” [titlul 5 articolul 552 litera (c) punctul 1 din U.S.C.].

([221]) Titlul 12 articolul 3414 din U.S.C. Titlul 15 articolele 1681u-1681v din U.S.C. și titlul 18 articolul 2709 din U.S.C. A se vedea considerentul 153.

([222]) Titlul 50 articolul 1804 din U.S.C., care se referă la supravegherea electronică individualizată tradițională.

([223]) Titlul 50 articolul 1822 din U.S.C., care se referă la perchezițiile fizice efectuate în scopuri legate de obținerea de informații externe.

([224]) Titlul 50 articolul 1842, coroborat cu articolul 1841 alineatul (2) și titlul 18 secțiunea 3127 din U.S.C., care se referă la instalarea de dispozitive de interceptare sau de capturare și trasabilitate.

([225]) Titlul 50 articolul 1861 din U.S.C, care permite FBI să depună „o cerere de emitere a unui ordin care să autorizeze un transportator comun, o unitate publice de cazare, o unitate de depozitare fizică sau o unitate de închiriere de vehicule să elibereze evidențele aflate în posesia sa pentru o investigație în vederea colectării de informații externe sau pentru o investigație privind terorismul internațional”.

([226]) Titlul 50 articolul 1881a din U.S.C, care permite elementelor Comunității Serviciilor de Informații din SUA să solicite accesul la informații, inclusiv la conținutul comunicațiilor pe internet, de la societăți din SUA, care vizează anumite persoane care nu sunt cetățeni americani/rezidenți SUA din afara Statele Unite ale Americii, cu sprijinul impus în baza legii al furnizorilor de comunicații electronice.

(122) Serviciile de informații din SUA au, de asemenea, posibilitatea de a colecta date cu caracter personal în afara Statelor Unite ale Americii, astfel de date putând include date cu caracter personal aflate în tranzit între Uniune și Statele Unite ale Americii. Colectarea de date în afara Statelor Unite ale Americii are la bază Ordinul executiv nr. 12333 (OE nr. 12333) ([227]), emis de președinte ([228]).

(123) Colectarea de informații de tip SIGINT este forma de colectare de informații cea mai relevantă pentru prezenta constatare a caracterului adecvat, deoarece se referă la colectarea comunicațiilor electronice și a datelor din sistemele informatice. O astfel de colectare poate fi efectuată de serviciile de informații din SUA atât în Statele Unite ale Americii (în temeiul FISA), cât și în timp ce datele se află în tranzit către Statele Unite ale Americii (în temeiul OE nr. 12333).

(124) La 7 octombrie 2022, președintele SUA a emis OE nr. 14086 privind consolidarea garanțiilor pentru informațiile de tip SIGINT colectate de Statele Unite ale Americii, stabilind limitări și garanții pentru toate activitățile de colectare de informații de tip SIGINT ale Statelor Unite ale Americii. Acest ordin executiv înlocuiește, în mare măsură, Directiva nr. 28 privind politica prezidențială (*Presidential Policy Directive*) (PPD-28) ([229]), consolidează condițiile, limitările și garanțiile care se aplică tuturor activităților de colectare de informații de tip SIGINT (și anume pe baza FISA și a OE nr. 12333), indiferent de locul în care se desfășoară ([230]), și stabilește un nou mecanism de recurs prin care aceste garanții pot fi invocate și exercitate de către persoane ([231]) (a se vedea mai detaliat considerentele 176-194). Astfel, acesta pune în aplicare în legislația SUA rezultatul discuțiilor care au avut loc între UE și SUA în urma invalidării de către Curtea de Justiție a deciziei Comisiei privind caracterul adecvat al nivelului de protecție oferit de Scutul de confidențialitate (a se vedea considerentul 6). Prin urmare, acesta este un element deosebit de important al cadrului juridic evaluat în prezenta decizie.

(125) Limitările și garanțiile introduse prin OE nr. 14086 le completează pe cele prevăzute în secțiunea 702 din FISA și OE nr. 12333. Cerințele descrise mai jos (în secțiunile 3.2.1.2 și 3.2.1.3) trebuie să fie aplicate de serviciile de informații atunci când întreprind activități de colectare de informații de tip SIGINT în temeiul secțiunii 702 din FISA și al OE nr. 12333, de exemplu atunci când identifică/selectează categoriile de informații externe care urmează să fie obținute în temeiul secțiunii 702 din FISA; colectează informații sau contrainformații externe în conformitate cu OE nr. 12333 și și iau decizii individuale de direcționare în temeiul secțiunii 702 din FISA și al OE nr. 12333.

(126) În plus, cerințele prevăzute în acest ordin executiv emis de președinte sunt obligatorii pentru întreaga Comunitate a Serviciilor de Informații. Ele trebuie puse în aplicare în continuare prin politici și proceduri ale serviciilor, care le transpun în direcții concrete pentru operațiunile de zi cu zi. În acest sens, OE nr. 14086 oferă serviciilor de informații din SUA un termen maxim de un an pentru a-și actualiza politicile și procedurile existente (și anume până la 7 octombrie 2023) în vederea alinierii acestora la cerințele ordinului executiv. Aceste politici și proceduri actualizate trebuie să fie elaborate în consultare cu procurorul general, cu responsabilul pentru protecția libertăților civile din cadrul Biroului Directorului Serviciului Național de Informații (*Office of the Director of National Intelligence*) (CLPO ODNI) și cu PCLOB – un organism independent de supraveghere autorizat să revizuiască politicile ramurii executive și punerea în aplicare a acestora, în vederea asigurării protecției vieții private și a libertăților civile (a se vedea considerentul 110 în ceea ce privește rolul și statutul PCLOB) – și trebuie să fie puse la dispoziția publicului ([232]). În plus, odată ce politicile și procedurile actualizate sunt instituite, PCLOB va efectua o revizuire a acestora pentru a se asigura că sunt în concordanță cu dispozițiile ordinului executiv. În termen de 180 de zile de la

([227]) OE nr. 12333: *United States Intelligence Activities* (Activitățile de colectare de informații ale Statelor Unite ale Americii), Registrul Federal Vol. 40. nr. 235 (8 decembrie 1981, cu modificările aduse la 30 iulie 2008). OE nr. 12333 definește, la un nivel mai general, obiectivele, direcțiile, atribuțiile și responsabilitățile serviciilor de informații din SUA (inclusiv rolul diverselor elemente ale Comunității Serviciilor de Informații) și stabilește parametrii generali pentru desfășurarea activităților de colectare de informații.

([228]) În temeiul articolului II din Constituția SUA, responsabilitatea de a asigura securitatea națională, inclusiv, în special, de a colecta informații externe, îi revine președintelui, în calitate de comandant-șef al forțelor armate.

([229]) OE nr. 14086 înlocuiește o directivă prezidențială anterioară, și anume PPD-28, cu excepția secțiunii 3 și a unei anexe de completare (care impune serviciilor de informații să își revizuiască anual prioritățile și cerințele în materie de informații de tip SIGINT colectate, ținând seama de beneficiile activităților de colectare de informații de tip SIGINT pentru interesele naționale ale SUA, precum și de riscul prezentat de aceste activități) și secțiunea 6 (care conține dispoziții generale); a se vedea *National Security Memorandum on Partial Revocation of Presidential Policy Directive 28* (Memorandumul privind securitatea națională referitor la revocarea parțială a Directivei nr. 28 privind politica prezidențială, disponibil la adresa https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/national-security-memorandum-on-partial-revocation-of-presidential-policy-directive-28/.

([230]) A se vedea secțiunea 5 litera (f) din OE nr. 14086, care explică faptul că ordinul executiv are același domeniu de aplicare precum PPD-28, care, în conformitate cu nota sa de subsol 3, s-a aplicat activităților de colectare de informații de tip SIGINT desfășurate pentru a colecta comunicații sau informații cu privire la comunicații, cu excepția activităților de colectare de informații de tip SIGINT întreprinse pentru a testa sau a dezvolta capacități de colectare de informații de tip SIGINT.

([231]) A se vedea în acest sens, de exemplu, secțiunea 5 litera (h) din OE nr. 14086, care clarifică faptul că garanțiile din ordinul executiv creează un drept legal, putând fi exercitate de persoane prin intermediul mecanismului de recurs.

([232]) A se vedea secțiunea 2 litera (c) punctul (iv) partea C din OE nr. 14086.

finalizarea unei astfel de revizuiri de către PCLOB, fiecare serviciu de informații trebuie să analizeze cu atenție și să pună în aplicare sau să abordeze în alt mod toate recomandările PCLOB. La 3 iulie 2023, guvernul SUA a publicat versiuni actualizate ale acestor politici și proceduri ([233]).

3.2.1.2 *Limitări și garanții în ceea ce privește colectarea datelor cu caracter personal în scopuri legate de securitatea națională*

(127) OE nr. 14086 stabilește o serie de cerințe extinse care se aplică tuturor activităților de colectare de informații de tip SIGINT (colectarea, utilizarea, diseminarea etc. a datelor cu caracter personal).

(128) În primul rând, astfel de activități trebuie să aibă la bază un act legislativ sau o autorizație prezidențială și să fie întreprinse în conformitate cu legislația SUA, inclusiv cu Constituția ([234]).

(129) În al doilea rând, trebuie să existe garanții adecvate pentru a se asigura că viața privată și libertățile civile reprezintă considerente care fac parte integrantă din planificarea unor astfel de activități ([235]).

(130) În special, orice activitate de colectare de informații de tip SIGINT poate fi efectuată numai „după ce s-a stabilit, în baza unei evaluări rezonabile a tuturor factorilor relevanți, că activitățile sunt necesare pentru a promova o prioritate validată în materie de informații” (în ceea ce privește noțiunea de „prioritate validată în materie de informații”, a se vedea considerentul 135) ([236]).

(131) În plus, astfel de activități se pot desfășura numai „în măsura și într-un mod proporționale cu respectiva prioritate validată în materie de informații pentru care au fost autorizate acestea” ([237]). Cu alte cuvinte, trebuie să se ajungă la un echilibru adecvat „între importanța priorității în materie de informații urmărite și impactul asupra vieții private și a libertăților civile ale persoanelor afectate, indiferent de cetățenie sau de locul de reședință al acestora” ([238]).

(132) În sfârșit, pentru a asigura respectarea acestor cerințe generale – care reflectă principiile legalității, necesității și proporționalității – activitățile de colectare de informații de tip SIGINT fac obiectul supravegherii (pentru informații detaliate în acest sens, a se vedea secțiunea 3.2.2) ([239]).

(133) Aceste cerințe ample sunt justificate suplimentar în ceea ce privește colectarea de informații de tip SIGINT printr-o serie de condiții și limitări care asigură faptul că ingerința în drepturile persoanelor este limitată la ceea ce este necesar și proporțional pentru promovarea unui obiectiv legitim.

(134) În primul rând, ordinul executiv limitează temeiurile în baza cărora pot fi colectate date în cadrul activităților de colectare de informații de tip SIGINT în două moduri. Pe de o parte, ordinul executiv stabilește obiectivele legitime care pot fi urmărite prin colectarea de informații de tip SIGINT, de exemplu, pentru a înțelege sau a evalua capacitățile, intențiile sau activitățile organizațiilor străine, inclusiv ale organizațiilor teroriste internaționale, care reprezintă o amenințare efectivă sau potențială la adresa securității naționale a Statelor Unite ale Americii, pentru a asigura protecția împotriva capacităților și activităților militare străine și pentru a înțelege sau evalua amenințările transnaționale care au impact asupra securității mondiale, cum ar fi schimbările climatice și alte schimbări ecologice, riscurile pentru sănătatea publică și pericolul unor crize umanitare ([240]). Pe de altă parte, ordinul executiv enumeră anumite obiective care nu trebuie niciodată urmărite prin activități de colectare de informații de tip SIGINT, de exemplu, pentru a face dificilă exprimarea criticilor sau a opiniilor contrare sau exprimarea liberă a

([233]) https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguards-in-executive-order-14086.

([234]) Secțiunea 2 litera (a) punctul (i) din OE nr. 14086.

([235]) Secțiunea 2 litera (a) punctul (ii) din OE nr. 14086.

([236]) Secțiunea 2 litera (a) punctul (ii) partea A din OE nr. 14086. Acest lucru nu impune întotdeauna ca informațiile de tip SIGINT colectate să fie singurul mijloc de promovare a aspectelor legate de o prioritate validată în materie de informații. De exemplu, colectarea de informații de tip SIGINT poate fi utilizată pentru a asigura căi alternative de validare (de exemplu, pentru a corobora informațiile primite din alte surse de informații) sau pentru a menține un acces fiabil la aceleași informații [secțiunea 2 litera (c) punctul (i) partea A din OE nr. 14086].

([237]) Secțiunea 2 litera (a) punctul (ii) partea B din OE nr. 14086.

([238]) Secțiunea 2 litera (a) punctul (ii) partea B din OE nr. 14086.

([239]) Secțiunea 2 litera (a) punctul (iii), coroborată cu secțiunea 2 litera (d) din OE nr. 14086.

([240]) Secțiunea 2 litera (b) punctul (i) din OE nr. 14086. Ca urmare a faptului că lista delimitată a obiectivelor legitime din ordinul executiv nu cuprinde posibilele amenințări viitoare, ordinul executiv prevede posibilitatea ca președintele să actualizeze această listă în cazul în care intervin noi imperative de securitate națională, cum ar fi amenințări noi la adresa securității naționale. În principiu, astfel de actualizări trebuie să fie făcute publice, cu excepția cazului în care președintele stabilește că acest lucru ar reprezenta un risc pentru securitatea națională a Statelor Unite ale Americii [secțiunea 2 litera (b) punctul (i) partea B din OE nr. 14086].

ideilor sau a opiniilor politice de către persoane sau presă, pentru a dezavantaja persoane pe criterii legate de originea etnică, rasă, gen, identitate de gen, orientare sexuală sau religie sau pentru a oferi un avantaj competitiv societăților din SUA ([241]).

(135) În plus, pentru a justifica o colectare de informații de tip SIGINT, serviciile de informații nu pot invoca doar obiectivele legitime în sine prevăzute în OE nr. 14086; acestea trebuie să fie susținute în continuare, în scopuri operaționale, de priorități mai concrete pentru care pot fi colectate informații pe baza semnalelor electromagnetice. Cu alte cuvinte, colectarea efectivă poate avea loc numai pentru a promova o prioritate mai specifică. Aceste priorități sunt stabilite printr-un proces specific menit să asigure respectarea cerințelor legale aplicabile, inclusiv a celor referitoare la viața privată și la libertățile civile. Mai precis, prioritățile în materie de informații sunt mai întâi elaborate de directorul Serviciului Național de Informații (prin așa-numitul Cadru național privind prioritățile în materie de informații) și transmise președintelui spre aprobare ([242]). Înainte de a-i propune președintelui priorități în materie de informații, directorul trebuie, în conformitate cu OE nr. 14086, să obțină o evaluare din partea CLPO ODNI pentru fiecare prioritate pentru a stabili că (1) promovează unul sau mai multe obiective legitime enumerate în ordinul executiv, (2) nu a fost concepută pentru colectarea de informații de tip SIGINT având în vedere un obiectiv interzis enumerat în ordinul executiv și nici nu s-a prevăzut ca aceasta să conducă la o astfel de colectare și (3) a fost instituită după luarea în considerare în mod corespunzător a vieții private și a libertăților civile ale tuturor persoanelor, indiferent de cetățenie sau de locul de reședință al acestora ([243]). În cazul în care directorul nu este de acord cu evaluarea realizată de responsabilul pentru protecția libertăților civile, ambele puncte de vedere trebuie prezentate președintelui ([244]).

(136) Prin urmare, acest proces asigură în special luarea în considerare a aspectelor legate de confidențialitate încă din etapa inițială în care sunt elaborate prioritățile în materie de informații.

(137) În al doilea rând, odată ce a fost stabilită o prioritate în materie de informații, o serie de cerințe reglementează decizia dacă și în ce măsură pot fi colectate informații de tip SIGINT pentru a promova o astfel de prioritate. Aceste cerințe operaționalizează standardele ample de necesitate și proporționalitate prevăzute în secțiunea 2 litera (a) din ordinul executiv.

(138) În special, se pot colecta informații prin sisteme de tip SIGINT numai „după ce s-a stabilit, în baza unei evaluări rezonabile a tuturor factorilor relevanți, că respectiva colectare este necesară pentru a promova o prioritate specifică în materie de informații" ([245]). Pentru a stabili dacă o activitate de colectare de informații de tip SIGINT este necesară pentru a promova o prioritate validată în materie de informații, serviciile de informații din SUA trebuie să ia în considerare disponibilitatea, fezabilitatea și caracterul adecvat al altor surse și metode mai puțin intruzive, printre care se numără canalele diplomatice și sursele publice ([246]). Atunci când sunt disponibile, trebuie să se acorde prioritate acestor surse și metode alternative mai puțin intruzive ([247]).

(139) Atunci când, în aplicarea acestor criterii, colectarea de informații de tip SIGINT este considerată necesară, aceasta trebuie să fie „cât mai adaptată posibil" și „nu trebuie să aibă un impact disproporționat asupra vieții private și a libertăților civile" ([248]). Pentru a se asigura că viața privată și libertățile civile nu sunt afectate în mod disproporționat – și anume pentru a se ajunge la un echilibru adecvat între necesitățile în materie de securitate națională și protecția vieții private și a libertăților civile – toți factorii relevanți trebuie luați în considerare în mod corespunzător, cum ar fi natura obiectivului urmărit, caracterul intruziv al activității de colectare, inclusiv durata acesteia, contribuția probabilă a colectării la obiectivul urmărit, consecințele previzibile în mod rezonabil pentru persoanele în cauză și natura și sensibilitatea datelor care urmează să fie colectate ([249]).

([241]) Secțiunea 2 litera (b) punctul (ii) din OE nr. 14086.
([242]) Articolul 102A din Legea privind securitatea națională (*National Security Act*) și secțiunea 2 litera (b) punctul (iii) din OE nr. 14086.
([243]) În cazuri excepționale (în special atunci când un astfel de proces nu poate fi efectuat din cauza necesității de a răspunde unei cerințe noi sau în evoluție în materie de informații), astfel de priorități pot fi stabilite direct de către președinte sau de către șeful unui element al Comunității Serviciilor de Informații, care, în principiu, trebuie să aplice aceleași criterii precum cele descrise în secțiunea 2 litera (b) punctul (iii) partea A subpunctele 1-3 – a se vedea secțiunea 4 litera (n) din OE nr. 14086.
([244]) Secțiunea 2 litera (b) punctul (iii) partea C din OE nr. 14086.
([245]) Secțiunea 2 litera (b) și litera (c) punctul (i) partea A din OE nr. 14086.
([246]) Secțiunea 2 litera (c) punctul (i) partea A din OE nr. 14086.
([247]) Secțiunea 2 litera (c) punctul (i) partea A din OE nr. 14086.
([248]) Secțiunea 2 litera (c) punctul (i) partea B din OE nr. 14086.
([249]) Secțiunea 2 litera (c) punctul (i) partea B din OE nr. 14086.

(140) În ceea ce privește tipul de colectare de informații de tip SIGINT, colectarea de date în Statele Unite ale Americii, care este cea mai relevantă pentru prezenta constatare privind caracterul adecvat, întrucât se referă la date care au fost transferate către organizații din SUA, trebuie să fie întotdeauna direcționată, astfel cum se explică în detaliu în considerentele 142-153.

(141) „Colectarea în masă" ([250]) se poate efectua numai în afara Statelor Unite ale Americii, în temeiul OE nr. 12333. De asemenea, în acest caz, în conformitate cu OE nr. 14086, colectarea direcționată trebuie să aibă prioritate ([251]). În schimb, colectarea în masă este permisă numai în cazul în care informațiile necesare pentru a promova o prioritate validată în materie de informații nu pot fi obținute în mod rezonabil printr-o colectare direcționată ([252]). Atunci când este necesar să se efectueze o colectare de date în masă în afara Statelor Unite ale Americii, se aplică garanții specifice în temeiul OE nr. 14086 ([253]). În primul rând, trebuie aplicate metode și măsuri tehnice pentru a limita datele colectate numai la ceea ce este necesar pentru promovarea unei priorități validate în materie de informații, reducând în același timp la minimum colectarea de informații nepertinente ([254]). În al doilea rând, ordinul executiv limitează utilizarea informațiilor colectate în masă (inclusiv interogarea) la șase obiective specifice, care includ protecția împotriva terorismului, luarea de ostatici și sechestrarea de persoane de către sau în numele unui guvern, al unei organizații sau al unei persoane străine, protecția împotriva spionajului străin și a sabotajului sau a asasinatelor plănuite din exterior, protecția împotriva amenințărilor generate de deținerea în vederea dezvoltării sau de proliferarea armelor de distrugere în masă sau a tehnologiilor și amenințărilor conexe etc ([255]). În sfârșit, orice interogare a informațiilor de tip SIGINT colectate în masă poate avea loc numai în cazul în care acest lucru este necesar pentru a promova o prioritate validată în materie de informații în vederea atingerii acestor șase obiective și în conformitate cu politici și proceduri care iau în considerare în mod corespunzător impactul interogărilor asupra vieții private și a libertăților civile ale tuturor persoanelor, indiferent de cetățenie sau de locul de reședință al acestora ([256]).

(142) În plus față de cerințele OE nr. 14086, colectarea de date de tip SIGINT transferată unei organizații din Statele Unite ale Americii face obiectul unor limitări și garanții specifice reglementate de secțiunea 702 din FISA ([257]). Secțiunea 702 din FISA permite colectarea de informații externe prin vizarea persoanelor care nu sunt cetățeni americani/rezidenți în SUA despre care se crede în mod rezonabil că se află în afara Statelor Unite ale Americii, cu sprijinul obligatoriu al furnizorilor de servicii de comunicații electronice din SUA ([258]). Pentru a colecta informații externe în temeiul secțiunii 702 din FISA, procurorul general și directorul Serviciului Național de Informații prezintă certificări anuale Curții de Supraveghere a Activităților Străine de Spionaj (*United States Foreign*

([250]) Și anume colectarea unor cantități mari de informații de tip SIGINT care, din motive tehnice sau operaționale, sunt obținute fără a se recurge la factori de diferențiere (de exemplu, fără utilizarea unor identificatori sau a unor termeni de selecție specifici) – a se vedea secțiunea 4 litera (b) din OE nr. 14086. În temeiul OE nr. 14086 și astfel cum se explică în considerentul 141, colectarea în masă în temeiul OE nr. 12333 are loc numai atunci când este necesar pentru a promova priorități specifice validate în materie de informații și face obiectul unei serii de limitări și garanții menite să asigure faptul că datele nu sunt accesate în mod nediferențiat. Prin urmare, colectarea în masă se diferențiază de colectarea generalizată și nediferențiată („supravegherea în masă"), fără limitări și garanții.

([251]) A se vedea secțiunea 2 litera (c) punctul (ii) partea A din OE nr. 14086.

([252]) A se vedea secțiunea 2 litera (c) punctul (ii) partea A din OE nr. 14086.

([253]) Normele specifice privind colectarea în masă prevăzute în OE nr. 14086 se aplică, de asemenea, unei activități specifice de colectare de informații de tip SIGINT care utilizează temporar date obținute fără factori de diferențiere (de exemplu, termeni de selecție sau identificatori specifici), și anume în masă (care este posibilă numai în afara teritoriului Statelor Unite). Acest lucru nu este valabil atunci când aceste date sunt utilizate numai pentru a sprijini faza tehnică inițială a activității specifice de colectare de informații de tip SIGINT, sunt păstrate numai pentru o perioadă scurtă de timp necesară pentru finalizarea acestei faze și sunt șterse imediat după aceea [secțiunea 2 litera (c) punctul (ii) partea D din OE nr. 14086]. În acest caz, singurul scop al colectării inițiale fără factori de diferențiere este de a permite o colectare direcționată de informații prin aplicarea unui identificator sau a unui termen de selecție specific. Într-un astfel de scenariu, numai datele care răspund aplicării unui anumit factor de diferențiere sunt introduse în bazele de date guvernamentale, în timp ce celelalte date sunt distruse. O astfel de colectare direcționată rămâne, prin urmare, reglementată de normele generale aplicabile colectării de informații de tip SIGINT, în special inclusiv secțiunea 2 literele (a)-(b) și secțiunea 2 litera (c) punctul (i) din OE nr. 14086.

([254]) A se vedea secțiunea 2 litera (c) punctul (ii) partea A din OE nr. 14086.

([255]) A se vedea secțiunea 2 litera (c) punctul (ii) partea B din OE nr. 14086. În cazul în care intervin noi imperative de securitate națională, cum ar fi amenințări noi la adresa securității naționale, președintele poate actualiza această listă. În principiu, astfel de actualizări trebuie să fie făcute publice, cu excepția cazului în care președintele stabilește că acest lucru ar reprezenta un risc pentru securitatea națională a Statelor Unite ale Americii [secțiunea 2 litera (c) punctul (ii) partea C din OE nr. 14086]. În ceea ce privește interogările de date colectate în masă, a se vedea secțiunea 2 litera (c) punctul (iii) partea D din OE nr. 14086.

([256]) Secțiunea 2 litera (a) punctul (ii) partea A, coroborată cu secțiunea 2 litera (c) punctul (iii) partea D din OE nr. 14086. A se vedea, de asemenea, anexa VII.

([257]) Titlul 50 articolul 1881 din U.S.C.

([258]) Titlul 50 articolul 1881a litera (a) din U.S.C. În special, astfel cum menționează PCLOB, supravegherea în temeiul secțiunii 702 „constă în întregime în vizarea anumitor persoane [care nu sunt cetățeni americani/rezidenți SUA] cu privire la care s-a luat o decizie individualizată" [Comitetul de supraveghere în materie de protecție a vieții private și a libertăților civile, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (Raport cu privire la programul de supraveghere desfășurat în temeiul secțiunii 702 din Legea privind supravegherea activităților străine de spionaj), 2 iulie 2014, raportul cu privire la articolul 702, p. 111]. A se vedea, de asemenea, CLPO NSA [Biroul pentru libertăți civile și viață privată al Agenției Naționale de Securitate – NSA (*National Security Agency*)], *Implementation of Foreign Intelligence Act Section 702* (Punerea în aplicare de către NSA a secțiunii 702 din Legea privind activitățile de colectare de informații externe), 16 aprilie 2014. Termenul „furnizor de servicii de comunicații electronice" este definit în titlul 50 articolul 1881 litera (a) punctul 4 din U.S.C.

Intelligence Surveillance Court) (FISC), care identifică respectivele categorii de informații externe care urmează să fie obținute ([259]). Certificările trebuie să fie însoțite de proceduri de direcționare și de reducere la minimum a intervențiilor, precum și de interogare, care sunt, de asemenea, aprobate de această instanță și sunt obligatorii din punct de vedere juridic pentru serviciile de informații din SUA.

(143) FISC este o instanță judecătorească independentă ([260]) creată în temeiul unei legi federale, ale cărui decizii pot fi atacate înaintea Curții de Reexaminare a Supravegherii Activităților Străine de Spionaj (*Foreign Intelligence Surveillance Court of Review*) (FISCR) ([261]) și, în ultimă instanță, înaintea Curții Supreme a Statelor Unite ale Americii ([262]). FISC beneficiază (la fel ca FISCR) de sprijinul furnizat de un complet permanent format din cinci avocați și cinci experți tehnici specializați în domeniul securității naționale, precum și al libertăților civile ([263]). Din cadrul acestui complet, instanța desemnează o persoană care servește drept *amicus curiae* pentru a contribui la examinarea oricărei cereri de emitere a unui ordin sau de 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 ([264]). Astfel se asigură, în special, faptul că aspectele legate de confidențialitate sunt reflectate în mod corespunzător în evaluarea instanței. De asemenea, instanța poate să numească o persoană sau organizație în calitate de *amicus curiae*, inclusiv pentru a furniza o 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* ([265]).

(144) FISC examinează certificările și procedurile aferente (în special procedurile de direcționare și de reducere la minimum a intervențiilor) din perspectiva respectării cerințelor FISA. În cazul în care FISC consideră că nu au fost îndeplinite cerințele, aceasta poate refuza certificarea, integral sau parțial, și poate solicita modificarea procedurilor ([266]). În acest sens, FISC a confirmat în repetate rânduri că revizuirea de către acesta a procedurilor de direcționare și reducere la minimum a intervențiilor în temeiul secțiunii 702 nu se limitează la procedurile scrise, ci include și modul în care procedurile sunt puse în aplicare de autorități ([267]).

(145) Agenția Națională de Securitate (NSA, serviciul de informații responsabil cu direcționarea intervențiilor în temeiul secțiunii 702 din FISA) ia decizii individuale de direcționare a intervențiilor în conformitate cu procedurile de direcționare aprobate de FISC, care impun NSA să evalueze, pe baza tuturor circumstanțelor, dacă este probabil ca vizarea unei anumite persoane să conducă la obținerea unei categorii de informații externe identificate într-o certificare ([268]). Această evaluare trebuie să fie individualizată și bazată pe fapte și se realizează pe baza

([259]) Titlul 50 articolul 1881a litera (g) din U.S.C.

([260]) FISC este alcătuită din 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 Senat. Judecătorii, cu titularizare pe viață, pot fi revocați din funcție 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 titlul 50 articolul 1803 litera (a) din U.S.C. 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 scrisoarea 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, disponibilă la adresa https://fas.org/irp/news/2013/07/fisc-leahy.pdf.

([261]) FISCR este formată din judecători numiți de către președintele Curții Supreme a Statelor Unite ale Americii, provin din instanțe districtuale sau curți de apel din SUA și își desfășoară activitatea în baza unui mandat eșalonat de șapte ani. A se vedea titlul 50 articolul 1803 litera (b) din U.S.C.

([262]) A se vedea titlul 50 articolul 1803 litera (b), articolul 1861a litera (f), articolul 1881a litera (h) și articolul 1881a litera (i) punctul 4 din U.S.C.

([263]) Titlul 50 articolul 1803 litera (i) punctul 1 și punctul 3 partea A din U.S.C.

([264]) Titlul 50 articolul 1803 litera (i) punctul 2 partea A din U.S.C.

([265]) Titlul 50 articolul 1803 litera (i) punctul 2 partea B din U.S.C.

([266]) A se vedea, de exemplu, avizul FISC din 18 octombrie 2018, disponibil la adresa https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, astfel cum a fost confirmat de Curtea de Reexaminare a Supravegherii Activităților Străine de Spionaj în avizul său din 12 iulie 2019, disponibil la adresa https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf.

([267]) A se vedea, de exemplu, FISC, *Memorandum Opinion and Order* – 35 (Aviz memorandum și ordin) (18 noiembrie 2020) (autorizat pentru publicare la 26 aprilie 2021), (anexa D).

([268]) Titlul 50 articolul 1881a litera (a) din U.S.C. – Procedurile utilizate de Agenția Națională de Securitate pentru vizarea persoanelor care nu sunt cetățeni americani/rezidenți SUA cu privire la care se presupune în mod rezonabil că se află în afara Statelor Unite ale Americii pentru obținerea de informații externe în temeiul secțiunii 702 din Legea privind supravegherea activităților străine de spionaj din 1978, astfel cum a fost modificată, din martie 2018 (procedurile NSA de direcționare a intervențiilor), disponibile la adresa https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_NSA_Targeting_27Mar18.pdf, p. 1-4, explicate în detaliu în raportul PCLOB, p. 41-42.

raționamentului analitic, a formării specializate și a experienței analistului, precum și a naturii informațiilor externe care urmează să fie obținute ([269]). Direcționarea intervențiilor se realizează prin identificarea așa-numiților termeni de selecție, care identifică mijloacele de comunicare specifice, cum ar fi adresa de e-mail sau numărul de telefon al persoanei vizate, dar niciodată cuvinte-cheie sau numele persoanelor ([270]).

(146) În primul rând, analiștii NSA vor identifica persoanele care nu sunt cetățeni americani/rezidenți în SUA aflate în străinătate a căror supraveghere va conduce, pe baza evaluării analiștilor, la informațiile externe relevante specificate în certificare ([271]). Astfel cum se prevede în procedurile NSA de direcționare a intervențiilor, NSA poate direcționa supravegherea către o persoană vizată numai atunci când are deja anumite informații despre aceasta ([272]). Acest lucru poate rezulta din obținerea de informații din diferite surse, de exemplu informații din surse umane. Prin intermediul acestor alte surse, analistul trebuie, de asemenea, să identifice un termen de selecție specific (și anume un cont de comunicare) utilizat de persoana vizată potențială. Odată ce aceste persoanele individualizate au fost identificate și vizarea lor a fost aprobată printr-un amplu mecanism de revizuire în cadrul NSA ([273]), se stabilesc sarcinile termenilor de selecție (și anume se elaborează și se aplică termenii de selecție) care identifică mijloacele de comunicare (precum adresele de e-mail) utilizate de persoanele vizate ([274]).

(147) NSA trebuie să documenteze situația de fapt utilizată ca temei pentru selectarea persoanei vizate ([275]) și, la intervale regulate după direcționarea inițială a intervențiilor, să declare că standardul de direcționare a intervențiilor continuă să fie îndeplinit ([276]). Odată ce standardul de direcționare a intervențiilor nu mai este îndeplinit, colectarea trebuie să înceteze ([277]). Selectarea de către NSA a fiecărei persoane vizate și evidențele acesteia cu privire la fiecare evaluare și justificare a direcționării intervențiilor înregistrate sunt revizuite bilunar din perspectiva respectării procedurilor de direcționare a intervențiilor de către funcționarii din cadrul birourilor de supraveghere a serviciilor de informații ale Departamentului de Justiție, care au obligația de a raporta orice încălcare către FISC și către Congres ([278]). Documentația scrisă a NSA facilitează supravegherea de către FISC a măsurii în care anumite persoane sunt vizate în mod corespunzător în temeiul secțiunii 702 din FISA, în conformitate cu competențele sale de supraveghere descrise în considerentele 173-174 ([279]). În sfârșit, directorul Serviciului Național de Informații (DNI) are, de asemenea, obligația de a raporta în fiecare an numărul total persoane vizate în temeiul secțiunii 702 din FISA în rapoartele publice anuale privind transparența statistică. Societățile care primesc directive în temeiul secțiunii 702 din FISA pot publica date agregate (prin intermediul rapoartelor privind transparența) cu privire la cererile pe care le primesc ([280]).

([269]) Procedurile NSA de direcționare a intervențiilor, p. 4.

([270]) A se vedea raportul PCLOB cu privire la secțiunea 702, p. 32-33 și 45 cu trimiteri suplimentare. A se vedea, de asemenea, *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (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 Serviciului Național de Informații, perioada de raportare: 1 decembrie 2016-31 mai 2017, p. 41 (octombrie 2018), disponibilă la adresa: https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

([271]) Raportul PCLOB cu privire la secțiunea 702, p. 42-43.

([272]) Procedurile NSA de direcționare a intervențiilor, p. 2.

([273]) Raportul PCLOB cu privire la secțiunea 702, p. 46. De exemplu, NSA trebuie să verifice dacă există o legătură între persoana vizată și termenul de selecție utilizat, trebuie să documenteze informațiile externe preconizate a fi obținute, aceste informații trebuie să fie revizuite și aprobate de doi analiști superiori ai NSA, iar procesul în ansamblul său va fi urmărit pentru realizarea de analize de conformitate ulterioare de către ODNI și Departamentul de Justiție. A se vedea CLPO NSA, Punerea în aplicare de către NSA a secțiunii 702 din Legea privind activitățile de colectare de informații externe, 16 aprilie 2014.

([274]) Titlul 50 articolul 1881a litera (h) din U.S.C.

([275]) Procedurile NSA de direcționare a intervențiilor, p. 8. A se vedea, de asemenea, raportul PCLOB cu privire la secțiunea 702, p. 46. Nefurnizarea unei justificări scrise constituie un incident de conformitate cu privire la documentare, care trebuie raportat FISC și Congresului. A se vedea *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (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 Serviciului Național de Informații, perioada de raportare: 1 decembrie 2016-31 mai 2017, p. 41 (octombrie 2018), precum și raportul DoJ/ODNI cu privire la conformitate adresat FISC pentru perioada decembrie 2016-mai 2017, p. A-6, disponibil la adresa https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

([276]) A se vedea documentul prezentat de guvernul SUA Curții de Supraveghere a Activităților Străine de Spionaj, care reprezintă o sinteză realizată în 2015 a principalelor cerințe în temeiul secțiunii 702, punctele 2-3 (15 iulie 2015) și informațiile furnizate în anexa VII.

([277]) A se vedea documentul prezentat de guvernul SUA Curții de Supraveghere a Activităților Străine de Spionaj, care reprezintă o sinteză realizată în 2015 a principalelor cerințe în temeiul secțiunii 702, punctele 2-3 (15 iulie 2015). Acesta prevede că „[î]n cazul în care guvernul evaluează ulterior că nu se preconizează că aplicarea în continuare a unui termen de selecție cu sarcini stabilite în legătură cu o persoană vizată va avea ca rezultat obținerea de informații externe, este necesară încetarea promptă a acestei activități, orice întârziere în acest sens putând conduce la un incident de conformitate raportabil". A se vedea, de asemenea, informațiile furnizate în anexa VII.

([278]) Raportul PCLOB cu privire la secțiunea 702, p. 70-72; Norma nr. 13 litera (b) din Regulamentul de procedură al Curții de Supraveghere a Activităților Străine de Spionaj a SUA, disponibil la adresa https://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

([279]) A se vedea, de asemenea, raportul DoJ/ODNI cu privire la conformitate adresat FISC pentru perioada decembrie 2016-mai 2017, p. A-6.

([280]) Titlul 50 articolul 1874 din U.S.C.

(148) În ceea ce privește celelalte temeiuri juridice pentru colectarea datelor cu caracter personal transferate către organizații din SUA, se aplică limitări și garanții diferite. În general, colectarea de date în masă este interzisă în mod specific în temeiul secțiunii 402 din FISA (competența de interceptare și de capturare și trasabilitate) și prin utilizarea NSL, iar utilizarea unor „termeni de selecție" specifici este, în schimb, obligatorie ([281]).

(149) Pentru a desfășura activități de supraveghere electronică individualizată tradițională (în conformitate cu secțiunea 105 din FISA), serviciile de informații trebuie să depună o cerere la FISC, însoțită de o expunere a faptelor și a circumstanțelor invocate în susținerea convingerii că există o cauză probabilă ca infrastructura vizată să fie utilizată sau să fie pe cale să fie utilizată de o putere străină sau de un agent al unei puteri străine ([282]). FISC va evalua, printre altele, dacă, pe baza faptelor prezentate, există o cauză probabilă să se considere că situația se prezintă într-adevăr astfel ([283]).

(150) Pentru a efectua o percheziție a spațiilor sau a bunurilor menită să conducă la o verificare sau la un sechestru etc. de informații, materiale sau bunuri (de exemplu, asupra unui dispozitiv informatic) în temeiul secțiunii 301 din FISA, este necesar să se înainteze FISC o cerere de emitere a unui ordin în acest sens ([284]). O astfel de cerere trebuie, printre altele, să demonstreze că există o cauză probabilă ca persoana vizată de percheziție să fie o putere străină sau un agent al unei puteri străine, ca spațiul sau bunurile care urmează să fie percheziționate să conțină informații externe și ca spațiul care urmează să fie percheziționat să fie deținut sau utilizat de sau ca obiectul percheziției să se afle în tranzit către sau de la o putere străină sau un agent al unei puteri străine ([285]).

(151) În mod similar, pentru instalarea unor dispozitive de interceptare și de capturare și trasabilitate (în temeiul secțiunii 402 din FISA), este necesar să se înainteze FISC (sau unui judecător magistrat al SUA) o cerere în acest sens, precum și să utilizeze un anumit termen de selecție, și anume un termen 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 vizate ([286]). 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 de care beneficiază, sursa/mecanismul de plată).

(152) Secțiunea 501 din FISA ([287]), care permite colectarea evidențelor comerciale ale unui transportator comun (și anume orice persoană sau entitate care transportă persoane sau bunuri pe cale terestră, feroviară, navală sau pe calea aerului în schimbul unei compensații), ale unei unități publice de cazare (de exemplu, un hotel, un motel sau o pensiune), ale unei unități de închiriere de vehicule sau ale unei unități de depozitare fizică (și anume o unitate care oferă spațiu sau servicii legate de depozitarea bunurilor și a materialelor) ([288]), impune, de asemenea, înaintarea unei cereri în acest sens către FISC sau un judecător magistrat. Această cerere trebuie să specifice evidențele vizate și faptele specifice și articulabile care susțin convingerea că persoana la care se referă evidențele respective este o putere străină sau un agent al unei puteri străine ([289]).

(153) În sfârșit, NSL sunt autorizate în temeiul unor legi diferite și permit agențiilor de investigare să obțină anumite informații (fără a include conținutul comunicațiilor) de la anumite entități (de exemplu, instituții financiare, agenții de raportare a creditelor, furnizori de comunicații electronice) conținute în rapoartele de credit, evidențele financiare și evidențele electronice privind abonații și tranzacțiile ([290]). Legea privind NSL care autorizează accesul la comunicațiile electronice poate fi utilizată numai de FBI și impune ca orice cerere în acest sens să utilizeze un termen care identifică în mod specific o persoană, o entitate, un număr de telefon sau un cont și să certifice faptul că informațiile sunt relevante pentru o investigație de securitate națională autorizată în vederea protejării împotriva terorismului internațional sau a activităților clandestine de colectare de informații ([291]). Destinatarii unei NSL au dreptul de a o contesta în instanță ([292]).

([281]) Titlul 50 articolul 1842 litera (c) punctul 3 din U.S.C. și, în ceea ce privește NSL, titlul 12 articolul 3414 litera (a) punctul 2 din U.S.C.; titlul 15 articolul 1681u din U.S.C.; titlul 15 articolul 1681v litera (a) din U.S.C. și titlul 18 articolul 2709 litera (a) din U.S.C.

([282]) „Un agent al unei puteri străine" poate include persoane care nu sunt cetățeni americani/rezidenți în SUA care desfășoară activități de terorism internațional sau activități internaționale de proliferare a armelor de distrugere în masă (inclusiv acțiuni pregătitoare în acest sens) [titlul 50 articolul 1801 litera (b) punctul 1 din U.S.C.].

([283]) Titlul 50 articolul 1804 din U.S.C. A se vedea, de asemenea, articolul 1841 alineatul (4) în ceea ce privește alegerea termenilor de selecție.

([284]) Titlul 50 articolul 1821 alineatul (5) din U.S.C.

([285]) Titlul 50 articolul 1823 litera (a) din U.S.C.

([286]) Titlul 50 articolul 1842 și articolul 1841 alineatul (2) din U.S.C., precum și titlul 18 secțiunea 3127.

([287]) Titlul 50 articolul 1862 din U.S.C.

([288]) Titlul 50 articolele 1861-1862 din U.S.C.

([289]) Titlul 50 articolul 1862 litera (b) din U.S.C.

([290]) Titlul 12 articolul 3414 din U.S.C. Titlul 15 articolele 1681u-1681v din U.S.C. și titlul 18 articolul 2709 din U.S.C.

([291]) Titlul 18 articolul 2709 litera (b) din U.S.C.

([292]) De exemplu, titlul 18 articolul 2709 litera (d) din U.S.C.

3.2.1.3 *Utilizarea ulterioară a informațiilor colectate*

(154) Prelucrarea datelor cu caracter personal colectate de serviciile de informații din SUA printr-un sistem de tip SIGINT face obiectul unei serii de garanții.

(155) În primul rând, fiecare serviciu de informații trebuie să asigure securitatea corespunzătoare a datelor și să împiedice accesul persoanelor neautorizate la datele cu caracter personal colectate printr-un sistem de tip SIGINT. În acest sens, diferite instrumente, care pot include legi, orientări și standarde, detaliază cerințele minime de securitate a informațiilor care trebuie puse în aplicare (de exemplu, autentificarea multifactorială, criptarea etc.) ([293]). Accesul la datele colectate trebuie limitat la personalul autorizat și instruit, care trebuie să cunoască informațiile necesare pentru a-și îndeplini atribuțiile ([294]). La un nivel mai general, serviciile de informații trebuie să ofere formare adecvată angajaților lor, inclusiv cu privire la procedurile de raportare și de abordare a încălcărilor legii (inclusiv cu privire la OE nr. 14086) ([295]).

(156) În al doilea rând, serviciile de informații trebuie să respecte standardele Comunității Serviciilor de Informații în ceea ce privește acuratețea și obiectivitatea, în special în ceea ce privește asigurarea calității și a fiabilității datelor, luarea în considerare a unor surse alternative de informații și obiectivitatea în efectuarea analizelor ([296]).

(157) În al treilea rând, în ceea ce privește păstrarea datelor, OE nr. 14086 clarifică faptul că datele cu caracter personal ale persoanelor care nu sunt cetățeni americani/rezidenți SUA fac obiectul acelorași perioade de păstrare precum cele aplicabile datelor persoanelor care sunt cetățeni americani/rezidenți SUA ([297]) Serviciile de informații au obligația de a defini perioade de păstrare specifice și/sau factorii care trebuie luați în considerare pentru a stabili durata perioadelor de păstrare aplicabile (de exemplu, dacă informațiile sunt dovezi ale unei infracțiuni; dacă informațiile constituie informații externe; dacă informațiile sunt necesare pentru a proteja siguranța persoanelor sau a organizațiilor, inclusiv a victimelor sau a țintelor terorismului internațional), care sunt prevăzute în diferite instrumente juridice ([298]).

(158) În al patrulea rând, se aplică norme specifice în ceea ce privește diseminarea datelor cu caracter personal colectate printr-un sistem de tip SIGINT. Ca o cerință generală, datele cu caracter personal privind persoanele care nu sunt cetățeni americani/rezidenți SUA pot fi diseminate numai dacă implică același tip de informații care pot fi diseminate cu privire la persoane care sunt cetățeni americani/rezidenți SUA, de exemplu, informațiile necesare pentru a proteja siguranța unei persoane sau a unei organizații (cum ar fi persoane vizate, victime sau ostatici ai organizațiilor teroriste internaționale) ([299]). În plus, datele cu caracter personal nu pot fi diseminate ținând cont exclusiv de cetățenia sau de țara de reședință a unei persoane sau în scopul eludării cerințelor OE nr. 14086 ([300]).

([293]) Secțiunea 2 litera (c) punctul (iii) partea B subpunctul 1 din OE nr. 14086. A se vedea, de asemenea, titlul VIII din Legea privind securitatea națională (care detaliază cerințele de acces la informațiile clasificate), OE nr. 12333 – secțiunea 1.5 (care impune șefilor serviciilor Comunității Serviciilor de Informații să respecte o serie de orientări privind schimbul de informații și securitatea acestora, confidențialitatea informațiilor și alte cerințe legale), Directiva nr. 42 privind securitatea națională (*National Security Directive 42*), „National Policy for the Security of National Security Telecommunications and Information Systems" (Politica națională de securitate a sistemelor informatice și de telecomunicații utilizate în domeniul securității naționale) [care însărcinează Comitetul privind sistemele de securitate națională (*Committee on National Security Systems*) să ofere orientări în materie de securitate a sistemelor de securitate națională departamentelor și agențiilor executive], și Memorandumul nr. 8 privind securitatea națională (*National Security Memorandum 8*) – „Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems" [Îmbunătățirea securității cibernetice a sistemelor de securitate națională, ale Departamentului Apărării (*Department of Defense*) și ale Comunității Serviciilor de Informații] (care stabilește termene și orientări de punere în aplicare a cerințelor de securitate cibernetică pentru sistemele de securitate națională, inclusiv cu privire la autentificarea multifactorială, criptarea, tehnologiile cloud și serviciile de detectare a punctelor terminale).

([294]) Secțiunea 2 litera (c) punctul (iii) partea B subpunctul 2 din OE nr. 14086. În plus, datele cu caracter personal pentru care nu s-a luat nicio decizie definitivă privind păstrarea pot fi accesate numai în scopul luării sau al justificării unei astfel de decizii sau în scopul îndeplinirii unor funcții administrative, de testare, de dezvoltare, de securitate sau de supraveghere autorizate [secțiunea 2 litera (c) punctul (iii) partea B subpunctul 3 din OE nr. 14086].

([295]) Secțiunea 2 litera (d) punctul (ii) din OE nr. 14086.

([296]) Secțiunea 2 litera (c) punctul (iii) partea C din OE nr. 14086.

([297]) Secțiunea 2 litera (c) punctul (iii) partea A subpunctul 2 literele (a)-(c) din OE nr. 14086. La un nivel mai general, fiecare serviciu de informații trebuie să instituie politici și proceduri menite să reducă la minimum diseminarea și păstrarea datelor cu caracter personal colectate printr-un sistem de tip SIGINT [secțiunea 2 litera (c) punctul (iii) partea A din OE nr. 14086].

([298]) A se vedea, de exemplu, secțiunea 309 din Legea privind autorizarea serviciilor de informații pentru anul fiscal 2015 (*Intelligence Authorization Act for Fiscal Year 2015*). procedurile de reducere la minimum adoptate de serviciile de informații individuale în temeiul secțiunii 702 din FISA și autorizate de FISC; procedurile aprobate de procurorul general și de FRA (care impun agențiilor federale din SUA, inclusiv agențiilor de securitate națională, să stabilească perioade de păstrare a evidențelor lor, care trebuie aprobate de Administrația Arhivelor și a Registrelor Naționale).

([299]) Secțiunea 2 litera (c) punctul (iii) partea A subpunctul 1 litera (a) și secțiunea 5 litera (d) din OE nr. 14086, coroborate cu secțiunea 2.3 din OE nr. 12333.

([300]) Secțiunea 2 litera (c) punctul (iii) partea A subpunctul 1 literele (b) și (e) din OE nr. 14086.

Diseminarea între autoritățile SUA poate avea loc numai dacă o persoană autorizată și instruită are convingerea rezonabilă că este necesar ca destinatarul să cunoască informațiile ([301]) și că acesta le va proteja în mod corespunzător ([302]). Pentru a stabili dacă datele cu caracter personal pot fi diseminate unor destinatari din afara autorităților SUA (inclusiv unui guvern străin sau unei organizații internaționale), trebuie să se țină seama de scopul diseminării, de natura și de amploarea datelor care sunt diseminate, precum și de potențialul impact negativ asupra persoanei (persoanelor) în cauză ([303]).

(159) În cele din urmă, inclusiv pentru a facilita supravegherea respectării cerințelor legale aplicabile, precum și existența unor căi de atac eficiente, fiecare serviciu de informații trebuie să păstreze, în temeiul OE nr. 14086, documentația corespunzătoare cu privire la colectarea de informații de tip SIGINT. Cerințele privind documentația vizează elemente precum situația de fapt utilizată ca temei pentru evaluarea caracterului necesar al unei anumite activități de colectare în scopul promovării unei priorități validate în materie de informații ([304]).

(160) Pe lângă garanțiile din OE nr. 14086 menționate mai sus pentru utilizarea informațiilor colectate printr-un sistem de tip SIGINT, toate serviciile de informații din SUA fac obiectul unor cerințe mai generale privind limitarea scopului, reducerea la minimum, acuratețea, securitatea, păstrarea și diseminarea datelor, în special în temeiul Circularei nr. A-130 a OMB, al Legii privind guvernarea electronică, al Legii privind registrele federale (a se vedea considerentele 101-106) și al orientărilor Comitetului privind sistemele de securitate națională (CNSS) ([305]).

3.2.2 ***Supraveghere***

(161) Activitățile serviciilor de informații din SUA fac obiectul supravegherii de către diferite organisme.

(162) În primul rând, OE nr. 14086 impune fiecărui serviciu de informații să dispună de funcționari la nivel înalt cu atribuții juridice, de supraveghere și de conformitate care să asigure conformitatea cu legislația aplicabilă a SUA ([306]). În special, aceștia trebuie să efectueze o supraveghere periodică a activităților de colectare de informații de tip SIGINT și să se asigure că orice neconformitate este remediată. Serviciile de informații trebuie să le ofere acestor funcționari acces la toate informațiile relevante pentru a-și îndeplini funcțiile de supraveghere și nu pot lua nicio măsură pentru a împiedica sau influența în mod necorespunzător activitățile lor de supraveghere ([307]). În plus, orice incident semnificativ de neconformitate ([308]) identificat de un funcționar de supraveghere sau de orice alt angajat trebuie raportat imediat șefului serviciului de informații respectiv și directorului Serviciului Național de Informații, care trebuie să se asigure că sunt luate toate măsurile necesare pentru a remedia și a preveni repetarea incidentului semnificativ de neconformitate respectiv ([309]).

(163) Această funcție de supraveghere este îndeplinită de funcționarii cu atribuții specifice de conformitate, precum și de responsabilii pentru protecția vieții private și a libertăților civile și de inspectorii generali ([310]).

([301]) A se vedea, de exemplu, AGG-DOM, care prevede, de pildă, că FBI poate disemina informații numai dacă destinatarul are nevoie să le cunoască pentru a-și îndeplini misiunea sau pentru a proteja publicul.

([302]) Secțiunea 2 litera (c) punctul (iii) partea A subpunctul 1 litera (c) din OE nr. 14086. Serviciile de informații pot, de exemplu, să disemineze informații în circumstanțe relevante pentru o investigare sau referitoare la o infracțiune, inclusiv, de exemplu, prin diseminarea de avertismente privind amenințările de ucidere, vătămare corporală gravă sau răpire; diseminarea de informații privind răspunsul la amenințările, incidentele sau intruziunile cibernetice; și notificarea victimelor sau avertizarea potențialelor victime ale criminalității.

([303]) Secțiunea 2 litera (c) punctul (iii) partea A subpunctul 1 litera (d) din OE nr. 14086.

([304]) Secțiunea 2 litera (c) punctul (iii) partea E din OE nr. 14086.

([305]) A se vedea Politica nr. 22 a CNSS, Politica de gestionare a riscurilor în materie de securitate cibernetică și Instrucțiunea nr. 1253 a CNSS, care oferă orientări detaliate privind măsurile de securitate care trebuie puse în aplicare pentru sistemele de securitate națională.

([306]) Secțiunea 2 litera (d) punctul (i) părțile A și B din OE nr. 14086.

([307]) Secțiunea 2 litera (d) punctul (i) părțile B și C din OE nr. 14086.

([308]) Și anume nerespectarea sistematică sau intenționată a legislației aplicabile a SUA, care ar putea aduce atingere reputației sau integrității unui element al Comunității Serviciilor de Informații sau ar putea pune sub semnul întrebării în alt mod corectitudinea unei activități a Comunității Serviciilor de Informații, inclusiv având în vedere orice impact semnificativ asupra intereselor persoanei sau persoanelor în cauză din perspectiva vieții private și a libertăților civile; a se vedea secțiunea 5 litera (l) din OE nr. 14086.

([309]) Secțiunea 2 litera (d) punctul (iii) din OE nr. 14086.

([310]) Secțiunea 2 litera (d) punctul (i) partea B din OE nr. 14086.

(164) La fel ca în cazul autorităților de aplicare a dreptului penal, responsabilii pentru protecția vieții private și a libertăților civile există la nivelul tuturor serviciilor de informații ([311]). Competențele acestor funcționari cuprind, de regulă, supravegherea procedurilor pentru a se asigura că departamentul/agenția în cauză 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/s-au încălcat dreptul la viață privată sau libertățile civile [și, în unele cazuri, de exemplu în cazul Biroului Directorului Serviciului Național de Informații (ODNI), pot avea competența de investiga plângerile respective ([312])]. Șefii serviciilor de informații trebuie să se asigure că responsabilii pentru protecția vieții private și a libertăților civile dispun de resursele necesare pentru a-și îndeplini mandatul, că au acces la orice material și personal necesar pentru îndeplinirea funcțiilor lor și că sunt informați și consultați cu privire la modificările de politică propuse ([313]). Responsabilii pentru protecția vieții private și a libertăților civile raportează periodic Congresului și PCLOB, inclusiv cu privire la numărul și natura plângerilor primite de către departament/agenție, punând la dispoziție și un rezumat al deciziilor luate în legătură cu astfel de plângeri, cu privire la evaluările și anchetele întreprinse și la impactul activităților desfășurate de aceștia ([314]).

(165) În al doilea rând, fiecare serviciu de informații dispune de un inspector general independent cu atribuții, printre altele, de supraveghere a activităților de colectare de informații externe. Astfel, în cadrul ODNI, există un birou al inspectorului general al Comunității Serviciilor de Informații, care are competență generală asupra întregii Comunități a Serviciilor de Informații și care este autorizat să realizeze investigații cu privire la plângeri sau informații care vizează acuzații de comportament ilicit sau abuz de autoritate în legătură cu ODNI și/sau programele și activitățile Comunității Serviciilor de Informații ([315]). La fel ca în cazul autorităților de aplicare a dreptului penal (a se vedea considerentul 109), acești inspectori generali sunt independenți din punct de vedere legal ([316]) și sunt responsabili pentru efectuarea de audituri și investigații privind programele și operațiunile desfășurate de serviciul respectiv în scopuri legate de obținerea de informații interne, inclusiv în ceea ce privește abuzul sau încălcarea legii ([317]). Aceștia au acces la toate evidențele, rapoartele, auditurile, analizele, documentele,

([311]) A se vedea titlul 42 articolul 2000ee-1 din U.S.C. Printre acestea se numără, de exemplu, Departamentul de Stat (*Department of State*), Departamentul de Justiție, Departamentul pentru Securitate Internă, Departamentul Apărării, NSA, Agenția Centrală de Informații (*Central Intelligence Agency* – CIA), FBI și ODNI.

([312]) A se vedea secțiunea 3 litera (c) din OE nr. 14086.

([313]) Titlul 42 articolul 2000ee-1 litera (d) din U.S.C.

([314]) A se vedea titlul 42 articolul 2000ee-1 litera (f) punctele 1-2 din U.S.C. De exemplu, raportul Biroului pentru libertăți civile, viață privată și transparență al NSA, care vizează perioada ianuarie 2021-iunie 2021, arată că acesta a efectuat 591 de evaluări ale impactului asupra libertăților civile și a vieții private în diferite contexte, de exemplu, în ceea ce privește activitățile de colectare, acordurile și deciziile privind schimbul de informații, deciziile privind păstrarea datelor etc., luând în considerare diferiți factori, cum ar fi cantitatea și tipul de informații asociate activității în cauză, persoanele implicate, scopul și utilizarea anticipată a datelor, garanțiile existente pentru atenuarea riscurilor potențiale la adresa vieții private etc.(https://media.defense.gov/2022/Apr/11/2002974486/-1/-1/1/REPORT%207_CLPT%20JANUARY%20-%20JUNE%202021%20_FINAL.PDF). În mod similar, rapoartele Biroului pentru protecția vieții private și a libertăților civile al CIA pentru perioada ianuarie-iunie 2019 oferă informații cu privire la activitățile de supraveghere ale biroului, de exemplu, cu privire la o evaluare a conformității cu Orientările procurorului general în temeiul OE nr. 12333 în ceea ce privește păstrarea și diseminarea informațiilor, orientările furnizate cu privire la punerea în aplicare a PPD-28 și cerințele de identificare și abordare a încălcărilor securității datelor, precum și evaluări ale utilizării și gestionării informațiilor cu caracter personal (https://www.cia.gov/static/9d762fbef6669c7e6d7f17e227fad82c/2019-Q1-Q2-CIA-OPCL-Semi-Annual-Report.pdf).

([315]) Acest inspector general este desemnat de președinte, cu confirmarea Senatului, și poate fi revocat din funcție numai de către președinte.

([316]) Inspectorii generali au un mandat sigur și pot fi revocați din funcție 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 îi poate interzice inspectorului general să demareze, să desfășoare sau să finalizeze un audit sau o investigație, în cazul în care acest lucru este considerat necesar pentru a conserva interese naționale importante (de securitate). Cu toate acestea, Congresul trebuie să fie informat cu privire la exercitarea acestei competențe și, pe această bază, poate trage la răspundere directorul respectiv. A se vedea, de exemplu, articolul 8 (pentru Departamentul Apărării), articolul 8E (pentru DoJ), articolul 8G litera (d) punctul 2 părțile A și B (pentru NSA) din Legea privind inspectorii generali din 1978, titlul 50 articolul 403q litera (b) (pentru CIA), articolul 405 litera (f) din Legea privind autorizarea serviciilor de informații pentru anul fiscal 2010 (pentru Comunitatea Serviciilor de Informații).

([317]) Legea privind inspectorii generali din 1978, astfel cum a fost modificată, Pub. L. 117-108 din 8 aprilie 2022. De exemplu, astfel cum se explică în rapoartele sale semestriale adresate Congresului pentru perioada 1 aprilie 2021-31 martie 2022, inspectorul general al NSA a realizat evaluări privind gestionarea informațiilor referitoare la persoane care sunt cetățeni americani/rezidenți SUA colectate în temeiul OE nr. 12333, procesul de eliminare a datelor de tip SIGINT, un instrument automatizat de direcționare utilizat de NSA și respectarea normelor privind documentația și a normelor de interogare în ceea ce privește colectarea de date în temeiul secțiunii 702 din FISA și a emis o serie de recomandări în acest context (a se vedea https://oig.nsa.gov/Portals/71/Reports/SAR/NSA%20OIG%20SAR%20-%20APR%202021%20-%20SEP%202021%20-%20Unclassified.pdf?ver=IwtrthntGdfEb-EKTOm3gg%3d%3d, p. 5-8 și https://oig.nsa.gov/Portals/71/Images/NSAOIGMAR2022.pdf?ver=jbq2rCrJ00HJ9qDXGHqHLw%3d%3d&timestamp=1657810395907, p. 10-13). A se vedea, de asemenea, auditurile și investigațiile realizate de inspectorul general al Comunității Serviciilor de Informații privind securitatea informațiilor și divulgările neautorizate de informații clasificate în materie de securitate națională (https://www.dni.gov/files/ICIG/Documents/Publications/Semiannual%20Report/2021/ICIG_Semiannual_Report_April_2021_to_September_2021.pdf, p. 8, 11 și https://www.dni.gov/files/ICIG/Documents/News/ICIGNews/2022/Oct21_SAR/Oct%202021-Mar%202022%20ICIG%20SAR_Unclass_FINAL.pdf, p. 19-20).

dosarele, recomandările sau alte materiale relevante, dacă este necesar, prin intermediul unei citații și pot lua declarații ale martorilor ([318]). Inspectorii generali trimit spre urmărire penală cazurile de presupuse încălcări penale și formulează recomandări de măsuri de remediere către șefii de serviciu ([319]). Deși recomandările lor nu au caracter obligatoriu, în general, rapoartele lor, inclusiv cu privire la acțiunile subsecvente (sau lipsa acestora) ([320]) sunt făcute publice și transmise Congresului, care poate să își exercite, pe această bază, propria funcție de supraveghere (a se vedea considerentele 168-169) ([321]).

(166) În al treilea rând, Comitetul pentru supravegherea serviciilor de informații (*Intelligence Oversight Board*) (IOB), instituit în cadrul Consiliului consultativ privind serviciile de informații al președintelui (PIAB), supraveghează respectarea de către serviciile de informații din SUA a Constituției și a tuturor normelor aplicabile ([322]). PIAB este un organism consultativ din cadrul Biroului executiv al președintelui, acesta din urmă fiind format din 16 membri numiți de președinte care nu fac parte din personalul autorităților SUA. IOB este format din maximum cinci membri desemnați de președinte dintre membrii PIAB. În conformitate cu OE nr. 12333 ([323]), șefii tuturor serviciilor de informații au obligația de a raporta către IOB orice activitate de colectare de informații pentru care există motive să se creadă că ar putea fi ilegală sau contrară vreunui ordin executiv sau vreunei directive prezidențiale. Pentru a asigura accesul IOB la informațiile necesare pentru îndeplinirea funcțiilor sale, Ordinul executiv nr. 13462 prevede că directorul Serviciului Național de Informații și șefii serviciilor de informații furnizează orice informații și asistență pe care IOB le consideră necesare pentru îndeplinirea funcțiilor sale, în măsura permisă de lege ([324]). La rândul său, IOB are obligația de a informa președintele cu privire la activitățile de colectare de informații cu privire la care consideră că încalcă legislația SUA (inclusiv ordinele executive) și nu sunt abordate în mod adecvat de procurorul general, de directorul Serviciului Național de Informații sau de șeful unui serviciu de informații ([325]). În plus, IOB are obligația de a informa procurorul general cu privire la posibilele încălcări ale dreptului penal.

(167) În al patrulea rând, serviciile de informații fac obiectul supravegherii de către PCLOB. În conformitate cu statutul său de constituire, PCLOB are responsabilități în domeniul politicilor de combatere a terorismului și al punerii în aplicare a acestora în vederea protejării vieții private și a libertăților civile. În cadrul evaluării efectuate cu privire la acțiunile serviciilor de informații, acesta poate avea acces la toate evidențele, rapoartele, auditurile, analizele, documentele, dosarele și recomandările, inclusiv la informații clasificate, poate desfășura interviuri și audia martori ([326]). Comitetul primește rapoarte de la responsabilii pentru protecția vieții private și a libertăților civile din mai multe departamente/agenții federale ([327]), poate emite recomandări pentru agențiile guvernamentale și serviciile de informații și prezintă rapoarte periodice către comisiile Congresului și către Președinte ([328]). Rapoartele comitetului, inclusiv cele adresate Congresului, trebuie puse la dispoziția publicului în cea mai mare măsură posibilă ([329]). PCLOB a emis mai multe rapoarte de supraveghere și monitorizare, inclusiv o analiză cu privire la programele derulate în temeiul secțiunii 702 din FISA și protecția vieții private în acest context, precum și cu privire la punerea în aplicare a PPD-28 și a OE nr. 12333 ([330]). PCLOB are, de asemenea, atribuții specifice de supraveghere în ceea ce privește

([318]) A se vedea articolul 6 din Legea privind inspectorii generali din 1978.

([319]) A se vedea *ibid* – articolele 4, 5 și 6.

([320]) În ceea ce privește acțiunile întreprinse în urma rapoartelor și a recomandărilor inspectorilor generali, a se vedea, de exemplu, răspunsul la un raport al inspectorului general al DoJ, care a constatat că FBI nu a fost suficient de transparent cu FISC în ceea ce privește cererile înaintate între 2014 și 2019, ceea ce a condus la reforme de consolidare a conformității, a supravegherii și a responsabilității FBI (de exemplu, directorul FBI a dispus peste 40 de acțiuni de remediere, inclusiv 12 măsuri specifice legate de procesul în baza FISA referitor la documentație, supraveghere, păstrarea dosarelor, instruire și auditori) (a se vedea https://www.justice.gov/opa/pr/department-justice-and-federal-bureau-investigation-announce-critical-reforms-enhance și https://oig.justice.gov/reports/2019/o20012.pdf). De asemenea, a se vedea, de pildă, auditul efectuat de inspectorul general al DoJ cu privire la rolul și responsabilitățile consilierului general al FBI în ceea ce privește supravegherea respectării legilor, a politicilor și a procedurilor aplicabile aferente activităților în materie de securitate națională ale FBI, precum și apendicele 2, care include o scrisoare din partea FBI prin care se acceptă toate recomandările. În acest sens, apendicele 3 oferă o imagine de ansamblu a acțiunilor subsecvente și a informațiilor pe care inspectorul general le-a solicitat de la FBI pentru a-și putea închide recomandările (https://oig.justice.gov/sites/default/files/reports/22-116.pdf).

([321]) A se vedea articolul 4 alineatul (5) și articolul 5 din Legea privind inspectorii generali din 1978.

([322]) A se vedea OE nr. 13462.

([323]) Secțiunea 1.6 litera (c) din OE nr. 12333.

([324]) Secțiunea 8 litera (a) din OE nr. 13462.

([325]) Secțiunea 6 litera (b) din OE nr. 13462.

([326]) Titlul 42 articolul 2000ee litera (g) din U.S.C.

([327]) A se vedea titlul 42 articolul 2000ee-1 litera (f) punctul 1 partea A subpunctul (iii) din U.S.C. Printre acestea se numără cel puțin Departamentul de Justiție, Departamentul Apărării, Departamentul pentru Securitate Internă, directorul Serviciului Național de Informații și Agenția Centrală de Informații (*Central Intelligence Agency*), precum și orice alt departament, agenție sau element al ramurii executive desemnate de PCLOB drept adecvate ca arie de acoperire.

([328]) Titlul 42 articolul 2000ee litera (e) din U.S.C.

([329]) Titlul 42 articolul 2000ee litera (f) din U.S.C.

([330]) Disponibile la adresa https://www.pclob.gov/Oversight.

punerea în aplicare a OE nr. 14086, în special prin evaluarea conformității procedurilor serviciilor cu ordinul executiv (a se vedea considerentul 126) și a funcționării corecte a mecanismului de recurs (a se vedea considerentul 194).

(168) În al cincilea rând, în plus față de mecanismul de supraveghere de la nivelul ramurii executive, o serie de comisii specifice din cadrul Congresului SUA (comisiile judiciare și comisiile pentru informații ale Camerei Reprezentanților și Senatului) au responsabilități de supraveghere cu privire la activitățile de colectare de informații externe ale SUA. Membrii acestor comisii au acces la informații clasificate, precum și la metode și programe care vizează colectarea de informații ([331]). Comisiile își exercită funcțiile de supraveghere în diferite moduri, în special prin audieri, investigații, analize și rapoarte ([332]).

(169) Comisiile Congresului primesc rapoarte periodice privind activitățile de colectare de informații, inclusiv din partea procurorului general, a directorului Serviciului Național de Informații, a serviciilor de informații și a altor organisme de supraveghere (de exemplu, inspectorii generali) – a se vedea considerentele 164-165. În special, în conformitate cu Legea privind securitatea națională, „[p]reședintele se asigură că respectivele comisii pentru informații ale Congresului sunt ținute la curent pe deplin cu privire la activitățile de colectare de informații ale Statelor Unite ale Americii, inclusiv orice cu privire la orice activitate semnificativă anticipată de colectare de informații în conformitate cu cerințele acestui subcapitol” ([333]). De asemenea, „[p]reședintele se asigură că orice activitate ilegală de colectare de informații, precum și orice măsuri de remediere care au fost luate sau sunt planificate în legătură cu o astfel de activitate ilegală sunt raportate imediat comisiilor pentru informații ale Congresului” ([334]).

(170) În plus, din legile specifice decurg o serie de cerințe de raportare suplimentare. În special, FISA impune procurorului general să „informeze pe deplin” comisiile pentru informații și comisiile judiciare ale Camerei Reprezentanților și Senatului cu privire la activitățile autorităților desfășurate în temeiul anumitor secțiuni din FISA ([335]). De asemenea, FISA impune autorităților să furnizeze comisiilor din cadrul Congresului copii după toate deciziile, ordinele sau avizele FISC sau FISCR care includ „o interpretare semnificativă a dispozițiilor FISA”. În ceea ce privește supravegherea în temeiul secțiunii 702 din FISA, supravegherea parlamentară este exercitată prin rapoarte prevăzute de lege către comisiile pentru informații și comisiile judiciare, precum și prin 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 rapoarte de conformitate ale Departamentului de Justiție și ODNI și o descriere a oricăror incidente de neconformitate ([336]), precum și o evaluare semestrială separată efectuată de către procurorul general și DNI privind respectarea procedurilor de direcționare și de reducere la minimum a intervențiilor ([337]).

([331]) Titlul 50 articolul 3091 din U.S.C.

([332]) De exemplu, comisiile organizează audieri tematice [a se vedea, de exemplu, o audiere recentă a comisiei judiciare a Camerei Reprezentanților pe tema „raziilor digitale” (*digital dragnets*) – https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983] și o audiere a comisiei pentru informații a Camerei Reprezentanților privind utilizarea IA de către Comunitatea Serviciilor de Informații, https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=114263], precum și audieri de supraveghere periodice, de exemplu a diviziei de securitate națională a DoJ și a FBI – a se vedea https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation; https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 și https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899. Un exemplu de investigație îl reprezintă investigația comisiei pentru informații a Senatului cu privire la imixtiunea Rusiei în alegerile din SUA din 2016 – a se vedea https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures. În ceea ce privește raportarea, a se vedea, de exemplu, prezentarea generală a activităților (de supraveghere) ale comisiei din raportul comisiei pentru informații a Senatului care vizează perioada 4 ianuarie 2019-3 ianuarie 2021 către Senat, https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-covering-period-january-4.

([333]) A se vedea titlul 50 articolul 3091 litera (a) punctul 1 din U.S.C. Această dispoziție conține cerințele generale în ceea ce privește supravegherea Congresului în domeniul securității naționale.

([334]) A se vedea titlul 50 articolul 3091 litera (b) din U.S.C.

([335]) A se vedea titlul 50 articolele 1808, 1846, 1862, 1871 și 1881f din U.S.C.

([336]) A se vedea titlul 50 articolul 1881f din U.S.C.

([337]) A se vedea titlul 50 articolul 1881a litera (l) punctul 1 din U.S.C.

(171) În plus, FISA impune autorităților SUA să comunice Congresului (și publicului larg) în fiecare an, printre altele, numărul de ordine în temeiul FISA solicitate și primite, precum și estimări ale numărului de persoane care sunt cetățeni americani/rezidenți în SUA și care nu sunt cetățeni americani/rezidenți SUA vizate de supraveghere ([338]). Legea impune, de asemenea, o raportare publică suplimentară cu privire la numărul de NSL emise, atât în ceea ce privește persoanele care sunt cetățeni americani/rezidenți în SUA, cât și persoanele care nu sunt cetățeni americani/rezidenți în SUA (permițând, în același timp, destinatarilor ordinelor și certificărilor FISA, precum și ai cererilor de NSL, să prezinte rapoarte de transparență în anumite condiții) ([339]).

(172) La un nivel mai general, Comunitatea Serviciilor de Informații depune diverse eforturi de a asigura transparența activităților sale de colectare de informații (externe). De exemplu, în 2015, ODNI a adoptat principii privind transparența serviciilor de informații și un plan de punere în aplicare în materie de transparență și a impus fiecărui serviciu de informații să desemneze un responsabil pentru transparența serviciului de informații pentru a promova transparența și a conduce inițiative în materie de transparență ([340]). Ca parte a acestor eforturi, serviciile de informații au făcut și continuă să facă publice părți declasificate ale politicilor, procedurilor, rapoartelor de supraveghere, rapoartelor privind activitățile desfășurate în temeiul secțiunii 702 din FISA și OE nr. 12333, precum și ale deciziilor FISC și ale altor materiale, inclusiv pe o pagină web specifică gestionată de ODNI, și anume „IC on the Record" ([341]).

(173) În cele din urmă, în plus față de supravegherea de către organismele de supraveghere menționate în considerentele 162-168, colectarea datelor cu caracter personal în temeiul secțiunii 702 din FISA face obiectul supravegherii FISC ([342]). În conformitate cu Norma nr. 13 din Regulamentul de procedură al FISC, funcționarii cu atribuții de conformitate din cadrul serviciilor de informații din SUA au obligația de a raporta orice încălcare a procedurilor de direcționare și de reducere la minimum a intervențiilor și a procedurilor de interogare în temeiul articolului 702 din FISA către DoJ și ODNI, care, la rândul lor, le raportează FISC. În plus, DoJ și ODNI prezintă FISC rapoarte semestriale comune de evaluare a activității de supraveghere, care identifică tendințele în ceea ce privește respectarea procedurilor de direcționare a intervențiilor, oferă date statistice, descriu categorii de incidente legate de conformitate, descriu în detaliu motivele pentru care au intervenit anumite incidente legate de respectarea procedurilor de direcționare a intervențiilor și precizează măsurile pe care le-au luat serviciile de informații pentru a evita recurența acestora ([343]).

(174) În cazul în care este necesar (de exemplu, în cazul în care se identifică încălcări ale procedurilor de direcționare a intervențiilor), curtea poate solicita serviciului de informații relevant să ia măsuri de remediere ([344]). Acestea pot varia de la măsuri individuale la măsuri structurale, de exemplu, de la încetarea acțiunii de obținere a datelor sau ștergerea datelor obținute în mod ilegal până la o modificare a practicii de colectare, inclusiv în ceea ce privește orientările pentru personal și formarea acestuia ([345]). În plus, în cursul revizuirii sale anuale a certificărilor în temeiul

([338]) Titlul 50 articolul 1873 litera (b) din U.S.C. 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, a fiecărui ordin sau a fiecărui aviz emis(e) de Curtea de Supraveghere a Activităților Străine de Spionaj sau de Curtea de Reexaminare a Supravegherii Activităților Străine de Spionaj [astfel cum sunt definite la secțiunea 601 litera (e)] care include o interpretarea semnificativă a oricărei dispoziții legale, inclusiv orice interpretare semnificativă sau nouă a noțiunii «termen de selecție specific» și, în concordanță cu această analiză, pune la dispoziția publicului, în măsura posibilului, fiecare astfel de decizie, ordin sau aviz".

([339]) A se vedea titlul 50 articolul 1873 litera (b) punctul 7 și articolul 1874 din U.S.C.

([340]) https://www.dni.gov/index.php/ic-legal-reference-book/the-principles-of-intelligence-transparency-for-the-ic.

([341]) A se vedea „IC on the Record", disponibilă la adresa https://icontherecord.tumblr.com/.

([342]) În trecut, FISC a concluzionat că „[î]n opinia Curții, agențiile de punere în aplicare, precum și [ODNI] și [divizia de securitate națională a DoJ] alocă resurse substanțiale responsabilităților lor de asigurare a conformității și de supraveghere în temeiul secțiunii 702. Ca regulă generală, cazurile de neconformitate sunt identificate cu promptitudine și se iau măsuri de remediere adecvate, care includ eliminarea informațiilor care au fost obținute în mod necorespunzător sau care au făcut în alt mod obiectul cerințelor de distrugere în conformitate cu procedurile aplicabile". Curtea FISA, Aviz memorandum și ordin [mențiune omisă] (2014), disponibil la adresa https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.

([343]) A se vedea, de exemplu, raportul DOJ/ODNI privind conformitatea în temeiul articolului 702 din FISA adresat FISC pentru perioada iunie 2018-noiembrie 2018 – 21-65.

([344]) Titlul 50 articolul 1803 litera (h) din U.S.C. A se vedea, de asemenea, raportul PCLOB cu privire la secțiunea 702, p. 76. În plus, a se vedea Avizul memorandum și ordinul FISC din 3 octombrie 2011 ca exemplu de ordin de constatare a deficiențelor prin care autoritățile au fost obligate să corecteze deficiențele identificate în termen de 30 de zile, disponibil la adresa https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf. A se vedea scrisoarea Walton, secțiunea 4, p. 10-11. A se vedea, de asemenea, Avizul FISC din 18 octombrie 2018, disponibil la adresa https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, astfel cum a fost confirmat de Curtea de Reexaminare a Supravegherii Activităților Străine de Spionaj în Avizul său din 12 iulie 2019, disponibil la adresa https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf, prin care FISC a impus autorităților, printre altele, să respecte anumite cerințe de notificare, documentare și raportare către FISC.

([345]) A se vedea, de exemplu, Avizul memorandum și ordinul FISC – 76 (6 decembrie 2019) (autorizat pentru publicare la 4 septembrie 2020), prin care FISC a solicitat autorităților să prezinte, până la 28 februarie 2020, un raport scris cu privire la măsurile luate pentru a îmbunătăți procesele de identificare și de eliminare a rapoartelor obținute în baza informațiilor colectate în temeiul articolului 702 din FISA care au fost rechemate din motive legate de conformitate, precum și cu privire la alte aspecte. A se vedea, de asemenea, anexa VII.

secțiunii 702, FISC ține seama de incidentele de neconformitate pentru a stabili dacă certificările prezentate respectă cerințele FISA. În mod similar, în cazul în care FISC constată că respectivele certificări ale autorităților nu au fost suficiente, inclusiv ca urmare a unor incidente specifice de conformitate, aceasta poate emite un așa-numit „ordin de constatare a deficiențelor" prin care le solicită acestora să remedieze încălcarea în termen de 30 de zile sau să înceteze sau să nu demareze punerea în aplicare a certificării în temeiul secțiunii 702. În sfârșit, FISC evaluează tendințele pe care le observă în ceea ce privește aspectele legate de conformitate și poate impune modificarea procedurilor sau măsuri suplimentare de supraveghere și de raportare pentru a aborda tendințele în materie de conformitate ([346]).

3.2.3 ***Căi de atac***

(175) Astfel cum se explică mai detaliat în prezenta secțiune, Statele Unite ale Americii oferă persoanelor vizate din Uniune o serie de posibilități de a introduce o acțiune în justiție în fața unei instanțe judecătorești independente și imparțiale, cu competențe obligatorii. Împreună, acestea permit persoanelor să aibă acces la datele lor cu caracter personal, să solicite revizuirea legalității accesului autorităților la datele lor și, în cazul în care se constată o încălcare, să obțină remedierea acestei încălcări, inclusiv prin rectificarea sau ștergerea datelor lor cu caracter personal.

(176) În primul rând, în temeiul OE nr. 14086, astfel cum este completat de Regulamentul PG de instituire a Curții de Reexaminare a Protecției Datelor, se instituie un mecanism specific de recurs pentru a gestiona și soluționa plângerile înaintate de persoane referitoare la activitățile SUA de colectare de informații de tip SIGINT. Orice persoană din UE are dreptul de a înainteze o plângere mecanismului de recurs cu privire la o presupusă încălcare a legislației SUA care reglementează activitățile de colectare de informații de tip SIGINT (de exemplu, OE nr. 14086, secțiunea 702 din FISA, OE nr. 12333) care îi afectează în mod negativ interesele din perspectiva vieții private și a libertăților civile ([347]). Acest mecanism de recurs este disponibil pentru persoane din țări sau organizații regionale de integrare economică care au fost desemnate de procurorul general al SUA drept „state eligibile" ([348]). La 30 iunie 2023, Uniunea Europeană și cele trei țări membre ale Asociației Europene a Liberului Schimb, care constituie împreună Spațiul Economic European, au fost desemnate de procurorul general al SUA, în temeiul secțiunii 3 litera (f) din OE nr. 14086, drept „stat eligibil" ([349]). Această desemnare nu aduce atingere articolului 4 alineatul (2) din Tratatul privind Uniunea Europeană.

(177) O persoană vizată care dorește să înainteze o astfel de plângere trebuie să o depună la o autoritate de supraveghere dintr-un stat membru al UE competentă să supravegheze prelucrarea datelor cu caracter personal de către autoritățile publice (o APD) ([350]). Acest lucru asigură un acces facil la mecanismul de recurs, permițând persoanelor să apeleze la o autoritate „aproape de casă" și cu care pot comunica în propria limbă. După ce se verifică cerințele pentru depunerea unei plângeri, menționate în considerentul 178, APD competentă, prin intermediul secretariatului Comitetului european pentru protecția datelor, va direcționa plângerea către mecanismul de recurs.

(178) Înaintarea unei plângeri mecanismului de recurs face obiectul unor cerințe de admisibilitate scăzute, iar persoanele nu trebuie să demonstreze că datele acestora au făcut, în fapt, obiectul activităților SUA de colectare de informații de tip SIGINT ([351]). În același timp, pentru a oferi un punct de plecare pentru examinarea cauzei de către mecanismul de recurs, trebuie furnizate anumite informații de bază, de exemplu, cu privire la datele cu caracter personal despre care se presupune în mod rezonabil că au fost transferate către SUA și la mijloacele prin care se crede că au fost transferate, Identitățile entităților guvernamentale din SUA despre care se crede că sunt implicate în presupusa încălcare (dacă sunt cunoscute), temeiul în baza căruia se susține că a avut loc o încălcare a legislației SUA (deși acest lucru nu necesită demonstrarea faptului că datele cu caracter personal au fost, în fapt, colectate de serviciile de informații din SUA) și natura măsurii reparatorii solicitate.

([346]) A se vedea anexa VII.

([347]) A se vedea secțiunea 4 litera (k) punctul (iv) din OE nr. 14086, care prevede că o plângere înaintată mecanismului de recurs trebuie depusă de un reclamant care acționează în nume propriu (și anume nu în calitate de reprezentant al unui organizații guvernamentale, neguvernamentale sau interguvernamentale). Noțiunea de „afectată în mod negativ" nu impune reclamantului să respecte un anumit prag pentru a avea acces la mecanismul de recurs (a se vedea considerentul 178 în acest sens). Mai degrabă, aceasta clarifică faptul că CLPO ODNI și DPRC au competența de a remedia încălcările prevederilor legislației SUA de reglementare a activităților de colectare de informații de tip SIGINT care afectează în mod negativ interesele individuale ale reclamantului în ceea ce privește viața privată și libertățile civile. În schimb, încălcările cerințelor prevăzute de legislația aplicabilă a SUA care nu sunt concepute pentru a proteja persoanele (de exemplu, cerințele bugetare) nu ar intra în sfera de competență a CLPO ODNI și a DPRC.

([348]) Secțiunea 3 litera (f) din OE nr. 14086.

([349]) https://www.justice.gov/opcl/executive-order-14086.

([350]) Secțiunea 4 litera (d) punctul (v) din OE nr. 14086.

([351]) A se vedea secțiunea 4 litera (k) punctele (i)-(iv) din OE nr. 14086.

(179) Investigarea inițială a plângerilor înaintate acestui mecanism de recurs este efectuată de CLPO ODNI, ale cărui rol și competențe legale existente au fost extinse pentru acele acțiuni specifice întreprinse în temeiul OE nr. 14086 ([352]). În cadrul Comunității Serviciilor de Informații, CLPO este, printre altele, responsabil pentru asigurarea faptului că protecția libertăților civile și a vieții private este integrată în mod corespunzător în politicile și procedurile ODNI și ale serviciilor de informații, supravegherea respectării de către ODNI a cerințelor aplicabile privind libertățile civile și viața privată și realizarea de evaluări ale impactului din perspectiva vieții private ([353]). CLPO ODNI poate fi revocat din funcție de directorul Serviciului Național de Informații numai din motive întemeiate, și anume pentru comiterea unei abateri, practici ilicite, încălcarea securității, neglijență în serviciu sau incapacitate ([354]).

(180) În activitatea sa de examinare a unei plângeri, CLPO ODNI are acces la informații pentru realizarea evaluării sale și poate apela la sprijinul obligatoriu al responsabililor pentru protecția vieții private și a libertăților civile din cadrul diferitelor servicii de informații ([355]). Serviciilor de informații le este interzis să împiedice sau să influențeze în mod necorespunzător activitatea de examinare a plângerilor desfășurată de CLPO ODNI. În mod similar, nici directorul Serviciului Național de Informații nu se poate implica în această activitate ([356]). Atunci când examinează o plângere, CLPO ODNI trebuie să aplice legea „în mod imparțial", având în vedere atât interesele naționale în materie de securitate vizate de activitățile de colectare de informații de tip SIGINT, cât și protecția vieții private ([357]).

(181) În cadrul activității sale de examinare a unei plângeri, CLPO ODNI stabilește dacă a avut loc o încălcare a legislației SUA aplicabile și, în caz afirmativ, decide cu privire la o remediere adecvată ([358]). Aceasta din urmă se referă la măsuri care remediază pe deplin o încălcare identificată, cum ar fi încetarea obținerii ilegale de date, ștergerea datelor colectate în mod ilegal, ștergerea rezultatelor interogărilor efectuate necorespunzător cu privire la date colectate în mod legal, restricționarea accesului la datele colectate în mod legal la personalul instruit în mod corespunzător sau rechemarea rapoartelor de informații care conțin date obținute fără deținerea unei autorizări legale în acest sens sau care au fost diseminate în mod ilegal ([359]). Deciziile CLPO ODNI cu privire la plângerile individuale (inclusiv cu privire la măsurile de remediere) sunt obligatorii pentru serviciile de informații în cauză ([360]).

(182) CLPO ODNI trebuie să păstreze documentația privind activitatea sa de examinare a plângerii și să emită o decizie clasificată în care să explice temeiurile constatărilor sale în fapt, concluzia cu privire la existența unei încălcări eligibile și remedierea adecvată stabilită ([361]). În cazul în care activitatea de examinare a plângerii desfășurată de CLPO ODNI indică o încălcare de către orice autoritate care face obiectul supravegherii FISC, CLPO trebuie, de asemenea, să prezinte un raport clasificat procurorului general adjunct pentru securitate națională, care, la rândul său, are obligația de a raporta neconformitatea respectivă către FISC, care poate lua măsuri suplimentare de asigurare a respectării legii (în conformitate cu procedura descrisă în considerentele 173-174) ([362]).

(183) Odată finalizată activitatea de examinare a plângerii, CLPO ODNI informează reclamantul că „examinarea fie nu a identificat încălcări eligibile, fie CLPO ODNI a emis o decizie care impune o remediere adecvată" ([363]). Acest lucru permite protejarea confidențialității activităților desfășurate pentru a proteja securitatea națională, oferind în același timp persoanelor o decizie prin care se confirmă investigarea și soluționarea corespunzătoare a plângerii. În plus, această decizie poate fi contestată de persoana în cauză. În acest scop, aceasta va fi informată cu privire la posibilitatea de a introduce o cale de atac la DPRC și să solicite o reexaminare a constatărilor CLPO (a se vedea considerentul 184 și următoarele) și că, în cazul în care este sesizată această instanță, se va alege un avocat special care să susțină interesul reclamantului ([364]).

([352]) Secțiunea 3 litera (c) punctul (iv) din OE nr. 14086. A se vedea, de asemenea, Legea privind securitatea națională din 1947, titlul 50 articolul 403-3d din U.S.C. – secțiunea 103D privind rolul CLPO în cadrul ODNI.
([353]) Titlul 50 articolul 3029 litera (b) din U.S.C.
([354]) Secțiunea 3 litera (c) punctul (iv) din OE nr. 14086.
([355]) Secțiunea 3 litera (c) punctul (iii) din OE nr. 14086.
([356]) Secțiunea 3 litera (c) punctul (iv) din OE nr. 14086.
([357]) Secțiunea 3 litera (c) punctul (i) partea B subpunctele (i) și (iii) din OE nr. 14086.
([358]) Secțiunea 3 litera (c) punctul (i) din OE nr. 14086.
([359]) Secțiunea 4 litera (a) din OE nr. 14086.
([360]) Secțiunea 3 literele (c) și (d) din OE nr. 14086.
([361]) Secțiunea 3 litera (c) punctul (i) părțile F-G din OE nr. 14086.
([362]) A se vedea, de asemenea, secțiunea 3 litera (c) punctul (i) partea D din OE nr. 14086.
([363]) Secțiunea 3 litera (c) punctul (i) partea E subpunctul 1 din OE nr. 14086.
([364]) Secțiunea 3 litera (c) punctul (i) partea E subpunctele 2-3 din OE nr. 14086.

(184) Orice reclamant, precum și fiecare element al Comunității Serviciilor de Informații, poate solicita reexaminarea deciziei CLPO ODNI de către Curtea de Reexaminare a Protecției Datelor (DPRC). Astfel de cereri de reexaminare trebuie depuse în termen de 60 de zile de la primirea notificării din partea CLPO ODNI cu privire la faptul că examinarea plângerii de către acesta s-a încheiat și includ orice informații pe care persoana în cauză dorește să le furnizeze DPRC (de exemplu, argumente privind aspecte de drept sau aplicarea legii la situația de fapt a cauzei) ([365]). Persoanele vizate din Uniune pot înainta din nou cererea APD competente (a se vedea considerentul 177).

(185) DPRC este o instanță judecătorească independentă înființată de procurorul general în temeiul OE nr. 14086 ([366]). Aceasta este formată din cel puțin șase judecători, numiți de procurorul general în consultare cu PCLOB, Secretarul pentru Comerț și directorul Serviciului Național de Informații pentru mandate reînnoibile de patru ani ([367]). Numirea judecătorilor de către procurorul general se bazează pe criteriile utilizate de ramura executivă atunci când evaluează candidații la sistemul judiciar federal, acordând importanță oricărei experiențe judiciare anterioare ([368]). În plus, judecătorii trebuie să fie practicieni în domeniul dreptului (și anume membri activi înscriși în barou și autorizați în mod corespunzător să exercite o profesie juridică) și să aibă experiență adecvată în domeniul legislației privind viața privată și securitatea națională. Procurorul general trebuie să depună eforturi pentru a se asigura că, în orice moment, cel puțin jumătate dintre judecători au experiență judiciară anterioară și toți judecătorii trebuie să dețină autorizații de securitate pentru a putea avea acces la informații clasificate privind securitatea națională ([369]).

(186) Numai persoanele care îndeplinesc condițiile menționate în considerentul 185 și nu sunt angajați ai ramurii executive la momentul numirii lor sau în ultimii doi ani pot fi numite în componența DPRC. În mod similar, pe durata mandatului lor în cadrul DPRC, judecătorii nu pot deține nicio altă funcție oficială în cadrul guvernului SUA (cu excepția celei de judecători în cadrul DPRC) ([370]).

(187) Independența procesului de judecată se realizează printr-o serie de garanții. În special, ramurii executive (procurorului general și serviciilor de informații) îi este interzis să intervină sau să influențeze în mod necorespunzător activitatea de reexaminare a DPRC ([371]). DPRC trebuie să soluționeze în mod imparțial cauzele ([372]) și funcționează în conformitate cu propriul său regulament de procedură (adoptat cu majoritate de voturi). În plus, judecătorii DPRC pot fi revocați din funcție numai de procurorul general și numai din motive întemeiate (și anume pentru comiterea unei abateri, practici ilicite, încălcarea securității, neglijență în serviciu sau incapacitate), după luarea în considerare în mod corespunzător a standardelor aplicabile judecătorilor federali prevăzute în Normele de procedură privind conduita judecătorilor și incapacitatea acestora de a-și desfășura activitatea ([373]).

([365]) Secțiunea 201.6 literele (a)-(b) din Regulamentul PG.

([366]) Secțiunea 3 litera (d) punctul (i) din Regulamentul PG. Curtea Supremă a Statelor Unite a Americii a recunoscut posibilitatea ca procurorul general să înființeze organisme independente cu competențe decizionale, inclusiv cu competența de a soluționa cauze individuale – a se vedea în special Statele Unite ale Americii *ex rel.* Accardi/Shaughnessy, 347 U.S. 260 (1954) și Statele Unite ale Americii/Nixon, 418 U.S. 683, 695 (1974). Respectarea diferitelor cerințe ale OE nr. 14086, de exemplu criteriile și procedura de numire și de revocare din funcție a judecătorilor DPRC, face în special obiectul supravegherii inspectorului general al Departamentului de Justiție (a se vedea, de asemenea, considerentul 109 privind competența statutară a inspectorilor generali).

([367]) Secțiunea 3 litera (d) punctul (i) partea A din OE nr. 14086 și articolul 201.3 litera (a) din Regulamentul PG.

([368]) Secțiunea 201.3 litera (b) din Regulamentul PG.

([369]) Secțiunea 3 litera (d) punctul (i) partea B din OE nr. 14086.

([370]) Secțiunea 3 litera (d) punctul (i) partea A din OE nr. 14086 și secțiunea 201.3 literele (a) și (c) din Regulamentul PG. Persoanele numite în cadrul DPRC pot participa la activități extrajudiciare, inclusiv la activități comerciale, financiare, de strângere de fonduri fără scop lucrativ și la activități fiduciare, putând, se asemenea, practica dreptul, atât timp cât aceste activități nu interferează cu îndeplinirea imparțială a îndatoririlor lor sau cu eficacitatea sau independența DPRC [secțiunea 201.7 litera (c) din Regulamentul PG].

([371]) Secțiunea 3 litera (d) punctele (iii)-(iv) din OE nr. 14086 și secțiunea 201.7 litera (d) din Regulamentul PG.

([372]) Secțiunea 3 litera (d) punctul (i) partea D din OE nr. 14086 și secțiunea 201.9 din Regulamentul PG.

([373]) Secțiunea 3 litera (d) punctul (iv) din OE nr. 14086 și articolul 201.7 litera (d) din Regulamentul PG. A se vedea, de asemenea, hotărârea Bumap/Statele Unite, 252 U.S. 512, 515 (1920), care a confirmat principiul de lungă durată din legislația SUA, potrivit căruia competența de revocare din funcție este accesorie în raport cu competența de numire [astfel cum a reamintit, de asemenea, Biroul de asistență juridică al DoJ în documentul intitulat *The Constitutional Separation of Powers Between the President and Congress* (Separarea constituțională a competențelor între președinte și Congres), 20 Op. O.L.C. 124, 166 (1996)].

(188) Cererile înaintate DPRC sunt examinate de completuri de trei judecători, care includ un președinte al completului; acestea trebuie să acționeze în conformitate cu Codul de conduită al judecătorilor din SUA ([374]). Fiecare complet este asistat de un avocat special ([375]), care are acces la toate informațiile referitoare la cauză, inclusiv la informații clasificate ([376]). Rolul avocatului special este de a se asigura că interesele reclamantului sunt reprezentate și că respectivul complet al DPRC este bine informat cu privire la toate aspectele relevante de drept și de fapt ([377]). Pentru a-și fundamenta suplimentar poziția cu privire la o cerere de reexaminare adresată DPRC de către o persoană, avocatul special poate solicita informații de la reclamant prin intermediul unor întrebări scrise ([378]).

(189) DPRC reexaminează constatările CLPO ODNI (atât în ceea ce privește eventuala încălcare a legislației SUA aplicabile, cât și în ceea ce privește remedierea adecvată), cel puțin pe baza evidențelor investigației CLPO ODNI, precum și orice informații și observații furnizate de reclamant, de avocatul special sau de un serviciu de informații ([379]). Un complet DPRC are acces la toate informațiile necesare pentru efectuarea unei reexaminări, pe care le poate obține prin intermediul CLPO ODNI (de exemplu, completul poate solicita CLPO să își completeze dosarul cu informații suplimentare sau constatări factuale, dacă acest lucru este necesar pentru efectuarea reexaminării) ([380]).

(190) La încheierea reexaminării sale, DPRC poate (1) să decidă că nu există elemente de probă care să indice că au avut loc activități de colectare de informații de tip SIGINT care implică date cu caracter personal ale reclamantului, (2) să decidă că respectivele constatări ale CLPO ODNI au fost corecte din punct de vedere juridic și sunt susținute de elemente de probă substanțiale sau (3) în cazul în care DPRC nu este de acord cu constatările CLPO ODNI (în ceea ce privește eventuala încălcare a legislației SUA aplicabile sau remedierea adecvată), să emită propriile constatări ([381]).

([374]) Secțiunea 3 litera (d) punctul (i) partea B din OE nr. 14086 și articolul 201.7 literele (a)-(c) din Regulamentul PG. Biroul pentru protecția vieții private și a libertăților civile din cadrul Departamentului de Justiție (OPCL), care este responsabil cu furnizarea de sprijin administrativ DPRC și avocaților speciali (a se vedea secțiunea 201.5 din Regulamentul PG), selectează un complet format din trei persoane, prin rotație, asigurându-se că fiecare complet are cel puțin un judecător cu experiență judiciară anterioară (în cazul în care niciunul dintre judecătorii completului nu are o astfel de experiență, președintele completului va fi judecătorul ales pentru prima dată de OPCL).

([375]) Secțiunea 201.4 din Regulamentul PG. Procurorul general numește cel puțin doi avocați speciali, în consultare cu Secretarul pentru Comerț, directorul Serviciului Național de Informații și PCLOB, pentru două mandate reînnoibile. Avocații speciali trebuie să aibă experiență adecvată în domeniul legislației privind viața privată și securitatea națională, să fie avocați experimentați, membri activi înscriși în barou și autorizați în mod corespunzător să exercite o profesie juridică. În plus, la momentul numirii lor inițiale, aceștia nu trebuie să fi fost angajați ai ramurii executive în ultimii doi ani. Pentru fiecare reexaminare a unei cereri, președintele completului alege un avocat special care să asiste completul de judecată – a se vedea secțiunea 201.8 litera (a) din Regulamentul PG.

([376]) Secțiunea 201.8 litera (c) și secțiunea 201.11 din Regulamentul PG.

([377]) Secțiunea 3 litera (d) punctul (i) partea C din OE nr. 14086 și secțiunea 201.8 litera (e) din Regulamentul PG. Avocatul special nu acționează în calitate de reprezentant al reclamantului și, între acesta și reclamant, nu există o relație de tipul celei între un avocat și clientul său.

([378]) A se vedea secțiunea 201.8 literele (d) și (e) din Regulamentul PG. Aceste întrebări sunt examinate mai întâi de OPCL, în consultare cu elementul relevant al Comunității Serviciilor de Informații, în vederea identificării și a excluderii oricăror informații clasificate sau privilegiate sau protejate înainte de a le transmite reclamantului. Informațiile suplimentare primite de avocatul special ca răspuns la astfel de întrebări sunt incluse în observațiile avocatului special adresate DPRC.

([379]) Secțiunea 3 litera (d) punctul (i) partea D din OE nr. 14086.

([380]) Secțiunea 3 litera (d) punctul (iii) din OE nr. 14086 și articolul 201.9 litera (b) din Regulamentul PG.

([381]) Secțiunea 3 litera (d) punctul (i) partea E din OE nr. 14086 și articolul 201.9 literele (c)-(e) din Regulamentul PG. Conform definiției „remedierii adecvate" din secțiunea 4 litera (a) din OE nr. 14086, DPRC trebuie să ia în considerare „modalitățile prin care o încălcare de tipul celei identificate a fost abordată în mod obișnuit" atunci când decide cu privire la o măsură de remediere pentru a aborda pe deplin o încălcare, și anume DPRC va lua în considerare, printre alți factori, modul în care probleme similare de conformitate au fost remediate în trecut pentru a se asigura că remedierea este eficace și adecvată.

(191) În toate cazurile, DPRC adoptă o decizie scrisă cu majoritate de voturi. În cazul în care reexaminarea identifică o încălcare a normelor aplicabile, decizia va specifica orice remediere adecvată, care include ștergerea datelor colectate în mod ilegal, ștergerea rezultatelor interogărilor efectuate necorespunzător, restricționarea accesului la datele colectate în mod legal la personalul instruit în mod corespunzător sau rechemarea rapoartelor de informații care conțin date obținute fără deținerea unei autorizări legale în acest sens sau care au fost diseminate în mod ilegal ([382]). Decizia DPRC este obligatorie și definitivă în ceea ce privește plângerea cu care este sesizată ([383]). În plus, în cazul în care reexaminarea indică o încălcare de către orice autoritate care face obiectul supravegherii FISC, DPRC trebuie, de asemenea, să prezinte un raport clasificat procurorului general adjunct pentru securitate națională, care, la rândul său, are obligația de a raporta neconformitatea respectivă către FISC, care poate lua măsuri suplimentare de asigurare a respectării legii (în conformitate cu procedura descrisă în considerentele 173-174) ([384]).

(192) Fiecare decizie a unui complet DPRC este transmisă CLPO ODNI ([385]). În cazurile în care reexaminarea de către DPRC a fost inițiată în urma unei cereri din partea reclamantului, reclamantul este informat prin intermediul autorității naționale că DPRC și-a finalizat reexaminarea și că „reexaminarea fie nu a identificat încălcări eligibile, fie DPRC a emis o decizie care impune o remediere adecvată” ([386]). Biroul pentru protecția vieții private și a libertăților civile din cadrul DoJ păstrează o evidență a tuturor informațiilor reexaminate de DPRC și a tuturor deciziilor emise, care sunt puse la dispoziție spre consultare ca precedent fără caracter obligatoriu pentru viitoarele completuri DPRC ([387]).

(193) De asemenea, DoC are obligația de a păstra o evidență pentru fiecare reclamant care a depus o plângere ([388]). Pentru a spori transparența, cel puțin o dată la cinci ani, DoC trebuie să contacteze serviciile de informații relevante pentru a verifica dacă informațiile referitoare la o reexaminare efectuată de DPRC au fost declasificate ([389]). În acest caz, persoanei în cauză i se va notifica faptul că astfel de informații pot fi disponibile în temeiul legislației aplicabile (și anume că aceasta poate solicita accesul la aceste informații în temeiul Legii privind libertatea de informare – a se vedea considerentul 199).

(194) În sfârșit, funcționarea corectă a acestui mecanism de recurs va face obiectul unei evaluări periodice independente. Mai precis, în conformitate cu OE nr. 14086, funcționarea mecanismului de recurs face obiectul unei reexaminări anuale de către PCLOB, un organism independent (a se vedea considerentul 110) ([390]). În cadrul acestei activități, PCLOB va evalua, printre altele, dacă CLPO ODNI și DPRC au gestionat plângerile în timp util, dacă au obținut acces deplin la informațiile necesare, dacă garanțiile de fond prevăzute de OE nr. 14086 au fost luate în considerare în mod corespunzător în procesul de reexaminare și dacă serviciile de informații au respectat pe deplin constatările CLPO ODNI și DPRC. PCLOB va prezenta un raport privind rezultatul reexaminării sale președintelui, procurorului general, directorului Serviciului Național de Informații, șefilor serviciilor de informații, CLPO ODNI și comisiilor pentru informații ale Congresului, care va fi, de asemenea, făcut public într-o versiune neclasificată – și, la rândul său, va contribui la revizuirea periodică a funcționării prezentei decizii, care va fi efectuată de Comisie. Procurorul general, directorul Serviciului Național de Informații, CLPO ODNI și șefii serviciilor de informații sunt obligați să pună în aplicare sau să abordeze în alt mod toate recomandările incluse în astfel de rapoarte. În plus, PCLOB va emite o certificare anuală publică cu privire la conformitatea instrumentării plângerilor de către mecanismul de recurs cu cerințele OE nr. 14086.

([382]) Secțiunea 4 litera (a) din OE nr. 14086.

([383]) Secțiunea 3 litera (d) punctul (ii) din OE nr. 14086 și secțiunea 201.9 litera (g) din Regulamentul PG. Având în vedere că decizia DPRC este definitivă și obligatorie, nicio altă instituție/organism executiv(ă) sau administrativ(ă) (inclusiv președintele Statelor Unite) nu poate anula decizia DPRC. Acest lucru a fost confirmat, de asemenea, în jurisprudența Curții Supreme, care a clarificat faptul că, prin delegarea către un organism independent a competenței unice a procurorului general în cadrul ramurii executive de a emite decizii obligatorii, procurorul general își contestă capacitatea de a dicta decizia organismului respectiv în orice mod (a se vedea Statele Unite ale Americii *ex rel.* Accardi/Shaughnessy, 347 U.S. 260 (1954).

([384]) Secțiunea 3 litera (d) punctul (i) partea F din OE nr. 14086 și secțiunea 201.9 litera (i) din Regulamentul PG.

([385]) Secțiunea 201.9 litera (h) din Regulamentul PG.

([386]) Secțiunea 3 litera (d) punctul (i) partea H din OE nr. 14086 și secțiunea 201.9 litera (h) din Regulamentul PG. În ceea ce privește natura notificării, a se vedea secțiunea 201.9 litera (h) punctul 3 din Regulamentul PG.

([387]) Secțiunea 201.9 litera (j) din Regulamentul PG.

([388]) Secțiunea 3 litera (d) punctul (v) partea A din OE nr. 14086.

([389]) Secțiunea 3 litera (d) punctul (v) din OE nr. 14086.

([390]) Secțiunea 3 litera (e) din OE nr. 14086. A se vedea, de asemenea, https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf.

(195) Pe lângă mecanismul specific de recurs instituit în temeiul OE nr. 14086, toate persoanele (indiferent de cetățenie sau de locul de reședință) au la dispoziție căi de atac înaintea instanțelor de drept comun din SUA ([391]).

(196) În special, FISA și o lege conexă prevăd posibilitatea ca persoanele să introducă o acțiune civilă prin care să solicite despăgubiri bănești împotriva Statelor Unite ale Americii, atunci când informațiile cu privire la acestea au fost folosite sau divulgate în mod ilegal și intenționat ([392]), să introducă o acțiune în justiție împotriva funcționarilor ai guvernului SUA în calitatea lor personală prin care să solicite despăgubiri bănești ([393]) 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 ([394]). La un nivel mai general, în cazul în care guvernul intenționează să utilizeze informațiile obținute în cursul operațiunilor de colectare de informații împotriva unui suspect într-o cauză penală, cerințele constituționale și legale ([395]) impun obligații de divulgare a anumitor informații, astfel că inculpatul poate contesta legalitatea colectării și utilizării elementelor de probă de către guvern.

(197) În plus, există o serie de modalități legale specifice de recurs împotriva funcționarilor guvernamentali pentru accesul ilegal al autorităților la date cu caracter personal sau pentru utilizarea acestora, inclusiv în scopuri presupuse de securitate națională (și anume în baza Legii privind fraudele și abuzurile informatice ([396]), Legea privind confidențialitatea comunicațiilor electronice ([397]) și Legea privind dreptul la confidențialitatea informațiilor financiare ([398])). Toate aceste acțiuni în justiție se referă la date, persoane vizate și/sau tipuri de acces specifice (de exemplu, accesul de la distanță la un calculator prin intermediul internetului) și sunt disponibile în anumite condiții (de exemplu, comportament intenționat, comportament în afara calității oficiale, prejudiciul suferit).

(198) O posibilitate de recurs cu caracter mai general este oferită în baza APA ([399]), potrivit căreia „o persoană care este victima unui abuz juridic în urma acțiunilor agenției sau este afectată ori lezată într-un alt mod în urma acțiunilor agenției" are dreptul la un control jurisdicțional al acestora ([400]). Acest lucru include posibilitatea de a solicita instanței „să declare ilegale sau să anuleze acțiunile, 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" ([401]). De exemplu, o instanță de apel federală a hotărât în 2015 cu privire la o cerere în temeiul APA că o colectare în masă de metadate de telefonie de către guvernul SUA nu a fost autorizată în temeiul secțiunii 501 din FISA ([402]).

([391]) Accesul la acestea este condiționat de dovedirea „calității procesuale". Acest standard, care se aplică oricărei persoane, indiferent de cetățenie, decurge din cerința de „cauză sau litigiu" prevăzută la articolul III din Constituția SUA. Potrivit Curții Supreme, acest lucru impune ca (1) persoana să fi suferit un „prejudiciu efectiv" (și anume un prejudiciu adus unui interes protejat legal care este concret și particular și real sau iminent), (2) să existe o legătură de cauzalitate între prejudiciu și comportamentul contestat în instanță și (3) să fie probabil și nu incert ca o decizie favorabilă a instanței să remedieze prejudiciul respectiv [a se vedea Lujan/Defenders of Wildlife, 504 U.S. 555 (1992)].

([392]) Titlul 18 articolul 2712 din U.S.C.

([393]) Titlul 50 articolul 1810 din U.S.C.

([394]) Titlul 50 articolul 1806 din U.S.C.

([395]) A se vedea Brady/Maryland, 373 U.S. 83 (1963), respectiv Legea Jencks, titlul 18 articolul 3500 din U.S.C.

([396]) Titlul 18 articolul 1030 din U.S.C.

([397]) Titlul 18 articolele 2701-2712 din U.S.C.

([398]) Titlul 12 articolul 3417 din U.S.C.

([399]) Titlul 5 articolul 702 din U.S.C.

([400]) În general, doar acțiunile „finale" ale agenției și nu „acțiunile preliminare, procedurale sau intermediare" ale acesteia fac obiectul unui control jurisdicțional. A se vedea titlul 5 articolul 704 din U.S.C.

([401]) Titlul 5 articolul 706 alineatul (2) partea A din U.S.C.

([402]) ACLU/Clapper, 785 F.3d 787 (al doilea circuit 2015). Programul de colectare în masă a datelor de telefonie contestat în aceste cauze a fost închis în baza Legii SUA privind libertatea (USA Freedom Act) în 2015.

(199) În sfârșit, pe lângă modalitățile de recurs menționate în considerentele 176-198, orice persoană are dreptul de a solicita accesul la evidențele existente ale agențiilor federale în temeiul FOIA, inclusiv în cazul în care acestea conțin datele cu caracter personal ale persoanei respective ([403]). Un astfel de acces poate facilita, de asemenea, introducerea unei acțiuni înaintea instanțelor de drept comun, inclusiv în sprijinul demonstrării calității procesuale. Agențiile pot refuza accesul la informații care se încadrează în anumite excepții enumerate, inclusiv accesul la informații clasificate în materie de securitate națională și la informații privind investigațiile autorităților de aplicare a legii ([404]), însă reclamanții care sunt nemulțumiți de răspunsul primit au posibilitatea de a-l contesta prin intermediul controlului administrativ și, ulterior, jurisdicțional (înaintea instanțelor federale) ([405]).

(200) Din cele de mai sus rezultă că, atunci când autoritățile de aplicare a legii și autoritățile de securitate națională din Statele Unite ale Americii accesează date cu caracter personal care intră în domeniul de aplicare al prezentei decizii, un astfel de acces este reglementat de un cadru juridic care prevede condițiile în care poate avea loc accesul și garantează că accesul și utilizarea ulterioară a datelor sunt limitate la ceea ce este necesar și proporțional în raport cu obiectivul de interes public urmărit. Aceste garanții pot fi invocate de persoane, care beneficiază de drepturi la căi de atac eficiente.

4. **CONCLUZIE**

(201) Comisia consideră că Statele Unite ale Americii – prin principiile publicate de DoC al SUA – asigură un nivel de protecție a datelor cu caracter personal transferate din Uniune unor organizații certificate din Statele Unite ale Americii în temeiul Cadrului UE-SUA privind confidențialitatea datelor care este în esență echivalent cu cel garantat de Regulamentul (UE) 2016/679.

(202) În plus, Comisia consideră că aplicarea efectivă a principiilor este garantată de obligațiile privind transparența și gestionarea CCD de către DoC. De asemenea, în ansamblu, mecanismele de supraveghere și de recurs prevăzute în legislația SUA permit identificarea și sancționarea în practică a încălcărilor normelor de protecție a datelor și pun la dispoziția persoanelor vizate căi de atac pentru a obține accesul la datele cu caracter personal care le privesc și, în cele din urmă, rectificarea sau ștergerea datelor respective.

(203) În sfârșit, pe baza informațiilor disponibile cu privire la ordinea juridică a SUA, inclusiv a informațiilor conținute în anexele VI și VII, Comisia consideră că orice ingerință a autorităților publice din SUA în interes public, în special în scopul asigurării respectării dreptului penal și în scopuri legate de securitatea națională, în drepturile fundamentale ale persoanelor ale căror date cu caracter personal sunt transferate din Uniune către Statele Unite ale Americii în temeiul Cadrului UE-SUA privind confidențialitatea datelor se va limita la ceea ce este strict necesar pentru atingerea obiectivului legitim în cauză și că există o protecție juridică efectivă împotriva unei astfel de ingerințe. Prin urmare, având în vedere constatările de mai sus, ar trebui să se decidă că Statele Unite ale Americii asigură un nivel de protecție adecvat în sensul articolului 45 din Regulamentul (UE) 2016/679, interpretat în lumina Cartei drepturilor fundamentale a Uniunii Europene, pentru datele cu caracter personal transferate din Uniunea Europeană unor organizații certificate în temeiul Cadrului UE-SUA privind confidențialitatea datelor.

(204) Având în vedere că limitările, garanțiile și mecanismul de recurs instituite prin OE nr. 14086 sunt elemente esențiale ale cadrului juridic al SUA pe care se bazează evaluarea Comisiei, adoptarea prezentei decizii se bazează în special pe adoptarea unor politici și proceduri actualizate de punere în aplicare a OE nr. 14086 de către toate serviciile de informații din SUA și pe desemnarea Uniunii ca organizație eligibilă în scopul mecanismului de recurs, care au avut loc la 3 iulie 2023 (a se vedea considerentul 126) și, respectiv, la 30 iunie 2023 (a se vedea considerentul 176).

([403]) Titlul 5 articolul 552 din U.S.C. Există legi similare la nivel de stat.

([404]) În acest caz, persoana respectivă va primi în mod normal numai un răspuns standard prin care agenția refuză să confirme sau să infirme existența vreunor evidențe. A se vedea ACLU/CIA, 710 F.3d 422 (circuitul D.C. 2014). Criteriile și durata clasificării sunt stabilite în Ordinul executiv nr. 13526, care prevede, ca regulă generală, că trebuie stabilită o dată specifică sau un eveniment specific pentru declasificare, pe baza duratei sensibilității informațiilor din punctul de vedere al securității naționale, moment în care informațiile trebuie să fie declasificate în mod automat (a se vedea secțiunea 1.5 din OE nr. 13526).

([405]) Instanța este obligată să se pronunțe *de novo* asupra legalității refuzului de a acorda accesul la evidențele în cauză și poate obliga guvernul să ofere accesul la acestea [titlul 5 articolul 552 litera (a) punctul 4 partea B].

5. EFECTELE PREZENTEI DECIZII ȘI ACȚIUNILE AUTORITĂȚILOR PENTRU PROTECȚIA DATELOR

(205) Statele membre și organele acestora au obligația de a lua măsurile necesare pentru a se conforma actelor instituțiilor Uniunii, întrucât se presupune că aceste acte sunt legale și, prin urmare, produc efecte juridice atât timp cât nu sunt retrase, anulate în cadrul unei acțiuni în anulare sau declarate nule ca urmare a unei trimiteri preliminare sau a unei excepții de nelegalitate.

(206) În consecință, o decizie a Comisiei privind caracterul adecvat al nivelului de protecție, adoptată în temeiul articolului 45 alineatul (3) din Regulamentul (UE) 2016/679, este obligatorie pentru toate organele statelor membre cărora li se adresează, inclusiv pentru autoritățile de supraveghere independente ale acestora. În special, transferurile de la un operator sau o persoană împuternicită de operator din Uniune către organizații certificate din Statele Unite ale Americii poate avea loc fără a fi necesară obținerea unei autorizări suplimentare.

(207) Ar trebui reamintit faptul că, în temeiul articolului 58 alineatul (5) din Regulamentul (UE) 2016/679 și astfel cum este explicat de Curtea de Justiție în Hotărârea Schrems ([406]), în cazul în care o autoritate națională pentru protecția datelor pune sub semnul întrebării, inclusiv în urma primirii unei plângeri, compatibilitatea unei decizii a Comisiei privind caracterul adecvat al nivelului de protecție cu dreptul fundamental al unei persoane la viață privată și la protecția datelor, legislația națională trebuie să prevadă o cale de atac pentru a invoca motivele respective în fața unei instanțe naționale, care poate fi obligată să efectueze o trimitere preliminară către Curtea de Justiție ([407]).

6. MONITORIZAREA ȘI REVIZUIREA PREZENTEI DECIZII

(208) În conformitate cu jurisprudența Curții de Justiție ([408]) și astfel cum se prevede la articolul 45 alineatul (4) din Regulamentul (UE) 2016/679, Comisia ar trebui să monitorizeze continuu evoluțiile relevante din țara terță, după adoptarea unei decizii privind caracterul adecvat al nivelului de protecție, pentru a evalua dacă țara terță continuă să asigure un nivel de protecție în esență echivalent. O astfel de verificare se impune, în orice caz, atunci când Comisia primește orice informație care dă naștere unor îndoieli justificate în această privință.

(209) Prin urmare, Comisia ar trebui să monitorizeze în permanență situația din Statele Unite ale Americii în ceea ce privește cadrul juridic și practica propriu-zisă de prelucrare a datelor cu caracter personal, astfel cum sunt evaluate în prezenta decizie. Pentru a facilita acest proces, autoritățile SUA ar trebui să informeze cu promptitudine Comisia cu privire la evoluțiile semnificative la nivelul ordinii juridice a Statele Unite ale Americii care au un impact asupra cadrului juridic care face obiectul prezentei decizii, precum și cu privire la orice evoluție a practicilor legate de prelucrarea datelor cu caracter personal evaluate în prezenta decizie, atât în ceea ce privește prelucrarea datelor cu caracter personal de către organizații certificate din Statele Unite ale Americii, cât și limitările și garanțiile aplicabile accesului autorităților publice la datele cu caracter personal.

(210) În plus, pentru a permite Comisiei să își exercite în mod eficace funcția de monitorizare, statele membre ar trebui să informeze Comisia cu privire la orice acțiune relevantă întreprinsă de autoritățile naționale pentru protecția datelor, în special în ceea ce privește solicitările sau plângerile formulate de persoane vizate din Uniune cu privire la transferul de date cu caracter personal din Uniune către organizații certificate din Statele Unite ale Americii. De asemenea, Comisia ar trebui să fie informată cu privire la orice indiciu potrivit căruia acțiunile autorităților publice din SUA responsabile cu prevenirea, investigarea, detectarea sau aducerea în fața instanței a infracțiunilor sau cu securitatea națională, inclusiv acțiunile oricărui organism de supraveghere, nu asigură nivelul de protecție necesar.

([406]) Hotărârea Schrems, punctul 65.

([407]) Hotărârea Schrems, punctul 65: „În această privință, revine legiuitorului național sarcina de a prevedea căi de atac care să permită autorității naționale de supraveghere în cauză să invoce motivele pe care le consideră întemeiate în fața instanțelor naționale, astfel încât acestea din urmă să efectueze, dacă împărtășesc îndoielile acestei autorități în ceea ce privește validitatea deciziei Comisiei, o trimitere preliminară în vederea examinării validității acestei decizii."

([408]) Hotărârea Schrems, punctul 76.

(211) În aplicarea articolului 45 alineatul (3) din Regulamentul (UE) 2016/679 ([409]), Comisia, în urma adoptării prezentei decizii, ar trebui să verifice periodic dacă respectivele constatări referitoare la caracterul adecvat al nivelului de protecție asigurat de Statele Unite ale Americii în temeiul Cadrului UE-SUA privind confidențialitatea datelor sunt în continuare justificate în fapt și în drept. Întrucât, în special, OE nr. 14086 și Regulamentul PG impun crearea de noi mecanisme și punerea în aplicare a unor noi garanții, prezenta decizie ar trebui să facă obiectul unei prime revizuiri în termen de un an de la intrarea sa în vigoare, pentru a se verifica dacă toate elementele relevante au fost puse în aplicare pe deplin și dacă funcționează în mod eficace în practică. În urma acestei prime revizuiri și în funcție de rezultatul acesteia, Comisia va decide, consultându-se îndeaproape cu comitetul instituit în temeiul articolului 93 alineatul (1) din Regulamentul (UE) 2016/679 și cu Comitetul european pentru protecția datelor, cu privire la periodicitatea revizuirilor viitoare ([410]).

(212) Pentru a efectua revizuirile, Comisia ar trebui să participe la reuniuni cu DoC, FTC și DoT însoțite, dacă este cazul, de alte departamente și agenții implicate în punerea în aplicare a CCD UE-SUA, precum și, în ceea ce privește aspectele legate de accesul autorităților la date, de reprezentanți ai DoJ, ODNI (inclusiv CLPO), alte elemente ale Comunității Serviciilor de Informații, DPRC și avocați speciali. Participarea la această reuniune ar trebui să fie deschisă reprezentanților membrilor Comitetului european pentru protecția datelor.

(213) Revizuirile ar trebui să vizeze toate aspectele legate de funcționarea prezentei decizii în ceea ce privește prelucrarea datelor cu caracter personal în Statele Unite ale Americii, în special de aplicarea și punerea în aplicare a principiilor, acordându-se o atenție deosebită protecției acordate în cazul transferurilor ulterioare, evoluțiilor relevante ale jurisprudenței, eficacității exercitării drepturilor individuale, monitorizării și asigurării respectării principiilor, precum și limitărilor și garanțiilor în ceea ce privește accesul autorităților, mai ales punerii în aplicare și aplicării garanțiilor introduse prin OE nr. 14086, inclusiv prin politici și proceduri elaborate de serviciile de informații, interacțiunii dintre OE nr. 14086 și secțiunea 702 din FISA și OE nr. 12333 și eficacității mecanismelor de supraveghere și de recurs (inclusiv funcționării noului mecanism de recurs instituit în temeiul OE nr. 14086). În contextul revizuirilor respective, se va acorda atenție și cooperării dintre APD și autoritățile competente din Statele Unite ale Americii, inclusiv elaborării de instrucțiuni și alte instrumente de interpretare cu privire la aplicarea principiilor, precum și la alte aspecte ale funcționării cadrului.

(214) Pe baza revizuirii, Comisia ar trebui să pregătească un raport public care trebuie să fie prezentat Parlamentului European și Consiliului.

7. **SUSPENDAREA, ABROGAREA SAU MODIFICAREA PREZENTEI DECIZII**

(215) În cazul în care informațiile disponibile, în special informațiile care rezultă din monitorizarea prezentei decizii sau cele furnizate de autoritățile SUA sau ale statelor membre, arată că nivelul de protecție oferit datelor transferate în temeiul prezentei decizii ar putea să nu mai fie adecvat, Comisia ar trebui să informeze cu promptitudine autoritățile SUA competente în acest sens și să solicite luarea unor măsuri adecvate într-un termen rezonabil specificat.

(216) În cazul în care, la expirarea termenului specificat, autoritățile SUA competente nu iau măsurile respective sau nu demonstrează în mod satisfăcător în alt fel că prezenta decizie continuă să se bazeze pe un nivel adecvat de protecție, Comisia va iniția procedura menționată la articolul 93 alineatul (2) din Regulamentul (UE) 2016/679 în vederea suspendării sau a abrogării parțiale sau integrale a prezentei decizii.

(217) Ca alternativă, Comisia inițiază această procedură în vederea modificării prezentei decizii, în special prin aplicarea unor condiții suplimentare transferurilor de date sau prin limitarea domeniului de aplicare al constatării referitoare la caracterul adecvat numai la transferurile de date pentru care se asigură în continuare un nivel adecvat de protecție.

([409]) În conformitate cu articolul 45 alineatul (3) din Regulamentul (UE) 2016/679, „[a]ctul de punere în aplicare prevede un mecanism de revizuire periodică […], care ia în considerare toate evoluțiile relevante din țara terță sau organizația internațională”.

([410]) Articolul 45 alineatul (3) din Regulamentul (UE) 2016/679 prevede că trebuie să se efectueze o revizuire periodică „cel puțin o dată la patru ani”. A se vedea, de asemenea, Comitetul european pentru protecția datelor, Criterii de referință privind caracterul adecvat al nivelului de protecție, WP 254 rev. 01.

(218) În special, Comisia ar trebui să inițieze procedura de suspendare sau de abrogare în cazul în care:

(a) există indicii că organizațiile care au primit date cu caracter personal din Uniune în temeiul prezentei decizii nu respectă principiile și că o astfel de neconformitate nu este abordată în mod eficace de către organismele competente de supraveghere și de asigurare a respectării legii;

(b) există indicii că autoritățile SUA nu respectă condițiile și limitările aplicabile în ceea ce privește accesul autorităților publice din SUA, în scopul asigurării respectării legii și în scopuri legate de securitatea națională, la date cu caracter personal transferate în temeiul CCD UE-SUA sau

(c) plângerile înaintate de persoanele vizate din Uniune nu sunt abordate în mod eficace, inclusiv de CLPO ODNI și/sau DPRC.

(219) De asemenea, Comisia ar trebui să aibă în vedere inițierea procedurii care conduce la modificarea, suspendarea sau abrogarea prezentei decizii în cazul în care autoritățile SUA competente nu furnizează informațiile sau clarificările necesare pentru evaluarea nivelului de protecție acordat datelor cu caracter personal transferate din Uniune către Statele Unite ale Americii sau în ceea ce privește respectarea prezentei decizii. În această privință, Comisia ar trebui să ia în considerare măsura în care informațiile relevante pot fi obținute din alte surse.

(220) Din motive imperioase de urgență justificate corespunzător, de exemplu, în cazul în care OE nr. 14086 sau Regulamentul PG ar urma să fie modificate, iar modificările aduse ar submina nivelul de protecție descris în prezenta decizie sau în cazul în care desemnarea de către procurorul general a Uniunii ca organizație eligibilă în scopul mecanismului de recurs este retrasă, Comisia va face uz de posibilitatea de a adopta, în conformitate cu procedura menționată la articolul 93 alineatul (3) din Regulamentul (UE) 2016/679, acte de punere în aplicare imediat aplicabile de suspendare, abrogare sau modificare a prezentei decizii.

8. **CONSIDERAȚII FINALE**

(221) Comitetul european pentru protecția datelor și-a publicat avizul ([411]), care a fost luat în considerare la pregătirea prezentei decizii.

(222) Parlamentul European a adoptat o rezoluție referitoare la caracterul adecvat al protecției oferite de Cadrul UE-SUA privind confidențialitatea datelor ([412]).

(223) Măsurile prevăzute în prezenta decizie sunt conforme cu avizul comitetului instituit în temeiul articolului 93 alineatul (1) din Regulamentul (UE) 2016/679,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

În sensul articolului 45 din Regulamentul (UE) 2016/679, Statele Unite ale Americii asigură un nivel adecvat de protecție a datelor cu caracter personal transferate din Uniune către organizații din Statele Unite ale Americii care sunt incluse în „Lista Cadrului privind confidențialitatea datelor”, gestionată și pusă la dispoziția publicului de către Departamentul Comerțului al SUA, în conformitate cu anexa I secțiunea I punctul 3.

Articolul 2

Ori de câte ori autoritățile competente din statele membre, pentru a proteja persoanele în ceea ce privește prelucrarea datelor cu caracter personal, își exercită competențele în temeiul articolului 58 din Regulamentul (UE) 2016/679 în ceea ce privește transferurile de date prevăzute la articolul 1 din prezenta decizie, statul membru în cauză informează fără întârziere Comisia.

([411]) Avizul 5/2023 din 28 februarie 2023 referitor la Proiectul de decizie de punere în aplicare a Comisiei Europene privind protecția adecvată a datelor cu caracter personal în temeiul Cadrului UE-SUA privind confidențialitatea datelor.

([412]) Rezoluția Parlamentului European din 11 mai 2023 referitoare la caracterul adecvat al protecției oferite de Cadrul UE-SUA privind confidențialitatea datelor [2023/2501(RSP)].

Articolul 3

(1) Comisia monitorizează în permanență aplicarea cadrului juridic care face obiectul prezentei decizii, inclusiv condițiile în care se efectuează transferurile ulterioare, în care se exercită drepturile individuale și în care autoritățile publice din SUA au acces la datele transferate în temeiul prezentei decizii, pentru a evalua dacă Statele Unite ale Americii continuă să asigure un nivel de protecție adecvat, astfel cum se prevede la articolul 1.

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

(3) Statele membre și Comisia se informează reciproc cu privire la orice indicii potrivit cărora ingerințele autorităților publice din SUA responsabile pentru urmărirea securității naționale, aplicarea legii sau a altor interese publice în exercitarea dreptului persoanelor la protecția datelor lor cu caracter personal depășesc ceea ce este necesar și proporțional și/sau că nu există o protecție juridică efectivă împotriva unor astfel de ingerințe.

(4) În termen de un an de la data notificării prezentei decizii către statele membre și, ulterior, cu o periodicitate care va fi decisă în strânsă consultare cu comitetul instituit în temeiul articolului 93 alineatul (1) din Regulamentul (UE) 2016/679 și cu Comitetul european pentru protecția datelor, Comisia evaluează constatarea menționată la articolul 1 alineatul (1) pe baza tuturor informațiilor disponibile, inclusiv a informațiilor obținute prin intermediul revizuirii realizate împreună cu autoritățile competente ale Statelor Unite ale Americii.

(5) În cazul în care Comisia dispune de indicii potrivit cărora nu mai este asigurat un nivel de protecție adecvat, aceasta informează autoritățile competente din SUA. Dacă este necesar, Comisia va decide să suspende, să modifice sau să abroge prezenta decizie ori să limiteze domeniul de aplicare al acesteia, în conformitate cu articolul 45 alineatul (5) din Regulamentul (UE) 2016/679. Comisia poate, de asemenea, să adopte o astfel de decizie în cazul în care lipsa de cooperare a autorităților SUA o împiedică să stabilească dacă Statele Unite ale Americii continuă să asigure un nivel de protecție adecvat.

Articolul 4

Prezenta decizie se adresează statelor membre.

Adoptată la Bruxelles, 10 iulie 2023.

Pentru Comisie
Didier REYNDERS
Membru al Comisiei

ANEXA I

PRINCIPIILE CADRULUI UE-SUA PRIVIND CONFIDENȚIALITATEA DATELOR EMISE DE DEPARTAMENTUL COMERȚULUI AL SUA

I. PREZENTARE GENERALĂ

1. Deși Statele Unite ale Americii și Uniunea Europeană („UE") împărtășesc angajamentul de a consolida protecția vieții private și statul de drept și recunosc importanța fluxurilor transatlantice de date pentru cetățenii, economiile și societățile noastre, Statele Unite ale Americii abordează în mod diferit protecția vieții private comparativ cu UE. Statele Unite ale Americii utilizează o abordare sectorială, care se bazează pe un ansamblu de dispoziții legislative, regulamente și dispoziții de autoreglementare. Departamentul Comerțului din SUA („Departamentul") publică principiile Cadrului UE-SUA privind confidențialitatea datelor, inclusiv principiile suplimentare (denumite în mod colectiv „principiile") și anexa I la principii („anexa I"), în calitate de autoritate competentă cu scopul de a stimula, a promova și a dezvolta comerțul internațional (titlul 15 articolul 1512 din U.S.C.). Principiile au fost elaborate prin consultări cu Comisia Europeană („Comisia"), precum și cu industria și cu alte părți interesate, în vederea facilitării comerțului și a relațiilor de afaceri dintre Statele Unite ale Americii și UE. Principiile, o componentă-cheie a Cadrului UE-SUA privind confidențialitatea datelor („ CCD UE-SUA") furnizează organizațiilor din Statele Unite ale Americii un mecanism fiabil pentru transferurile de date cu caracter personal din UE către Statele Unite ale Americii, asigurându-se, în același timp, că persoanele vizate din UE continuă să beneficieze de protecția și garanțiile eficace 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. Principiile sunt destinate exclusiv organizațiilor eligibile din Statele Unite ale Americii care primesc date cu caracter personal din UE cu scopul de a se califica pentru aplicarea CCD UE-SUA și, astfel, de a beneficia de decizia Comisiei privind caracterul adecvat al nivelului de protecție ([1]). Principiile nu afectează aplicarea Regulamentului (UE) 2016/679 („Regulamentul general privind protecția datelor" sau „RGPD") ([2]) care se aplică prelucrării datelor cu caracter personal în statele membre ale UE. Principiile nu limitează obligațiile de confidențialitate care se aplică în alt mod în temeiul legislației SUA.

2. Cu scopul de a se prevala de CCD UE-SUA pentru a efectua transferuri de date cu caracter personal din UE, o organizație trebuie să prezinte autocertificarea adeziunii sale la principii departamentului (sau reprezentantului acestuia). Deciziile organizațiilor de a participa astfel la CCD UE-SUA sunt complet voluntare, însă respectarea efectivă a principiilor 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 CCD UE-SUA, o organizație trebuie (a) să facă obiectul competențelor de investigare și de asigurare a respectării legii ale Comisiei Federale pentru Comerț („FTC"), ale Departamentului Transporturilor („DoT") sau ale altui organism oficial care va asigura efectiv respectarea 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 ([3]). Nerespectarea principiilor de către o organizație poate fi sancționată de FTC în temeiul secțiunii 5 din Legea privind Comisia Federală pentru Comerț (FTC), care interzice practicile neloiale și frauduloase în domeniul comerțului sau care afectează comerțul (titlul 15 articolul 45 din U.S.C.), de DoT în temeiul titlului 49 articolul 41712 din U.S.C., care interzice unui transportator sau unui agent de bilete să desfășoare orice practică neloială sau frauduloasă în cadrul activității de transport aerian sau pentru vânzarea de servicii de transport aerian sau în temeiul altor legi sau reglementări care interzic astfel de practici.

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

([2]) 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).

([3]) Principiile Cadrului privind Scutul de confidențialitate UE-SUA au fost modificate drept „Principiile Cadrului UE-SUA privind confidențialitatea datelor". (*A se vedea* principiul suplimentar privind autocertificarea).

3. Departamentul 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 („lista Cadrului privind confidențialitatea datelor"). Beneficiile CCD UE-SUA sunt asigurate de la data la care departamentul include organizația pe lista Cadrului privind confidențialitatea datelor. Departamentul va elimina de pe lista Cadrului privind confidențialitatea datelor organizațiile care se retrag în mod voluntar din CCD UE-SUA sau care nu își finalizează recertificarea anuală la departament; aceste organizații fie trebuie să continue să aplice principiile informațiilor cu caracter personal pe care le-au primit în temeiul CCD UE-SUA și să își afirme anual în fața departamentului angajamentul de a face acest lucru (și anume atât timp cât păstrează astfel de informații), să furnizeze o protecție „adecvată" a informațiilor prin alte mijloace autorizate (de exemplu, aplicând un contract care reflectă pe deplin cerințele clauzelor contractuale standard relevante adoptate de către Comisia Europeană), fie trebuie să returneze sau să șteargă informațiile respective. De asemenea, departamentul va elimina de pe lista Cadrului privind confidențialitatea datelor organizațiile care încalcă în mod sistematic principiile; aceste organizații trebuie să returneze sau să șteargă informațiile cu caracter personal pe care le-au primit în temeiul CCD UE-SUA. Eliminarea unei organizații de pe lista Cadrului privind confidențialitatea datelor înseamnă că aceasta nu mai are dreptul să beneficieze de decizia Comisiei privind caracterul adecvat al nivelului de protecție pentru a primi informații cu caracter personal din UE.

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 de pe lista Cadrului privind confidențialitatea datelor. Departamentul va furniza un avertisment clar că aceste organizații nu participă la CCD UE-SUA, că eliminarea de pe lista Cadrului privind confidențialitatea datelor înseamnă că organizațiile respective nu pot afirma că respectă CCD UE-SUA și trebuie să evite orice declarații sau practici înșelătoare care ar sugera că acestea participă la CCD UE-SUA și că organizațiile respective nu mai au dreptul să beneficieze de decizia Comisiei privind caracterul adecvat al nivelului de protecție pentru a primit informații cu caracter personal din UE. O organizație care continuă să afirme că participă la CCD UE-SUA sau face alte declarații false legate de CCD UE-SUA după ce aceasta a fost eliminată de pe lista Cadrului privind confidențialitatea datelor poate face obiectul unor măsuri de asigurare a respectării legii luate de către FTC, DoT sau alte autorități de aplicare a legii.

5. Aderarea la aceste principii poate fi limitată: (a) în măsura necesară pentru a respecta o hotărâre judecătorească sau pentru a îndeplini cerințe de interes public, de asigurare a respectării legii sau de securitate națională, inclusiv în cazul în care legile sau regulamentele administrative stabilesc obligații contradictorii, (b) în temeiul unei legi, al unei hotărâri judecătorești sau al unui regulament administrativ care prevede autorizații exprese, cu condiția ca organizația care a recurs la o asemenea autorizație să poată demonstra că nerespectarea principiilor se limitează la măsura necesară pentru garantarea intereselor legitime superioare pe care această autorizație urmărește să le servească sau (c) de excepțiile sau derogările permise de RGPD, în condițiile prevăzute în acesta, cu condiția ca aceste excepții sau derogări să fie aplicate în contexte comparabile. În acest context, garanțiile prevăzute în legislația SUA pentru protecția vieții private și a libertăților civile le includ pe cele impuse de Ordinul executiv nr. 14086 ([4]) în condițiile prevăzute în acesta (inclusiv cerințele sale privind necesitatea și proporționalitatea). În conformitate cu obiectivul consolidării protecției vieții private, organizațiile ar trebui să depună eforturi să pună în aplicare aceste principii pe deplin și în mod transparent, inclusiv să indice în politicile lor de confidențialitate domeniile în care se vor aplica excepțiile menționate la litera (b) de mai sus. Din același motiv, atunci când principiile și/sau legile SUA 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 baza CCD UE-SUA ulterior aderării lor la CCD UE-SUA. O organizație care dorește să extindă beneficiile oferite de CCD UE-SUA la informațiile cu caracter personal privind resursele umane transferate din UE pentru a le utiliza în contextul unui raport de muncă trebuie să menționeze această intenție atunci când își prezintă autocertificarea departamentului și trebuie să respecte cerințele stabilite în principiul suplimentar privind autocertificarea.

([4]) Ordinul executiv din 7 octombrie 2022 – „Enhancing Safeguards for US Signals Intelligence Activities" (Consolidarea garanțiilor pentru activitățile de colectare de informații de tip SIGINT desfășurate de Statele Unite ale Americii).

7. Se aplică legislația SUA în ceea ce privește aspectele legate de interpretarea și respectarea principiilor și a politicilor de confidențialitate relevante de către organizațiile care participă la CCD UE SUA, cu excepția cazurilor în care organizațiile respective s-au angajat să coopereze cu autoritățile UE 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 identificată sau identificabilă care intră în domeniul de aplicare al RGPD, primite din UE de o organizație din Statele Unite ale Americii 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, cu sau fără utilizarea de mijloace automatizate, precum colectarea, înregistrarea, organizarea, stocarea, adaptarea sau modificarea, extragerea, 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 principiilor și a anexei I la principii este data intrării în vigoare a deciziei Comisiei Europene privind caracterul adecvat al nivelului de protecție.

II. **PRINCIPII**

1. **NOTIFICAREA**

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

   i. participarea sa la CCD UE-SUA și să comunice un link sau adresa URL pentru lista Cadrului privind confidențialitatea datelor,

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

   iii. angajamentul său de a supune principiilor toate datele cu caracter personal primite din UE în baza CCD UE-SUA,

   iv. scopurile pentru care colectează și utilizează informațiile cu caracter personal despre acestea,

   v. modul în care pot contacta organizația pentru orice solicitări de informații sau plângeri, inclusiv cu privire la orice unitate relevantă din UE care poate răspunde la astfel de solicitări de informații sau plângeri,

   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 cu caracter personal,

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

   ix. organismul independent de soluționare a litigiilor desemnat pentru a gestiona plângerile și pentru a oferi persoanei respective căi de atac adecvate în mod gratuit, precum și dacă acesta este reprezentat de: (1) comitetul special constituit de APD, (2) un organism de soluționare alternativă a litigiilor cu sediul în UE sau (3) un organism de soluționare alternativă a litigiilor cu sediul în Statele Unite ale Americii,

   x. faptul că face obiectul competențelor de investigare și de asigurare a respectării legii ale FTC, ale DoT sau ale oricărui alt organism statutar autorizat din SUA,

   xi. posibilitatea, în anumite condiții, ca o persoană să recurgă la procedura de arbitraj obligatoriu ([5]),

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

   xiii. răspunderea sa în cazul transferurilor ulterioare către părți terțe.

([5]) *A se vedea, de exemplu,* litera (c) din principiul recursului, punerii în aplicare și răspunderii.

b. Această notificare trebuie formulată într-un limbaj clar și lizibil și trebuie comunicată persoanelor în cauză atunci când acestora li se solicită pentru prima dată să furnizeze informațiile cu caracter personal organizației sau cât mai curând posibil după aceasta, dar, în orice caz, înainte ca informațiile să fie utilizate de organizație într-un scop diferit de cel în care au fost colectate inițial sau prelucrate de organizația care a efectuat transferul sau înainte ca ele să fie divulgate pentru prima dată unei părți terțe.

2. **OPȚIUNEA**

a. O organizație trebuie să ofere persoanelor în cauză posibilitatea de a alege (și anume de a refuza) ca informațiile lor cu caracter personal (i) să fie divulgate unui părți terțe sau (ii) să fie utilizate într-un scop care diferă în mod semnificativ de scopul (scopurile) în care au fost colectate inițial sau scopul (scopurile) aprobat(e) 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 divulgate către o parte terță care acționează ca agent pentru a îndeplini o sarcină (sarcini) în numele și pe baza instrucțiunilor organizației. Cu toate acestea, o organizație trebuie să încheie întotdeauna un contract cu agentul respectiv.

c. În ceea ce privește informațiile sensibile (și anume informațiile cu caracter personal privind dosarul medical sau starea de sănătate a unei persoane, originea rasială sau etnică, opiniile politice, credințele religioase sau convingerile filosofice, apartenența sindicală sau viața sexuală a persoanei respective), organizațiile trebuie să obțină consimțământul explicit (și anume acordul) persoanelor dacă astfel de informații urmează să fie (i) divulgate unei părți terțe sau (ii) utilizate în alte scopuri decât cele în care au fost colectate inițial acestea sau cele aprobate ulterior de către persoanele respective prin exprimarea acordului. În plus, o organizație ar trebui să considere drept informații sensibile orice informații cu caracter personal primite de la o parte terță în cazul în care partea terță respectivă indică faptul că aceste informații sunt sensibile și le tratează în consecință.

3. **RESPONSABILITATEA PENTRU TRANSFERURILE ULTERIOARE**

a. Pentru a transfera informații cu caracter personal către o parte terță care acționează în calitate de operator, organizațiile trebuie să respecte principiile notificării și opțiunii. De asemenea, organizațiile trebuie să încheie un contract cu operatorul terț, care să prevadă că astfel de date pot fi prelucrate numai în scopuri limitate și specificate în conformitate cu consimțământul acordat de către persoana în cauză și că destinatarul va asigura același nivel de protecție precum principiile, precum și că va transmite o notificare organizației în cazul în care ajunge la concluzia că nu mai poate îndeplini această obligație. Contractul trebuie să prevadă că, în cazul în care se ajunge la o astfel de concluzie, prelucrarea de către partea terță respectivă încetează sau aceasta ia alte măsuri rezonabile și adecvate pentru a remedia situația.

b. Pentru a transfera date cu caracter personal către o parte terță care acționează ca agent, organizațiile trebuie: (i) să transfere aceste date numai în scopuri limitate și specificate, (ii) să confirme faptul că agentul este obligat să asigure cel puțin același nivel de protecție a vieții private precum cel impus în baza principiilor, (iii) să ia măsuri rezonabile și adecvate 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, (iv) să prevadă că agentul trebuie să transmită o notificare organizației în cazul în care ajunge la concluzia că nu își mai poate îndeplini obligația de a furniza același nivel de protecție precum cel impus în baza principiilor, (v) în urma notificării, inclusiv în conformitate cu subpunctul (iv), să ia măsuri rezonabile și adecvate pentru a opri și a remedia prelucrarea neautorizată și (vi) să furnizeze departamentului, la cerere, un rezumat sau o copie reprezentativă a dispozițiilor privind confidențialitatea incluse în contractul cu agentul respectiv.

4. **SECURITATEA**

a. Organizațiile care creează, gestionează, utilizează sau diseminează informații cu caracter personal trebuie să ia măsuri rezonabile și adecvate pentru a preveni pierderea, utilizarea abuzivă, accesul neautorizat, divulgarea, modificarea și distrugerea acestor informații, ținând seama în mod corespunzător de riscurile pe care le presupune prelucrarea și natura datelor cu caracter personal în cauză.

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 ([6]). O organizație nu poate prelucra informații cu caracter personal într-un mod care este incompatibil cu scopurile în care au fost colectate acestea sau cu scopurile aprobate ulterior de persoana în cauză. În măsura în care acest lucru este necesar în scopurile respective, o organizație trebuie să ia măsuri rezonabile pentru a asigura fiabilitatea datelor cu caracter personal în raport cu utilizarea preconizată, 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 ([7]) persoanei numai în măsura în care servește la atingerea obiectivului de prelucrare în sensul punctului 5 litera (a). 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 unor scopuri legate de arhivarea în interes public, jurnalism, literatură și artă, cercetarea științifică și istorică și analiza statistică. În aceste cazuri, o astfel de prelucrare face obiectul celorlalte principii și dispoziții ale CCD UE-SUA. Organizațiile ar 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 inexacte sau au fost prelucrate cu încălcarea principiilor, cu excepția cazurilor în care dificultatea sau costurile ocazionate de acordarea dreptului de acces ar fi 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.

7. **RECURSUL, PUNEREA ÎN APLICARE ȘI RĂSPUNDEREA**

a. O protecție efectivă a vieții private trebuie să includă mecanisme solide care să permită asigurarea respectării principiilor, modalități de recurs pentru persoanele afectate de nerespectarea principiilor și consecințe pentru organizații atunci când acestea nu respectă principiile. Aceste mecanisme trebuie să includă cel puțin:

i. mecanisme independente de recurs ușor accesibile, care să permită investigarea și soluționarea în mod rapid a litigiilor și a plângerilor oricărei persoane, fără ca aceasta să implice costuri pentru persoana în cauză și în conformitate cu principiile, precum și acordarea de despăgubiri în cazurile prevăzute de legislația aplicabilă sau de inițiativele din sectorul privat;

ii. proceduri de urmărire pentru verificarea veridicității afirmațiilor și a declarațiilor organizațiilor cu privire la practicile lor de protecție a vieții private și pentru verificarea punerii în aplicare a acestor practici astfel cum au fost prezentate și, în special, cu privire la cazurile de nerespectare și

iii. obligații de remediere a problemelor care rezultă în urma nerespectării principiilor de către organizațiile care își fac publică adeziunea la acestea și consecințele pentru aceste organizații. Sancțiunile trebuie să fie suficient de severe pentru a garanta respectarea principiilor de către organizații.

b. Organizațiile și mecanismele independente de recurs selectate vor răspunde cu promptitudine la solicitările de informații și cererile formulate de departament referitoare la CCD UE-SUA. Toate organizațiile trebuie să răspundă rapid plângerilor referitoare la respectarea principiilor transmise de autoritățile statelor membre ale UE prin intermediul departamentului. Organizațiile care au ales să coopereze cu APD, inclusiv organizațiile care prelucrează date privind resursele umane, trebuie să răspundă în mod direct acestor autorități în ceea ce privește investigarea și soluționarea plângerilor.

([6]) În funcție de circumstanțe, printre exemplele de scopuri de prelucrare compatibile se pot număra cele care vizează, în mod rezonabil, relațiile cu clienții, respectarea reglementărilor și considerații de ordin juridic, activitățile de audit, securitatea și prevenirea fraudei, conservarea și apărarea drepturilor legale ale organizației sau alte scopuri care sunt conforme cu așteptările unei persoane rezonabile, având în vedere contextul în care sunt colectate.

([7]) În acest context, dacă, 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 sunt păstrate datele, o persoană ar putea să fie identificată în mod rezonabil de organizație sau de o parte terță în cazul în care ar avea acces la date, se poate considera că persoana este „identificabilă”.

c. Organizațiile sunt obligate să supună plângerile procedurii de arbitraj și să respecte condițiile prevăzute în anexa I, cu condiția ca persoana în cauză să fi recurs la procedura de arbitraj obligatoriu prin notificarea organizației în cauză, în conformitate cu procedurile și în condițiile prevăzute în anexa I.

d. În contextul unui transfer ulterior, o organizație care participă la CCD este responsabilă pentru prelucrarea informațiilor cu caracter personal pe care le primește în temeiul CCD UE-SUA și pe care le transferă ulterior către o parte terță care acționează în numele său în calitate de agent. Organizația participantă la CCD 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 unei ordin judecătoresc emis în urma unei neconformități sau al unui ordin emis de un organism statutar din SUA (de exemplu, de FTC sau DoT) enumerat în principii sau într-o viitoare anexă la principii emis în urma unei neconformități, organizația face publică toate secțiunile relevante cu privire la CCD UE-SUA din orice raport de conformitate sau de evaluare transmis instanței sau organismului statutar din SUA în măsura permisă de cerințele de confidențialitate. Departamentul a instituit un punct de contact specific pentru APD pentru orice încălcări ale conformității de către organizațiile care participă la CCD. FTC și DoT vor acorda prioritate sesizărilor privind nerespectarea principiilor primite de la departament și autoritățile statelor membre ale UE și va face schimb de informații cu privire la sesizări cu autoritățile statului 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 (și anume 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 instanță;

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

iv. este efectuată în cadrul activităților lor legitime de către o fundație, o asociație sau orice alt organism fără scop lucrativ și cu specific politic, filozofic, religios sau sindical, cu condiția ca prelucrarea să se refere numai la membrii organismului respectiv sau la persoane cu care acesta are contacte permanente în legătură cu scopurile sale și ca datele să nu fie divulgate unei părți terțe fără consimțământul persoanelor vizate;

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

vi. are legătură cu date care sunt făcute publice în mod clar 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, atunci când drepturile presei libere menționate la primul amendament al Constituției Statelor Unite ale Americii se intersectează cu interese ce țin de protecția vieții private, primul amendament trebuie să reglementeze modul de punere în balanță a acestor interese cu privire la activitățile persoanelor care sunt cetățeni americani/rezidenți în SUA sau ale organizațiilor din SUA.

b. Informațiile cu caracter personal care sunt colectate în vederea publicării, a difuzării sau a comunicării publice prin alte forme a unui material jurnalistic, indiferent dacă sunt utilizate sau nu, precum și informațiile din materiale publicate anterior și diseminate din arhive mass-media nu fac obiectul principiilor.

3. Răspunderea secundară

a. Furnizorii de servicii de internet („FSI”), societățile de telecomunicații și alte organizații nu sunt răspunzătoare în temeiul principiilor în numele altei organizații atunci când acestea se limitează la transmiterea, direcționarea, înlocuirea sau stocarea în memoria cache a informațiilor. CCD UE-SUA nu creează o răspundere secundară. În măsura în care un organism funcționează doar ca vector pentru datele transmise de părți terțe și nu stabilește nici obiectivele și nici mijloacele de prelucrare a acestor date cu caracter personal, răspunderea sa nu este angajată.

4. **Realizarea procesului de diligență 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 în cauză. 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 participă la CCD, 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 participă la CCD implicată într-o potențială fuziune sau preluare va trebui să efectueze sau să facă obiectul unui proces de diligență. Adesea, acest lucru presupune colectarea și prelucrarea de date cu caracter personal, cum ar fi informațiile cu privire la persoanelor din conducerea executivă 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 realizarea unui proces de diligență sau auditorii care efectuează un audit pot prelucra informații fără cunoștința persoanei în cauză numai în măsura și pe perioada necesară îndeplinirii cerințelor legale sau a cerințelor legate de interesul public, precum și în alte circumstanțe în care aplicarea prezentelor principii ar aduce atingere intereselor legitime ale organizației. Aceste interese legitime includ supravegherea respectării de către organizații a obligațiilor lor legale și a activităților lor contabile legitime și necesitatea confidențialității în contextul eventualelor achiziții, fuziuni, asocieri în participațiune sau al altor tranzacții similare efectuate de băncile de investiții sau de auditori.

5. **Rolul autorităților pentru protecția datelor**

a. Organizațiile își vor asuma un angajament de cooperare cu APD, astfel cum se descrie mai jos. În temeiul CCD UE-SUA, organizațiile din SUA care primesc date cu caracter personal din UE trebuie să se angajeze să utilizeze mecanisme eficace pentru a asigura respectarea principiilor. Mai exact, astfel cum prevede principiul recursului, punerii în aplicare și răspunderii, organizațiile participante trebuie să prevadă: (a)(i) modalități de recurs persoanelor la care se referă datele, (a)(ii) proceduri de urmărire pentru verificarea veridicității afirmațiilor și a declarațiilor pe care le fac organizațiile cu privire la practicile lor de protecție a vieții private și (a)(iii) obligații de remediere a problemelor care rezultă în urma nerespectării principiilor și consecințele pentru aceste organizații. O organizație trebuie să îndeplinească cerințele prevăzute la punctele (a)(i) și (a)(iii) din principiul recursului, punerii în aplicare și răspunderii în cazul în care aderă la cerințele stabilite în prezenta secțiune pentru cooperarea cu APD.

b. O organizație își ia angajamentul de a coopera cu APD declarând în autocertificarea sa de aderare la CCD UE-SUA adresată departamentului (a se vedea principiul suplimentar privind autocertificarea) că organizația:

i. decide să îndeplinească cerințele de la punctele (a)(i) și (a)(iii) din principiul recursului, punerii în aplicare și răspunderii, luându-și angajamentul de a coopera cu APD;

ii. va coopera cu APD în investigarea și soluționarea plângerilor înaintate în temeiul principiilor și

iii. se va conforma oricărui aviz emis de APD potrivit căruia organizația trebuie să adopte măsuri specifice în vederea respectării principiilor, inclusiv măsuri reparatorii sau compensatorii în beneficiul persoanelor afectate de nerespectarea principiilor, și va informa APD în scris că au fost întreprinse astfel de acțiuni.

c. Funcționarea comitetelor APD

i. Cooperarea cu APD se traduce prin informații și avize acordate în modul următor:

1. APD vor fi consultate prin intermediul unui comitet informal al APD înființat la nivel european care, printre altele, va contribui la elaborarea unei abordări armonizate și coerente;

2. comitetul va emite un aviz organizațiilor din SUA în cauză cu privire la plângerile nesoluționate din partea unor persoane privind prelucrarea informațiilor cu caracter personal care au fost transferate din UE în temeiul CCD UE-SUA. Acest aviz are ca obiectiv asigurarea unei aplicări corecte a principiilor și se referă, de asemenea, la măsurile reparatorii pe care APD le consideră corespunzătoare pentru persoana (persoanele) în cauză;

3. comitetul va emite acest aviz ca răspuns la sesizările organizațiilor în cauză și/sau la plângerile introduse direct de persoane împotriva organizațiilor care și-au luat angajamentul de a coopera cu APD în sensul respectării principiilor CCD UE-SUA, încurajând și sprijinind, după caz, aceste persoane să apeleze mai întâi la eventualele mecanisme interne de gestionare a plângerilor ale organizației în cauză;

4. avizul se emite numai după ce ambele părți implicate în litigiu au avut posibilitatea rezonabilă de a-și prezenta observațiile și de a aduce toate elementele de probă pe care doresc să le prezinte. Comitetul va încerca să transmită avizul cât mai repede posibil, însă respectând garanțiile procedurale. Ca regulă generală, comitetul se va pronunța în termen de 60 de zile după primirea unei plângeri sau înaintarea unei sesizări și înainte de expirarea acestui termen, atunci când acest lucru este posibil.

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

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

ii. Astfel cum s-a menționat mai sus, organizațiile care optează pentru acest mod de soluționare a litigiilor trebuie să-și asume 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 furnizarea avizului și nu oferă o explicație satisfăcătoare pentru întârziere, comitetul își va notifica intenția fie de a sesiza în această privință FTC, DoT sau un alt organism federal sau statal din SUA cu competențe legale de stabilire a unor măsuri de asigurare a respectării legii în situații de fraudă și declarații false, fie de a concluziona că angajamentul de cooperare a fost grav încălcat și prin urmare trebuie considerat nul și neavenit. În acest ultim caz, comitetul informează departamentul în acest sens pentru ca lista Cadrului privind confidențialitatea datelor să poată fi modificată corespunzător. Orice încălcare a angajamentului de cooperare cu APD, precum și nerespectarea principiilor pot fi sancționate ca practici frauduloase în temeiul secțiunii 5 din Legea FTC (titlul 15 articolul 45 din U.S.C.), titlul 49 articolul 41712 din U.S.C. sau în temeiul unei legi similare.

d. O organizație care dorește ca beneficiile CCD UE-SUA să vizeze datele 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 referitor la datele privind resursele umane).

e. Organizațiile care aleg această opțiune vor trebui să plătească o taxă anuală, care va fi concepută pentru a acoperi costurile de funcționare ale comitetului. În plus, acestora li se poate cere să suporte orice cheltuieli de traducere necesare care decurg din examinarea de către comitet a sesizărilor sau a plângerilor împotriva organizațiilor. Valoarea taxei va fi stabilită de departament după consultarea Comisiei. Colectarea taxei poate fi efectuată de o parte terță aleasă de departament pentru a servi drept custode al fondurilor colectate în acest scop. Departamentul va coopera îndeaproape cu Comisia și cu APD cu privire la stabilirea unor proceduri adecvate pentru distribuirea fondurilor colectate prin intermediul taxei, precum și cu privire la alte aspecte procedurale și administrative care vizează comitetul. Departamentul și Comisia pot conveni să modifice frecvența colectării taxei.

6. **Autocertificarea**

a. Beneficiile CCD UE-SUA sunt asigurate de la data la care departamentul include organizația pe lista Cadrului privind confidențialitatea datelor. Departamentul va include o organizație pe lista Cadrului privind confidențialitatea datelor numai după ce a stabilit că solicitarea inițială de autocertificare a organizației este completă și va elimina organizația de pe lista respectivă dacă aceasta se retrage în mod voluntar, nu își finalizează recertificarea anuală sau dacă nu respectă în mod sistematic principiile (*a se vedea* principiul suplimentar privind soluționarea litigiilor și punerea în aplicare a deciziilor).

b. Pentru a se autocertifica inițial sau pentru a se recertifica ulterior în ceea ce privește CCD UE-SUA, o organizație trebuie să prezinte departamentului, de fiecare dată, o cerere din partea reprezentantului organizației în numele organizației care se autocertifică sau care recertifică (după caz) adeziunea la principii ([8]), care să conțină cel puțin următoarele informații:

([8]) Cererea se transmite prin intermediul site-ului web al departamentului destinat Cadrului privind confidențialitatea datelor, de către o persoană din cadrul organizației care este autorizată să prezinte observații în numele organizației și al oricărei entități a acesteia care face obiectul cererii respective cu privire la adeziunea la principii.

i. denumirea organizației din SUA care se autocertifică sau se recertifică, precum și denumirea (denumirile) oricăreia dintre entitățile sale din SUA sau ale filialelor sale din SUA care aderă, de asemenea, la principii, și pe care organizația dorește să le includă în certificare;

ii. descrierea activităților organizației cu privire la informațiile cu caracter personal care ar urma să fie primite din UE în temeiul CCD UE-SUA;

iii. descrierea politicii/politicilor relevante de confidențialitate a organizației cu privire la informațiile cu caracter personal menționate, care să precizeze:

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

2. data punerii în aplicare a acestor dispoziții;

iv. unitatea din cadrul organizației care poate fi contactată pentru gestionarea plângerilor, pentru cererile de acces sau pentru orice altă problemă legată de principii ([9]), inclusiv:

1. numele, funcția (funcțiile) (după caz), adresa (adresele) de e-mail și numărul (numerele) de telefon ale persoanei (persoanelor) relevante sau ale unității (unităților) de contact relevante din cadrul organizației și

2. adresa poștală relevantă din SUA a organizației;

v. denumirea organismului statutar specific care deține competența de examinare a oricăror plângeri înaintate împotriva organizației în legătură cu eventuale practici neloiale sau frauduloase și încălcări ale legilor sau reglementărilor privind protecția vieții private (și care este menționat în principii sau într-o viitoare anexă la principii);

vi. numele oricărui program de protecție a vieții private la care participă organizația;

vii. metoda de verificare (și anume autoevaluarea sau evaluări externe ale conformității, inclusiv partea terță care realizează aceste evaluări) ([10]) și

viii. mecanismul (mecanismele) independent(e) de recurs relevant(e), disponibil(e) pentru investigarea plângerilor nesoluționate legate de principii ([11]).

c. În cazul în care o organizație dorește să extindă beneficiile CCD UE-SUA la informațiile privind resursele umane transferate din UE pentru a fi utilizate în contextul unui raport de muncă, aceasta poate face acest lucru atunci când unul dintre organismele statutare menționate în principii sau într-o viitoare anexă la principii deține competența de a examina plângerile depuse împotriva organizației care rezultă din prelucrarea informațiilor privind resursele umane. În plus, organizația trebuie să indice în cererea sa de autocertificare inițială, precum și în orice cerere de recertificare că dorește acest lucru și că se angajează să coopereze cu autoritatea sau autoritățile din UE în cauză în conformitate cu principiile suplimentare referitoare la datele privind resursele umane și rolul autorităților pentru protecția datelor (după caz), precum și că vor respecta recomandările acestor 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 angajații afectați.

([9]) Principalul „punct de contact al organizației" sau „reprezentantul organizației" nu poate fi din afara organizației (de exemplu, un consilier sau un consultant extern).

([10]) *A se vedea* principiul suplimentar privind verificarea).

([11]) *A se vedea* principiul suplimentar privind soluționarea litigiilor și punerea în aplicare a deciziilor.

d. Departamentul va menține și va pune la dispoziția publicului lista organizațiilor care au depus cereri de autocertificare inițială complete în temeiul Cadrului privind confidențialitatea datelor și va actualiza lista respectivă pe baza cererilor de recertificare anuale complete, precum și a notificărilor primite în temeiul principiului suplimentar privind soluționarea litigiilor și punerea în aplicare a deciziilor. Aceste cereri de autocertificare trebuie trimise cel puțin o dată pe an; în caz contrar, organizația va fi eliminată de pe lista Cadrului privind confidențialitatea datelor, iar beneficiile CCD UE-SUA nu vor mai fi asigurate. Toate organizațiile incluse de departament pe lista Cadrului privind confidențialitatea datelor trebuie să dispună de politici de confidențialitate relevante care respectă principiul notificării și să își precizeze adeziunea la principii în politicile de confidențialitate respective ([12]). În cazul în care este disponibilă online, politica de confidențialitate a unei organizații trebuie să includă un hyperlink către site-ul web al departamentului destinat Cadrului privind confidențialitatea datelor și un hyperlink către site-ul web sau către formularul de înaintare a plângerilor al mecanismului independent de recurs disponibil pentru a investiga gratuit plângerile nesoluționate legate de principii.

e. Principiile se aplică imediat după autocertificare. Organizațiile participante care s-au autocertificat anterior în conformitate cu principiile Cadrului privind Scutul de confidențialitate vor trebui să își actualizeze politicile de confidențialitate pentru a face trimitere la „principiile Cadrului UE-SUA privind confidențialitatea datelor”. Aceste organizații trebuie să includă trimiterea respectivă cât mai curând posibil și, în orice caz, nu mai târziu de trei luni de la data intrării în vigoare a principiilor Cadrului UE-SUA privind confidențialitatea datelor.

f. O organizație trebuie să supună principiilor toate datele cu caracter personal primite din UE în baza CCD UE-SUA. Angajamentul de aderare la principii nu este limitat în timp în ceea ce privește datele cu caracter personal primite în perioada în care organizația beneficiază de CCD UE-SUA; 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, CCD UE-SUA. O organizație care dorește să se retragă din CCD UE-SUA trebuie să notifice departamentul în acest sens în avans. Această notificare trebuie să indice, de asemenea, ce anume va face organizația respectivă cu datele cu caracter personal primite în temeiul CCD UE-SUA (și anume păstrează, returnează sau șterge datele și, în cazul în care păstrează datele, mijloacele autorizate prin care va asigura protecția datelor). O organizație care se retrage din CCD UE-SUA, însă dorește să păstreze astfel de date, trebuie să își declare anual în fața departamentului angajamentul de a continua să aplice principiile sau să furnizeze un nivel „adecvat” de protecție în ceea ce privește datele prin alte mijloace autorizate (de exemplu, aplicând un contract care reflectă pe deplin cerințele clauzelor contractuale standard relevante adoptate de către Comisie); în caz contrar, organizația trebuie să returneze sau să șteargă informațiile respective ([13]). O organizație care se retrage din CCD UE-SUA trebuie să elimine din orice politică de confidențialitate relevantă orice trimiteri la CCD UE-SUA care implică faptul că organizația continuă să participe la CCD UE-SUA și că are dreptul să beneficieze de acesta.

([12]) O organizație care se autocertifică pentru prima dată nu poate preciza participarea la CCD UE-SUA în politica sa finală de confidențialitate înainte ca departamentul să notifice organizația că poate acționa astfel. Organizația în cauză trebuie să furnizeze departamentului un proiect de politică de confidențialitate, care să fie în conformitate cu principiile, atunci când își prezintă cererea de autocertificare inițială. Odată ce departamentul a stabilit că respectiva cerere de autocertificare inițială a organizației este completă în celelalte privințe, departamentul va notifica organizației că ar trebui să își finalizeze (de exemplu, să publice, dacă este cazul) politica de confidențialitate conformă cu CCD UE-SUA. Organizația trebuie să informeze cu promptitudine departamentul de îndată ce politica de confidențialitate relevantă este finalizată, moment în care departamentul va înscrie organizația pe lista Cadrului privind confidențialitatea datelor.

([13]) Dacă, la momentul retragerii, o organizație alege să păstreze datele cu caracter personal pe care le-a primit în temeiul CCD UE-SUA și să declare anual departamentului că va continua să aplice principiile în ceea ce privește astfel de date, organizația trebuie să comunice departamentului o dată pe an de la retragerea sa (și anume cu excepția cazului în care și până când organizația oferă un nivel „adecvat” de protecție în ceea ce privește astfel de date prin alte mijloace autorizate sau returnează sau șterge toate aceste date și notifică departamentul în acest sens) care sunt acțiunile pe care le-a întreprins în legătură cu datele cu caracter personal respective, care sunt acțiunile pe care le va întreprinde în legătură cu oricare dintre datele cu caracter personal pe care continuă să le păstreze și care este punctul de contact permanent desemnat pentru orice întrebări legate de principii.

g. O organizație care încetează să existe ca persoană juridică distinctă ca urmare a unei schimbări a statutului său corporativ, precum o schimbare survenită în urma unei fuziuni, a unei preluări, a falimentului sau a dizolvării trebuie să notifice departamentul în acest sens în avans. Notificarea ar trebui să indice, de asemenea, dacă entitatea rezultată în urma schimbării statutului corporativ (i) va continua să participe la CCD UE-SUA prin intermediul unei autocertificări existente, (ii) se va autocertifica în calitate de organizație nou participantă la CCD UE-SUA (de exemplu, în cazul în care noua entitate sau entitatea rămasă nu dispune deja de o autocertificare prin care ar putea participa la CCD UE-SUA) sau (iii) va institui alte garanții, cum ar fi un acord scris prin care se obligă să asigure aplicarea în continuare a principiilor în ceea ce privește orice date cu caracter personal pe care organizația le-a primit în temeiul CCD UE-SUA și care vor fi păstrate. În cazul în care nu se aplică niciunul dintre subpunctele (i), (ii) și nici (iii), orice date cu caracter personal primite în temeiul CCD UE-SUA trebuie returnate sau șterse cu promptitudine.

h. Atunci când o organizație părăsește CCD UE-SUA, indiferent de motiv, aceasta trebuie să elimine toate declarațiile care implică faptul că organizația participă în continuare la CCD UE-SUA sau are dreptul să beneficieze de CCD UE-SUA. Dacă se utilizează marca de certificare aferentă CCD UE-SUA, aceasta trebuie, de asemenea, eliminată. Orice declarație falsă adresată publicului larg cu privire la adeziunea unei organizații la principii poate fi sancționată de FTC, DoT sau alt organism guvernamental relevant. Orice declarație falsă adresată departamentului poate fi sancționată în temeiul Legii privind declarațiile false (titlul 18 articolul 1001 din U.S.C).

7. **Verificarea**

a. Organizațiile trebuie să asigure proceduri de urmărire pentru verificarea veridicității afirmațiilor și a declarațiilor pe care le fac cu privire la practicile lor de protecție a vieții private în temeiul CCD UE-SUA și pentru verificarea punerii în aplicare a acestor practici astfel cum au fost prezentate și în conformitate cu principiile.

b. Pentru a răspunde cerințelor de verificare ale principiului recursului, punerii în aplicare și răspunderii, o organizație trebuie să verifice astfel de afirmații și declarații fie prin intermediul unei autoevaluări, fie prin intermediul unor evaluări externe ale conformității.

c. În cazul în care organizația optează pentru autoevaluare, această verificare trebuie să demonstreze că politica sa de confidențialitate în ceea ce privește informațiile cu caracter personal primite din UE este exactă, cuprinzătoare, ușor accesibilă, conformă cu principiile și pusă în aplicare integral (și anume respectată). De asemenea, aceasta trebuie să indice faptul că persoanele sunt informate cu privire la orice mecanism intern de gestionare a plângerilor și cu privire la mecanismul (mecanismele) independent(e) de recurs prin care pot depune plângeri, că organizația dispune de proceduri de formare a angajaților cu privire la punerea în aplicare a acestora și de sancționare în cazul nerespectării lor și că există proceduri interne privind evaluarea obiectivă și periodică a respectării celor de mai sus. O declarație care confirmă că a fost efectuată autoevaluarea trebuie semnată, cel puțin o dată pe an, de către reprezentantul organizației sau de către alt reprezentat autorizat al acesteia și trebuie pusă la dispoziție, la cerere, persoanelor în cauză sau în contextul unei investigații ori al unei plângeri pentru neconformitate.

d. În cazul în care organizația optează pentru evaluarea externă a conformității, această verificare trebuie să demonstreze că politica sa de confidențialitate în ceea ce privește informațiile cu caracter personal primite din UE este exactă, cuprinzătoare, ușor accesibilă, conformă cu principiile și pusă în aplicare integral (și anume respectată). De asemenea, aceasta trebuie să indice faptul că persoanele sunt informate cu privire la mecanismul (mecanismele) prin care pot depune plângeri. Metodele de evaluare pot include, fără a se limita la acestea, auditul, verificările aleatorii, utilizarea de „capcane” sau utilizarea unor instrumente tehnologice, după caz. O declarație care confirmă că a fost efectuată o evaluare externă a conformității trebuie semnată, cel puțin o dată pe an, de către cel care a efectuat evaluarea sau de către reprezentantul organizației sau de către alt reprezentat autorizat al acesteia și trebuie pusă la dispoziție, la cerere, persoanelor în cauză sau în contextul unei investigații ori al unei plângeri pentru neconformitate.

e. Organizațiile trebuie să păstreze evidențe referitoare la punerea în aplicare a practicilor lor cu privire la protecția vieții private în temeiul CCD UE-SUA și să le pună la dispoziție, la cerere, organismului independent de soluționare a litigiilor responsabil pentru investigarea plângerilor sau agenției competente în materie de practici neloiale și frauduloase, în contextul unei investigații sau al unei plângeri pentru neconformitate. De asemenea, organizațiile trebuie să răspundă cu promptitudine 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, dreptul de acces este fundamental pentru protecția vieții private. În special, acesta îi 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 cum că organizația respectivă prelucrează sau nu date cu caracter personal care o privesc ([14]);

2. de a i se comunica aceste date, astfel încât să poată verifica acuratețea 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 principiilor.

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 sau care este natura sau utilizarea informațiilor care fac obiectul cererii de acces.

iii. Întrucât dreptul de acces este fundamental, organizațiile trebuie să depună întotdeauna eforturi cu bună credință pentru a acorda accesul la date. 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 omită informațiile protejate și să pună la dispoziție celelalte informații. În cazul în care organizația decide să refuze accesul într-un anumit caz, aceasta trebuie să îi comunice persoanei care a solicitat accesul motivele care stau la baza acestei decizii, precum și un punct de contact pentru orice solicitări de informații suplimentare.

b. Dificultatea sau costurile ocazionate de acordarea accesului

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 dificultatea sau costurile ocazionate de acordarea dreptului de acces ar fi disproporționată(e) în raport cu riscurile la adresa vieții private a persoanei în cauză. Costurile și dificultatea aferente acordării accesului sunt factori importanți de care ar trebui să se țină seama, dar nu au un rol decisiv în stabilirea caracterului rezonabil al accesului.

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 beneficii importante precum o asigurare, o ipotecă sau un loc de muncă), în concordanță cu celelalte dispoziții ale prezentelor 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 accesului deplin 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.

([14]) Organizația ar trebui să răspundă solicitărilor din partea unei persoane 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. În cazul în care informațiile comerciale confidențiale pot fi separate cu ușurință de alte informații cu caracter personal care fac obiectul unei cereri de acces, organizația ar trebui să omită informațiile comerciale confidențiale și să pună la dispoziție informațiile neconfidențiale.

d. Organizarea bazelor de date

i. Accesul poate fi acordat sub forma transmiterii de informații cu caracter personal relevante de către o organizație persoanei în cauză și nu implică în mod obligatoriu accesul acesteia la baza de date a organizației.

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

e. Situații în care accesul poate fi restricționat

i. Întrucât organizațiile trebuie să depună întotdeauna eforturi cu 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 RGPD, organizația poate restricționa accesul la anumite informații în măsura în care divulgarea acestora poate aduce atingere protejării unor importante interese publice, cum ar fi securitatea 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 includ:

1. împiedicarea executării sau a aplicării legii sau a utilizării unor temeiuri private pentru introducerea unei acțiuni în justiție, inclusiv a prevenirii, a detectării sau a investigării infracțiunilor ori a exercitării dreptului la un proces echitabil;

2. divulgarea informațiilor într-o situație în care drepturile legitime sau interesele importante ale unor părți terțe ar fi încălcate;

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

4. compromiterea investigațiilor de securitate cu privire la angajați sau a mecanismelor de soluționare a reclamațiilor sau a planificării succesiunii angajaților și a restructurărilor întreprinderilor sau

5. compromiterea confidențialității necesare în legătură cu funcțiile de monitorizare, de control sau de reglementare aferente unei bune gestiuni sau în cadrul negocierilor viitoare sau în curs în care este implicată organizația.

ii. O organizație care invocă o excepție trebuie să demonstreze necesitatea acesteia și motivele pentru restricționarea accesului, precum și să indice persoanelor în cauză un punct de contact pentru solicitări de informații suplimentare.

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

i. O persoană are dreptul de a obține confirmarea cum că o organizație deține sau nu 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 percepe o taxă în acest sens, care să nu fie excesivă.

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

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

g. Cereri de acces repetate sau abuzive

i. O organizație poate stabili limite rezonabile ale 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. Cereri de acces frauduloase

i. O organizație nu este obligată să acorde accesul în cazul în care nu primește informații suficiente care să îi permită să confirme identitatea solicitantului.

i. Termenul pentru furnizarea răspunsurilor

i. Organizațiile trebuie să răspundă la cererile 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 vizate 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. Aplicabilitatea CCD UE-SUA

i. În cazul în care o organizație din UE transferă informații cu caracter personal, colectate în contextul unui raport de muncă, despre (foștii sau actualii săi) angajați către o societate-mamă, un furnizor de servicii afiliat sau un furnizor de servicii neafiliat din Statele Unite ale Americii care participă la CCD UE-SUA, transferul beneficiază de CCD UE-SUA. În acest caz, colectarea de informații, precum și prelucrarea lor înainte de transfer intră sub incidența legislației naționale a statului membru al UE în care a avut loc colectarea și toate condițiile sau restricțiile privind transferul lor în conformitate cu legislația respectivă vor trebui respectate.

ii. Principiile sunt relevante numai în caz de transfer sau de acces la evidențe identificate sau identificabile individual. Raportarea statistică bazată pe date agregate cu privire la ocuparea forței de muncă și care nu conține date cu caracter personal sau utilizarea datelor anonimizate nu prezintă riscuri pentru viața privată.

b. Aplicarea principiilor notificării și opțiunii

i. O organizație din SUA care a primit din UE informații despre angajați în temeiul CCD UE-SUA le poate comunica unor părți terțe sau le poate utiliza în alte scopuri numai în conformitate cu principiile notificării și opțiunii. 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 comunicări cu caracter publicitar –, organizația din SUA trebuie să ofere în prealabil persoanelor afectate posibilitatea de a-și exprima opțiunea, 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 au fost colectate informațiile cu caracter personal sau cu scopurile aprobate ulterior de persoana în cauză. În plus, 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 de date din unele state membre UE pot exclude alte utilizări ale acestor informații inclusiv după transferul lor în afara UE, 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, de exemplu, restricționarea accesului la datele cu caracter personal, anonimizarea anumitor date sau atribuirea de coduri sau pseudonime atunci când numele reale nu sunt necesare în scopurile administrative respective.

iv. În măsura și pe durata necesară pentru a evita afectarea capacității organizației de a lua decizii de promovare, numire sau alte decizii similare privind raporturile de muncă, o organizație nu este obligată să realizeze notificarea și să ofere posibilitatea exprimării opțiunii.

c. Aplicarea principiului accesului

i. Principiul suplimentar privind accesul oferă indicații cu privire la motivele care pot justifica refuzarea sau limitarea accesului solicitat în contextul resurselor umane. Angajatorii din UE trebuie să se respecte reglementările locale și să se asigure că angajații din UE au acces la aceste informații în conformitate cu legile din țările lor, indiferent de locul în care sunt prelucrate și păstrate datele. CCD UE-SUA prevede că o organizație care prelucrează astfel de date în Statele Unite ale Americii trebuie să coopereze la acordarea accesului fie direct, fie prin intermediul angajatorului din UE.

d. Asigurarea respectării legii

i. În măsura în care informațiile cu caracter personal sunt utilizate numai în contextul 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 o încălcare a dreptului său la protecția datelor și nu este mulțumit de rezultatul procedurii interne de reclamații, al procedurii de înaintare a plângerilor și al procedurii de recurs (sau al oricărui mecanism de soluționare a reclamațiilor aplicabil în temeiul unui contract încheiat cu un sindicat), acesta trebuie direcționat spre autoritatea națională de muncă sau pentru protecția datelor din jurisdicția în care în desfășoară activitatea angajatul respectiv. Aceasta include, de asemenea, cazurile în care responsabilitatea pentru pretinsa utilizare necorespunzătoare a informațiilor cu caracter personal îi revine organizației din SUA care a primit informațiile de la angajator și, prin urmare, implică o presupusă încălcare a principiilor. Acesta este modul cel mai eficient de soluționare a suprapunerilor care există adesea între drepturile și obligațiile stabilite, pe de o parte, de legislația muncii și de contractele de muncă la nivel local și, pe de altă parte, de legislația privind protecția datelor.

ii. O organizație din SUA participantă la CCD UE-SUA care utilizează date din UE privind resursele umane transferate din UE în contextul unui raport de muncă și care dorește ca aceste transferuri să facă obiectul CCD UE-SUA trebuie, astfel, să își ia angajamentul de a coopera în cadrul investigațiilor autorităților competente din UE și de a respecta avizele acestora.

e. Aplicarea principiului responsabilității pentru transferurile ulterioare

i. Pentru necesitățile operaționale ocazionale în contextul unui raport de muncă ale organizației care participă la CCD UE-SUA în ceea ce privește datele cu caracter personal transferate în temeiul CCD UE-SUA, cum ar fi rezervarea unui bilet de avion, rezervarea unei camere de hotel sau contractarea unei asigurări, 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 în celelalte cazuri, cu condiția ca organizația care participă la CCD UE-SUA să fi respectat principiile notificării și opțiunii.

10. **Contracte obligatorii pentru transferurile ulterioare**

a. Contracte de prelucrare a datelor

i. Transferul de date cu caracter personal din UE în Statele Unite ale Americii efectuat doar în scopul prelucrării impune încheierea unui contract, independent de participarea persoanei împuternicite de operator la CCD UE-SUA.

ii. Operatorii de date din UE 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 UE sau în afara acesteia și indiferent dacă persoana împuternicită de operator participă sau nu la CCD UE-SUA. Scopul contractului este de a asigura că persoana împuternicită de operator:

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. Deoarece organizațiile participante oferă o protecție adecvată, contractele cu aceste organizații pentru simpla prelucrare nu necesită autorizare prealabilă.

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

i. 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 transferurile ulterioare. 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 protecției informațiilor cu caracter personal în temeiul principiilor. În cazul unor astfel de transferuri, organizația care participă la CCD UE-SUA rămâne responsabilă pentru respectarea principiilor.

c. Transferurile între operatori

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

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

a. Principiul recursului, punerii în aplicare și răspunderii stabilește cerințele pentru punerea în aplicare a CCD UE-SUA. Modul în care sunt îndeplinite cerințele de la litera (a) punctul (ii) al principiului este prezentat în principiul suplimentar privind verificarea. Acest principiu suplimentar vizează litera (a) punctul (i) și litera (a) punctul (iii), ambele impunând necesitatea unor mecanisme independente de recurs. Astfel de mecanisme pot lua forme diferite, dar trebuie să îndeplinească cerințele principiului recursului, punerii în aplicare și răspunderii. Organizațiile satisfac aceste cerințe în următoarele moduri: (i) participând la programele elaborate de sectorul privat cu privire la protecția vieții private care integrează principiile în normele lor și care includ mecanisme eficiente de asigurare a respectării legii de tipul celor descrise în principiul recursului, punerii în aplicare și răspunderii, (ii) conformându-se instrucțiunilor autorităților de supraveghere sau de reglementare legale care asigură gestionarea plângerilor persoanelor și soluționarea litigiilor sau (iii) luându-și angajamentul de a coopera cu APD din UE 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 legii, atât timp cât acestea îndeplinesc cerințele principiului recursului, punerii în aplicare și răspunderii, precum și ale principiilor suplimentare. Trebuie remarcat faptul că respectivele cerințe ale principiului recursului, punerii în aplicare și răspunderii vin în completarea cerinței conform căreia inițiativele de autoreglementare trebuie să poată fi aplicate în conformitate cu secțiunea 5 din Legea FTC (titlul 15 articolul 45 din U.S.C) care interzice practicile neloiale și frauduloase, titlul 49 articolul 41712 din U.S.C., care interzice unui transportator sau unui agent de bilete să desfășoare orice practică neloială sau frauduloasă în cadrul activității de transport aerian sau pentru vânzarea de servicii de transport aerian sau o altă lege sau reglementare care interzice astfel de practici.

c. Pentru a asigura respectarea angajamentelor asumate în temeiul CCD UE-SUA și pentru a sprijini gestionarea programului, organizațiile, precum și mecanismele independente de recurs ale acestora trebuie să furnizeze informații cu privire la CCD UE-SUA 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. Mecanisme de recurs

i. Persoanele ar trebui să fie încurajate să adreseze eventualele plângeri organizației în cauză înainte de a se adresa mecanismelor independente de recurs. Organizațiile trebuie să răspundă unei persoane în termen de 45 de zile de la primirea plângerii. Independența unui mecanism 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 răspunderii, mecanismele de recurs disponibile persoanelor trebuie să fie ușor accesibile și să nu implice costuri pentru acestea. Organismele independente de soluționare a litigiilor trebuie să examineze fiecare plângere primită de la persoane, exceptând cazurile în care acestea sunt în mod evident nefondate sau abuzive. Această dispoziție nu împiedică stabilirea unor condiții de eligibilitate de către organismul independent de soluționare a litigiilor 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 al programului sau care sunt de competența altei instanțe) și nu trebuie să aibă ca rezultat subminarea angajamentului de examinare a plângerilor legitime. În plus, mecanismele de recurs ar trebui să ofere persoanelor informații complete și ușor accesibile cu privire la modul în care funcționează procedura de soluționare a litigiilor atunci când acestea depun o plângere. Aceste informații ar trebui să includă o descriere a practicilor de protecție a vieții private ale mecanismului, în conformitate cu principiile. De asemenea, acestea ar trebui să coopereze în vederea elaborării de instrumente, precum formularele tip pentru plângeri, pentru a facilita procedura de soluționare a litigiilor.

ii. Mecanismele independente de recurs trebuie să includă pe site-urile lor web publice informații cu privire la principii și serviciile pe care acestea le furnizează în temeiul CCD UE-SUA. Informațiile în cauză trebuie să includă: (1) informații despre sau un link către cerințele principiilor referitoare la mecanismele independente de recurs, (2) un hyperlink către site-ul web al departamentului destinat Cadrului privind confidențialitatea datelor, (3) o explicație privind caracterul gratuit al serviciilor de soluționare a litigiilor în temeiul CCD UE-SUA, (4) o descriere a modului în care se poate înainta o plângere legată de principii, (5) termenul în care sunt prelucrate plângerile legate principii și (6) o descriere a gamei de soluții posibile.

iii. Mecanismele independente de recurs trebuie să publice un raport anual care să furnizeze statistici agregate privind serviciile lor de soluționare a litigiilor. Raportul anual trebuie să conțină: (1) numărul total de plângeri legate de principii primite în cursul anului de raportare, (2) tipurile de plângeri primite, (3) măsurile cu privire la calitatea procesului de soluționare a litigiilor, cum ar fi perioada de timp necesară pentru soluționarea plângerilor și (4) rezultatele plângerilor primite, în special numărul și tipul de măsuri reparatorii sau sancțiuni impuse.

iv. Astfel cum se prevede în anexa I, o opțiune de arbitraj este pusă la dispoziția unei persoane pentru a se stabili, pentru plângerile reziduale, dacă o organizație care participă la CCD UE-SUA și-a încălcat obligațiile care îi revin în temeiul principiilor cu privire la persoana în cauză și dacă orice astfel de încălcare rămâne neremediată integral sau parțial. Această opțiune este disponibilă numai în aceste scopuri. Această opțiune nu este disponibilă, de exemplu, în ceea ce privește exceptările de la principii ([15]) sau o afirmație cu privire la caracterul adecvat al CCD UE-SUA. În cadrul acestei opțiuni de arbitraj, „comisia de arbitraj pentru Cadrul UE-SUA privind confidențialitatea datelor” (formată din unul sau din trei arbitri, astfel cum s-a convenit de către părți) are autoritatea de a impune măsuri nemonetare, echitabile și personalizate (precum accesul la datele persoanei în cauză și rectificarea, ștergerea sau returnarea acestora) necesare pentru a remedia încălcarea principiilor numai cu privire la persoana în cauză. Persoanele și organizațiile care participă la CCD UE-SUA vor putea să inițieze o procedură de control jurisdicțional și să solicite punerea în aplicare a hotărârilor arbitrale în temeiul legislației SUA, în conformitate cu Legea federală privind arbitrajul.

e. Măsuri reparatorii și sancțiuni

i. Rezultatul oricăror măsuri reparatorii oferite de organismul independent de soluționare a litigiilor ar trebui să fie că efectele nerespectării sunt anulate sau corectate de organizație, în măsura în care acest lucru este fezabil, și că prelucrarea viitoare de către organizație se va efectua în conformitate cu principiile și, după caz, că prelucrarea datelor cu caracter personal ale persoanei care a depus plângerea va înceta. 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 organismelor de soluționare a litigiilor să răspundă în

([15]) Punctul 5 secțiunea „Prezentare generală” din principii.

mod corespunzător diferitelor niveluri de nerespectare a principiilor. Sancțiunile ar trebui să includă atât publicarea constatărilor de nerespectare, cât și obligația de a șterge datele în anumite circumstanțe ([16]). Alte sancțiuni pot include suspendarea sau îndepărtarea unei mărci de conformitate, despăgubirea persoanelor pentru prejudiciile suferite ca urmare a nerespectării principiilor, precum și ordine cu caracter reparatoriu. Organismele independente de soluționare a litigiilor și de autoreglementare din sectorul privat trebuie să semnaleze organismului guvernamental competent sau instanțelor, după caz, și departamentului nerespectarea de către organizațiile care participă la CCD UE-SUA a deciziilor acestora.

f. Acțiunile FTC

i. FTC s-a angajat să acorde prioritate examinării sesizărilor referitoare la pretinsa nerespectare a principiilor, prezentate de: (i) organizații de autoreglementare în domeniul protecției vieții private și de alte organisme independente de soluționare a litigiilor, (ii) state membre ale UE și (iii) de departament, pentru a stabili dacă a fost încălcată secțiunea 5 din Legea FTC, care interzice actele sau practicile neloiale sau frauduloase în comerț. În cazul în care stabilește că există un temei pentru a considera că secțiunea 5 a fost încălcată, FTC poate soluționa această problemă obținând un ordin administrativ de încetare care să interzică practicile contestate sau depunând o plângere la o instanță districtuală federală, care, în cazul în care plângerea este soluționată favorabil, poate emite un ordin judecătoresc cu aceleași efecte. Această situație vizează declarațiile false de adeziune la principii sau de participare la CCD UE-SUA emise de către organizații care fie nu se mai află pe lista Cadrului privind confidențialitatea datelor, fie nu au prezentat niciodată o autocertificare departamentului. FTC poate obține impunerea unor sancțiuni civile pentru încălcarea unui ordin administrativ de încetare și poate urmări contravenientul pentru sfidarea curții în materie de drept civil sau penal în cazul încălcării ordinului unei instanțe federale. FTC informează departamentul cu privire la orice acțiune de acest tip întreprinsă. Departamentul încurajează alte organisme guvernamentale să îl înștiințeze cu privire la luarea unei decizii definitive în cazul oricăror astfel de sesizări sau a altor decizii care vizează aderarea la principii.

g. Încălcarea sistematică a principiilor

i. În cazul în care o organizație încalcă sistematic principiile, aceasta nu mai are dreptul să beneficieze de CCD UE-SUA. Organizațiile care au încălcat în mod sistematic principiile vor fi eliminate de pe lista Cadrului privind confidențialitatea datelor de către departament și trebuie să returneze sau să șteargă informațiile cu caracter personal primite în temeiul CCD UE-SUA.

ii. Principiile sunt încălcate sistematic atunci când o organizație care a prezentat departamentului o autocertificare refuză să se conformeze unei decizii definitive luate de orice organism de autoreglementare în domeniul protecției vieții private, un organism independent de soluționare a litigiilor sau un organism guvernamental sau, atunci când un asemenea organism, inclusiv departamentul, constată că aceasta încalcă atât de frecvent principiile încât declarația sa de respectare a acestora nu mai este credibilă. În cazurile în care o astfel de decizie este luată de un alt organism decât departamentul, organizația trebuie să notifice imediat departamentul în acest sens. În caz contrar, aceasta este pasibilă de sancțiuni în temeiul Legii privind declarațiile false (titlul 18 articolul 1001 din U.S.C). Retragerea unei organizații dintr-un program de autoreglementare în domeniul protecției vieții private elaborat 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 acestora.

iii. Departamentul va elimina o organizație de pe lista Cadrului privind confidențialitatea datelor pentru o încălcare sistematică a principiilor, inclusiv ca răspuns la orice notificare pe care o primește cu privire la o astfel de nerespectare din partea organizației, a unui organism de autoreglementare în domeniul protecției vieții private sau a unui alt organism independent de soluționare a litigiilor sau a unui organism guvernamental, însă numai după ce a acordat organizației un preaviz de 30 de zile și posibilitatea de a răspunde ([17]). În consecință, lista Cadrului privind confidențialitatea datelor gestionată de departament va preciza care organizații beneficiază de CCD UE-SUA și care organizații nu mai beneficiază de acesta.

iv. O organizație care solicită să fie supusă autorității unui organism de autoreglementare pentru a putea beneficia din nou de CCD UE-SUA trebuie să furnizeze acestui organism informații complete cu privire la participarea sa anterioară la CCD UE-SUA.

([16]) Organismele independente 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.

([17]) Departamentul va indica în notificare perioada de timp, care va fi în mod necesar mai mică de 30 de zile, în care organizația trebuie să răspundă la notificare.

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

a. În general, obiectivul principiului opțiunii este de a garanta că informațiile cu caracter personal sunt utilizate și divulgate 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, o persoană ar trebui să poată să își exercite opțiunea de a refuza în orice moment o astfel de utilizare, în limitele rezonabile definite de organizație, cum ar fi timpul necesar pentru a permite organizației punerea în aplicare a refuzului. De asemenea, organizația poate solicita informații suficiente pentru a confirma identitatea persoanei care și-a exprimat refuzul. În Statele Unite ale Americii, persoanele își pot exercita această opțiune prin intermediul unui program central de refuz. În orice caz, exercitarea acestei opțiuni ar trebui să se realizeze în baza unui mecanism ușor accesibil și puțin costisitor.

b. În mod similar, o organizație poate utiliza informații în anumite scopuri de marketing direct atunci când condițiile nu permit exprimarea opțiunii de refuz a 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 ca aceasta să implice costuri pentru persoana în cauză) să primească orice alte comunicări directe cu caracter publicitar și ca aceasta să se conformeze dorințelor acestor persoane.

13. **Informații cu privire la călătorii**

a. Informațiile cu privire la rezervările pasagerilor curselor aeriene și alte informații cu privire la călătorii, 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 UE în diferite circumstanțe. În temeiul RGPD, datele cu caracter personal pot fi transferate, în absența unei decizii privind caracterul adecvat al nivelului de protecție, către o țară terță dacă sunt prevăzute garanții adecvate în materie de protecție a datelor în temeiul articolului 46 din RGPD sau, în situații specifice, dacă este îndeplinită una dintre condițiile prevăzute la articolul 49 din RGPD (de exemplu, în cazul în care persoana vizată și-a exprimat în mod explicit acordul cu privire la transfer). Organizațiile din SUA care subscriu la CCD UE-SUA oferă o protecție adecvată a datelor cu caracter personal și, prin urmare, pot primi transferuri de date din UE în temeiul articolului 45 din RGPD, fără a fi nevoite să instituie un instrument de transfer în temeiul articolului 46 din RGPD sau să îndeplinească condițiile prevăzute la articolul 49 din RGPD. Întrucât CCD UE-SUA cuprinde reguli specifice cu privire la informațiile sensibile, acest tip de informații (care pot fi colectate, de exemplu, în legătură cu necesitatea clientului de a beneficia de asistență fizică) poate fi inclus în transferurile către organizații care participă la CCD UE-SUA. În toate cazurile, însă, organizația care transferă informațiile trebuie să respecte legislația statului membru al UE în care își desfășoară activitatea, care poate impune, printre altele, condiții speciale pentru gestionarea datelor sensibile.

14. **Produse farmaceutice și medicale**

a. Aplicarea legislației UE/a statelor membre sau a principiilor

i. Legislația UE/a statelor membre se aplică în cazul colectării de date cu caracter personal și al oricărei prelucrări care are loc înainte de transferul către Statele Unite ale Americii. Principiile se aplică datelor odată ce acestea au fost transferate către Statele Unite ale Americii. Datele utilizate pentru cercetarea farmaceutică și în alte scopuri ar trebui anonimizate, după caz.

b. Cercetarea științifică viitoare

i. Datele cu caracter personal elaborate în cadrul studiilor medicale sau farmaceutice joacă adesea un rol important în cercetarea științifică viitoare. Atunci când datele cu caracter personal colectate pentru un studiu de cercetare sunt transferate unei organizații din SUA care participă la CCD UE-SUA, 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 monitorizarea periodică, 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 inițiale, noi descoperiri și progrese medicale, precum și evoluția în domeniul sănătății publice și al reglementărilor ar putea determina noi utilizări ale datelor în scopuri de cercetare. 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 în care au fost colectate inițial datele sau pentru care persoana în cauză și-a exprimat acordul, trebuie obținut un nou acord al persoanei vizate.

c. Retragerea dintr-un studiu clinic

i. Participanții pot decide sau pot fi invitați să se retragă dintr-un studiu clinic în orice moment. Cu toate acestea, datele cu caracter personal 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 de participare.

d. Transferurile în scopuri de reglementare și de supraveghere

i. Societățile farmaceutice și societățile producătoare de dispozitive medicale au dreptul de a transmite date cu caracter personal extrase din studiile clinice efectuate în UE către autoritățile din Statele Unite ale Americii în scopuri de reglementare și de supraveghere. Este permisă realizarea unor transferuri similare și altor părți decât autoritățile de reglementare, cum ar fi întreprinderile și alți cercetători, în conformitate cu principiile notificării și opțiunii.

e. Studii „oarbe”

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

ii. Acordul de a participa la studiu în aceste condiții presupune renunțarea în mod rezonabil la dreptul de acces. La încheierea studiului 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 furnizor de asistență medicală de la care au primit tratamentul în cadrul studiului clinic sau, în al doilea rând, organizației care a sponsorizat programul.

f. Controlul securității și al eficacității produsului

i. O societate farmaceutică sau producătoare de dispozitive medicale nu trebuie să aplice principiul notificării, al opțiunii, al responsabilității pentru transferurile ulterioare și al accesului în activitățile sale de control al securității și al eficacității produsului, inclusiv în cadrul raportării incidentelor și al urmăririi 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, atât rapoartele prezentate de furnizorii de servicii medicale societăților farmaceutice și societăților producătoare de dispozitive medicale, cât și cele prezentate de acestea agențiilor guvernamentale precum Agenția pentru Alimentație și Medicamente (*Food and Drug Administration*).

g. Date codificate

i. Datele provenite din cercetare sunt codificate în mod unic, de regulă, la sursă de către cercetătorul principal pentru a nu fi dezvăluită identitatea persoanelor vizate. Societățile farmaceutice care sponsorizează aceste cercetări nu primesc codul de acces. Codul unic de acces 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). Un transfer din UE către Statele Unite ale Americii de date codificate în acest mod, care sunt date cu caracter personal din UE în temeiul legislației UE, ar fi reglementat de principii.

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

a. O organizație trebuie să aplice principiul securității, al integrității datelor și al limitării scopului, precum și principiul recursului, punerii în aplicare și răspunderii față de datele cu caracter personal obținute 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 agenții sau entități guvernamentale la orice nivel și care pot fi consultate de publicul larg).

b. Nu este necesar să se aplice principiul notificării, al opțiunii sau al responsabilității pentru transferurile ulterioare informațiilor din registrele publice atât timp cât acestea nu sunt asociate cu informații care nu au caracter public și sunt respectate toate condițiile de consultare stabilite în jurisdicția relevantă. De asemenea, în general, nu este necesară aplicarea principiului notificării, al opțiunii sau al responsabilității pentru transferurile ulterioare în cazul informațiilor accesibile publicului decât în cazul în care entitatea europeană care efectuează transferul indică faptul că aceste informații fac obiectul unor restricții care impun aplicarea respectivelor principii de către organizație pentru utilizările preconizate. Organizațiile nu au nicio răspundere 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 înceta să mai fie eligibilă pentru a beneficia de CCD UE-SUA.

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 volume reduse de informații utilizate pentru indexarea sau organizarea registrelor publice); cu toate acestea, trebuie respectate toate condițiile de consultare stabilite în jurisdicția relevantă. În schimb, atunci când informațiile din registre publice sunt asociate cu alte informații care nu au caracter public (altele decât cele menționate mai sus), o organizație trebuie să permită accesul la toate aceste informații, în cazul în care acestea nu fac obiectul altor derogări permise.

e. La fel ca în cazul informațiilor extrase din registrele publice, nu este necesar să se acorde accesul la informații care sunt deja accesibile publicului, atât timp cât acestea nu sunt asociate cu alte date care nu sunt au caracter public. 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, persoanele pot obține accesul la informațiile care le privesc adresându-se direct primei organizații care a compilat 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 participă la CCD UE-SUA 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 asigurare a respectării legii, în măsura în care divulgările sunt admisibile în conformitate cu legislația aplicabilă.

b. Informațiile furnizate de organizațiile care participă la CCD UE-SUA în aceste rapoarte, împreună cu informațiile comunicate de către comunitatea serviciilor de informații, alături de alte informații, pot fi utilizate ca fundament pentru revizuirea comună realizată periodic cu privire la funcționarea CCD UE-SUA 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 solicitare legală.

ANEXA I: MODELUL DE ARBITRAJ

Prezenta anexă I prevede condițiile în baza cărora organizațiile participante la CCD UE-SUA sunt obligate să supună plângerile unei proceduri de arbitraj, în conformitate cu principiul recursului, punerii în aplicare și răspunderii. Opțiunea arbitrajului obligatoriu descrisă mai jos se aplică anumitor plângeri „reziduale" privind datele aflate sub incidența CCD UE-SUA. Obiectivul acestei opțiuni este de a oferi un mecanism echitabil, independent și prompt, la alegerea persoanelor în cauză, pentru soluționarea oricăror presupuse încălcări ale principiilor care nu au fost soluționate prin niciunul dintre celelalte mecanisme ale CCD UE-SUA.

A. **Domeniul de aplicare**

Această opțiune de arbitraj este pusă la dispoziția unei persoane pentru a se stabili, pentru plângerile reziduale, dacă o organizație care participă la CCD UE-SUA și-a încălcat obligațiile care îi revin în temeiul principiilor cu privire la persoana în cauză și dacă orice astfel de încălcare rămâne neremediată integral sau parțial. Această opțiune este disponibilă numai în aceste scopuri. Această opțiune nu este disponibilă, de exemplu, în ceea ce privește exceptările de la principii ([1]) sau o afirmație cu privire la caracterul adecvat al CCD UE-SUA.

B. **Măsuri reparatorii disponibile**

În cadrul acestei opțiuni de arbitraj, „comisia de arbitraj pentru Cadrul UE-SUA privind confidențialitatea datelor" (comisia de arbitraj formată din unul sau din trei arbitri, astfel cum s-a convenit de către părți) are autoritatea de a impune măsuri nemonetare, echitabile și personalizate (precum accesul la datele persoanei în cauză și rectificarea, ștergerea sau returnarea acestora) necesare pentru a remedia încălcarea principiilor numai cu privire la persoana în cauză. Acestea sunt singurele competențe ale comisiei de arbitraj pentru Cadrul UE-SUA privind confidențialitatea datelor referitoare la măsurile reparatorii. Atunci când are în vedere măsurile reparatorii, comisia de arbitraj pentru Cadrul UE-SUA privind confidențialitatea datelor este obligată să țină seama de alte măsuri reparatorii deja impuse prin alte mecanisme ale CCD UE-SUA. Nu sunt disponibile despăgubiri, măsuri reparatorii pentru costuri sau taxe sau de altă natură. Fiecare parte suportă onorariile propriilor avocați.

C. **Cerințe care trebuie îndeplinite înainte de arbitraj**

O persoană care decide să se prevaleze de această opțiune de arbitraj trebuie să ia următoarele măsuri înainte de introducerea unei cereri de arbitraj: (1) să invoce presupusa încălcare direct la organizație și să ofere organizației posibilitatea de a soluționa problema în termenele prevăzute la litera (d) punctul (i) din principiul suplimentar privind soluționarea litigiilor și punerea în aplicare a deciziilor, (2) să utilizeze mecanismul independent de recurs în temeiul principiilor, fără ca aceasta să implice vreun cost pentru persoana respectivă și (3) să se adreseze, prin intermediul APD individuale, departamentului și să ofere departamentului oportunitatea de a depune toate eforturilor pentru a soluționa problema în termenele prevăzute în scrisoarea din partea Administrației pentru Comerțul Internațional (*International Trade Administration*) din cadrul departamentului, fără ca aceasta să implice vreun cost pentru persoana respectivă.

Această opțiune de arbitraj nu poate fi invocată în cazul în care aceeași presupusă încălcare a principiilor invocată de o persoană (1) a făcut deja obiectul unei proceduri de arbitraj obligatoriu, (2) a făcut obiectul unei hotărâri cu caracter definitiv într-o acțiune în justiție la care persoana respectivă a fost parte sau (3) a fost soluționată de părți prin intermediul unei tranzacții. În plus, această opțiune nu poate fi invocată în cazul în care o APD (1) are autoritate în temeiul principiului suplimentar privind rolul autorităților pentru protecția datelor sau al principiului suplimentar referitor la datele privind resursele umane 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 APD.

D. **Caracterul obligatoriu al hotărârilor**

Decizia unei persoane de a invoca opțiunea arbitrajului obligatoriu este exclusiv voluntară. Hotărârile 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 încălcare, în care caz invocarea arbitrajului nu împiedică introducerea unei acțiuni în despăgubiri care este disponibilă în alt mod în instanță.

([1]) Punctul 5 secțiunea „Prezentare generală" din principii.

E. **Reexaminarea și punerea în aplicare**

Persoanele și organizațiile care participă la CCD UE-SUA vor putea să inițieze o procedură de control jurisdicțional și să solicite punerea în aplicare a hotărârilor arbitrale în temeiul legislației SUA, în conformitate cu Legea federală privind arbitrajul ([2]). Orice astfel de cauze trebuie introduse la instanța districtuală federală pe a cărei rază teritorială se află sediul principal al organizației care participă la CCD UE-SUA.

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

F. **Comisia de arbitraj**

Părțile selectează arbitrii care vor intra în componența comisiei de arbitraj pentru Cadrul UE-SUA privind confidențialitatea datelor din lista de arbitri discutată mai jos.

În conformitate cu legislația aplicabilă, departamentul și Comisia vor elabora o listă care va cuprinde cel puțin zece arbitri, selectați pe criterii de independență, integritate și competențe. În ceea ce privește acest proces, se aplică următoarele dispoziții:

Arbitrii

(1) vor rămâne pe listă pentru o perioadă de 3 ani, cu absențe în circumstanțe excepționale sau ca urmare a revocării din funcție din motive întemeiate, termen care poate fi reînnoit cu notificarea prealabilă a Comisiei pentru o perioadă suplimentară de 3 ani,

(2) nu se supun niciunei instrucțiuni din partea, nici nu au legătură cu vreuna dintre părți, nici cu vreo organizație care participă la CCD UE-SUA, 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 profesie juridică în SUA și să fie experți în legislația SUA privind protecția vieții private și să fie specializați în legislația UE privind protecția datelor.

([2]) Capitolul 2 din Legea federală privind arbitrajul („FAA") prevede că „[u]n acord de arbitraj sau o hotărâre arbitrală care decurge dintr-un raport juridic, contractual sau nu, care este considerată comercial, inclusiv o tranzacție, un contract sau un acord descrise în [secțiunea 2 din FAA], intră în domeniul de aplicare al Convenției [privind recunoașterea și punerea în aplicare a hotărârilor arbitrale străine din 10 iunie 1958, 21 U.S.T. 2519, T.I.A.S. nr. 6997 («Convenția de la New York»)." Titlul 9 articolul 202 din U.S.C. De asemenea, FAA prevede că, „[u]n acord sau o hotărâre arbitrală care decurge dintr-un astfel de raport exclusiv între cetățenii Statelor Unite ale Americii se consideră ca neintrând în domeniul de aplicare al Convenției [de la New York], cu excepția cazului în care acest raport implică bunuri aflate în străinătate, prevede executarea sau aplicarea în străinătate sau implică o altă legătură cu unul sau mai multe state terțe." *Idem*. În conformitate cu capitolul 2, „orice parte la arbitraj poate apela la orice instanță care are competență în temeiul prezentului capitol pentru emiterea unui ordin 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." *Idem* articolul 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 valoarea în litigiu". *Idem* articolul 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 a fost ratificată de Statele Unite ale Americii." *Idem* articolul 208. Capitolul 1, în schimb, prevede că „[o] dispoziție scrisă dintr-un [...] contract care demonstrează existența unei tranzacții care implică raporturi comerciale pentru a soluționa prin arbitraj un litigiu, 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 un litigiu existent 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 pentru revocarea unui contract." *Idem* articolul 2. Capitolul 1 prevede, de asemenea, că „orice parte la procedura de arbitraj poate solicita instanței susmenționate un ordin care să confirme ulterior hotărârea, iar instanța trebuie să acorde un 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]." *Idem* articolul 9.

G. **Procedurile de arbitraj**

Departamentul și Comisia au convenit, în conformitate cu legislația aplicabilă, asupra adoptării unor norme de arbitraj care să reglementeze procedurile desfășurate înaintea comisiei de arbitraj pentru Cadrul UE-SUA privind confidențialitatea datelor ([3]). În cazul în care normele care reglementează procedurile trebuie modificate, departamentul și Comisia vor conveni să modifice normele respective sau să adopte un set diferit de proceduri de arbitraj existente consacrate din SUA, după caz, sub rezerva următoarelor considerații:

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

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

3. Acțiunile FTC se pot desfășura în paralel cu arbitrajul.

4. Niciun reprezentant al SUA, UE sau al vreunui stat membru al UE sau vreo altă autoritate guvernamentală, autoritate publică sau autoritate de aplicare a legii nu poate participa la aceste arbitraje, cu condiția ca, la cererea unei persoane din UE, APD să poată oferi asistență doar în pregătirea notificării, fără ca APD să aibă acces la materialele divulgate în cadrul prezentării dovezilor sau la orice alte materiale referitoare la aceste proceduri de arbitraj.

5. Locul arbitrajului este Statele Unite ale Americii, iar persoana în cauză poate alege să participe prin teleconferință sau videoconferință, servicii care vor fi furnizate cu titlu gratuit persoanei în cauză. Nu va fi necesară participarea în persoană.

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 vor oferi servicii de interpretare în cadrul ședinței de arbitraj, precum și traducerea materialelor de arbitraj fără ca aceasta să implice vreun cost pentru persoana în cauză. Comisia de arbitraj pentru Cadrul UE-SUA privind confidențialitatea datelor poate considera că, în împrejurările unei anumite proceduri de arbitraj, aceasta ar 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 astfel de materiale vor fi tratate confidențial de către părți și vor fi utilizate numai în legătură cu procedura de arbitraj.

9. Procedurile de arbitraj 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.

([3]) Departamentul a selectat Centrul Internațional pentru Soluționarea Litigiilor (*International Centre for Dispute Resolution*) („ICDR"), divizia internațională a Asociației Americane de Arbitraj (*American Arbitration Association*) („AAA"), (denumite în mod colectiv „ICDR-AAA"), pentru desfășurarea procedurilor de arbitraj în conformitate cu anexa I la principii și pentru a gestiona fondul de arbitraj identificat în aceasta. La 15 septembrie 2017, departamentul și Comisia au convenit cu privire la adoptarea unui set de norme de arbitraj care să reglementeze procedurile de arbitraj obligatoriu descrise în anexa I la principii, precum și a unui cod de conduită pentru arbitri care să fie în concordanță cu standardele etice general acceptate pentru arbitrii comerciali și cu anexa I la principii. Departamentul și Comisia au convenit să adapteze normele de arbitraj și codul de conduită pentru a reflecta actualizările în temeiul CCD UE-SUA, iar departamentul va colabora cu ICDR-AAA pentru a realiza aceste actualizări.

H. **Cheltuielile de judecată**

Arbitrii ar trebui să ia măsurile necesare pentru a reduce la minimum costurile sau onorariile aferente procedurilor de arbitraj.

Departamentul va facilita, în conformitate cu legislația aplicabilă, menținerea unui fond la care organizațiile care participă la CCD UE-SUA vor trebui să contribuie, parțial în funcție de dimensiunea organizației, care va acoperi costurile de arbitraj, inclusiv onorariile arbitrilor, până la sume maxime („plafoane”). Fondul va fi gestionat de o parte terță, care va raporta cu regularitate departamentului cu privire la operațiunile aferente fondului. Departamentul va coopera cu partea terță respectivă pentru a revizui periodic funcționarea fondului, inclusiv necesitatea de a ajusta valoarea contribuțiilor sau a plafoanelor privind costurile procedurilor de arbitraj, ținând seama, printre altele, de numărul de arbitri, costurile și calendarul arbitrajelor și înțelegându-se că nu se va impune o sarcină financiară excesivă asupra organizațiilor care participă la CCD UE-SUA. Departamentul va informa Comisia cu privire la rezultatul acestor revizuiri realizate împreună cu partea terță și va transmite Comisiei o notificare prealabilă cu privire la orice ajustare a cuantumului contribuțiilor. Onorariile avocaților nu sunt vizate de prezenta dispoziție sau de vreun fond instituit în temeiul acestei dispoziții.

ANEXA II

DEPARTAMENTUL COMERȚULUI DIN STATELE UNITE ALE AMERICII
Secretarul pentru comerț
Washington, D.C. 20230

6 iulie 2023

Onorabilului Didier Reynders
Comisar pentru justiție
Comisia Europeană
Rue de la Loi/Wetstraat 200
1049 Bruxelles
Belgia

Stimate Domnule Comisar Reynders,

în numele Statelor Unite ale Americii, am plăcerea de a vă transmite în anexă un pachet de materiale referitoare la Cadrul UE-SUA privind confidențialitatea datelor, care, alături de Ordinul executiv nr. 14086 – „Enhancing Safeguards for US Signals Intelligence Activities" (Consolidarea garanțiilor pentru activitățile de colectare de informații de tip SIGINT desfășurate de Statele Unite ale Americii) și titlul 28 partea 201 din CFR de modificare a regulamentelor Departamentului de Justiție pentru instituirea „Curții de Reexaminare a Protecției Datelor", reflectă negocierile importante și detaliate derulate în vederea consolidării protecției vieții private și a libertăților civile. Aceste negocieri au condus la noi garanții care asigură necesitatea și proporționalitatea activităților de colectare de informații de tip SIGINT în urmărirea unor obiective definite de securitate națională și la un nou mecanism de recurs pentru persoanele din Uniunea Europeană („UE") în cazul în care consideră că sunt vizate în mod ilegal de activitățile de colectare de informații de tip SIGINT. Împreună, acestea vor asigura confidențialitatea datelor cu caracter personal din UE. CCD UE-SUA va sta la baza unei economii digitale favorabile incluziunii și competitive. Ar trebui să fim cu toții mândri de îmbunătățirile reflectate în acest cadru, care vor spori protecția vieții private în întreaga lume. Acest pachet, alături de ordinul executiv, regulamentele și alte materiale provenite din surse publice, oferă o bază foarte solidă pentru o nouă constatare a caracterului adecvat efectuată de Comisia Europeană ([1]).

Se anexează următoarele materiale:

— principiile Cadrului UE-SUA privind confidențialitatea datelor, inclusiv principiile suplimentare (denumite în mod colectiv „principiile") și anexa I la principii (și anume o anexă care prevede condițiile în care organizațiile care participă la Cadrul privind confidențialitatea datelor sunt obligate să supună arbitrajului anumite cereri reziduale în ceea ce privește datele cu caracter personal reglementate de principii);

— o scrisoare din partea Administrației pentru Comerțul Internațional care gestionează programul aferent Cadrului privind confidențialitatea datelor, în care se descriu angajamentele luate de departamentul nostru pentru asigurarea funcționării eficace a Cadrului UE-SUA privind confidențialitatea datelor;

— o scrisoare din partea Comisiei Federale pentru Comerț, care descrie acțiunile sale de asigurare a respectării principiilor;

— o scrisoare din partea Departamentului Transporturilor, care descrie acțiunile sale de asigurare a respectării principiilor;

— o scrisoare redactată de Biroul Directorului Serviciului Național de Informații cu privire la garanțiile și limitările aplicabile autorităților de securitate națională din SUA 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.

([1]) Cu condiția ca decizia Comisiei privind caracterul adecvat al protecției oferite de Cadrul UE-SUA privind confidențialitatea datelor să se aplice Islandei, Liechtensteinului și Norvegiei, Cadrul UE-SUA privind confidențialitatea datelor va viza atât Uniunea Europeană, cât și aceste trei țări.

Pachetul integral aferent Cadrului UE-SUA privind confidențialitatea datelor va fi publicat pe site-ul web al departamentului destinat Cadrului privind confidențialitatea datelor, iar principiile și anexa I la principii vor intra în vigoare la data intrării în vigoare a deciziei Comisiei Europene privind caracterul adecvat al nivelului de protecție.

Puteți fi sigur că Statele Unite ale Americii iau aceste angajamente în serios. Așteptăm cu interes să colaborăm cu dumneavoastră pe parcursul punerii în aplicare a Cadrului UE-SUA privind confidențialitatea datelor și pe măsură ce ne angajăm împreună în următoarea fază a acestui proces.

Cu stimă,

Gina M. RAIMONDO

ANEXA III

UNITED STATES DEPARTMENT OF COMMERCE
International Trade Administration
Washington, D C 20230

12 decembrie 2022

Onorabilului Didier Reynders
Comisar pentru justiție
Comisia Europeană
Rue de la Loi/Wetstraat 200
1049 Bruxelles
Belgia

Stimate Domnule Comisar Reynders,

În numele Administrației pentru Comerțul Internațional („ITA”), am plăcerea de a descrie angajamentele asumate de Departamentul Comerțului („departamentul”) pentru a asigura protecția datelor cu caracter personal prin administrarea și supravegherea programului aferent Cadrului privind confidențialitatea datelor. Finalizarea Cadrului UE-SUA privind confidențialitatea datelor („ CCD UE-SUA”) este o realizare majoră pentru protecția vieții private și pentru întreprinderile de pe ambele maluri ale Atlanticului, deoarece va oferi încredere persoanelor din UE că datele lor vor fi protejate și că aceștia vor dispune de căi de atac pentru a răspunde preocupărilor legate de datele lor, totodată permițând în continuare realizarea de investiții de către mii de întreprinderi și implicarea lor în alt mod în comerțul transatlantic, în beneficiul economiilor și al cetățenilor noștri. CCD UE-SUA reflectă ani de muncă asiduă și de colaborare cu dumneavoastră și colegii dumneavoastră din Comisia Europeană („Comisia”). Așteptăm cu interes să continuăm activitatea desfășurată în colaborare cu Comisia pentru a ne asigura că acest efort de colaborare funcționează în mod eficace.

CCD UE-SUA va aduce 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 persoanelor din UE transferate către Statele Unite ale Americii. Cadrul impune organizațiilor din SUA care participă la acesta să elaboreze o politică de confidențialitate conformă, să se angajeze public să respecte „ principiile Cadrului UE-SUA privind confidențialitatea datelor”, inclusiv principiile suplimentare (denumite în mod colectiv „principiile”) și anexa I la principii (și anume o anexă care prevede condițiile în care organizațiile care participă la CCD UE-SUA sunt obligate să supună arbitrajului anumite cereri reziduale în ceea ce privește datele cu caracter personal reglementate de principii), astfel încât angajamentul să devină executoriu în temeiul legislației SUA ([1]), să recertifice anual respectarea principiilor adresându-se departamentului, să ofere mecanisme independente gratuite de soluționare a litigiilor persoanelor din UE și să se supună competențelor de investigare și de asigurare a respectării legii a unui organism statutar al SUA menționat în principii [de exemplu, Comisia Federală pentru Comerț („FTC”) și Departamentul Transporturilor („DoT”)] sau a unui organism statutar din SUA enumerat într-o viitoare anexă la principii. Decizia unei organizații de a se autocertifica este voluntară, însă, odată ce o organizație s-a angajat public să respecte CCD UE-SUA, angajamentul său este executoriu în temeiul legislației SUA de către FTC, DoT sau un alt organism statutar din SUA, în funcție de organismul care are jurisdicție asupra organizației care participă la CCD UE-SUA. În al doilea rând, CCD UE-SUA va permite întreprinderilor din Statele Unite ale Americii, inclusiv filialelor întreprinderilor europene situate în Statele Unite ale Americii, să primească date cu caracter personal din Uniunea Europeană pentru a facilita fluxurile de date care sprijină comerțul transatlantic. Fluxurile de date dintre Statele Unite ale Americii și Uniunea Europeană sunt cele mai mari din lume și susțin relația economică SUA-UE în valoare de 7,1 mii de miliarde USD, care

([1]) Organizațiile care și-au autocertificat angajamentul de a respecta principiile Cadrului UE-SUA privind confidențialitatea datelor și doresc să beneficieze de participarea la CCD UE-SUA trebuie să respecte „ principiile Cadrului UE-SUA privind confidențialitatea datelor”. Acest angajament de a respecta „ principiile Cadrului UE-SUA privind confidențialitatea datelor” se va reflecta în politicile de confidențialitate ale acestor organizații care participă la CCD UE-SUA cât mai curând posibil și, în orice caz, nu mai târziu de trei luni de la data intrării în vigoare a „ principiilor Cadrului UE-SUA privind confidențialitatea datelor”. [*A se vedea* litera (e) din principiul suplimentar privind autocertificarea].

oferă 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. Fluxurile transatlantice de date permit organizațiilor din SUA să prelucreze datele necesare pentru a oferi bunuri, servicii și oportunități de ocupare a forței de muncă persoanelor din UE.

Departamentul se angajează să colaboreze îndeaproape și în mod productiv cu omologii noștri din UE pentru a gestiona și a supraveghea în mod eficace programul aferent Cadrului privind confidențialitatea datelor. Acest angajament se reflectă în dezvoltarea și perfecționarea continuă de către departament a unei varietăți de resurse pentru a sprijini organizațiile în procesul de autocertificare, în crearea unui site web care să furnizeze informații specifice părților interesate, în colaborarea cu Comisia și cu autoritățile europene pentru protecția datelor („APD") pentru a elabora orientări care să clarifice elemente importante ale CCD UE-SUA, în activități de informare menite să faciliteze o mai bună înțelegere a obligațiilor organizațiilor în materie de protecție a datelor, precum și în supravegherea și monitorizarea respectării de către organizații a cerințelor programului.

Cooperarea noastră permanentă cu omologii noștri valoroși din UE îi va permite departamentului să se asigure că CCD UE-SUA funcționează în mod eficace. Guvernul Statelor Unite ale Americii are o lungă tradiție de colaborare cu Comisia în ceea ce privește promovarea principiilor comune de protecție a datelor, eliminând diferențele dintre abordările noastre juridice și sprijinind totodată comerțul și creșterea economică în Uniunea Europeană și în Statele Unite ale Americii. Considerăm că CCD UE-SUA, un exemplu al acestei cooperări, îi va permite Comisiei să emită o nouă decizie privind caracterul adecvat al nivelului de protecție, care le va permite organizațiilor să utilizeze CCD UE-SUA pentru a transfera date cu caracter personal din Uniunea Europeană către Statele Unite ale Americii, în conformitate cu legislația UE.

Gestionarea și supravegherea programului aferent Cadrului privind confidențialitatea datelor de către Departamentul Comerțului

Departamentul se angajează ferm să asigure gestionarea și supravegherea eficace a programului aferent Cadrului privind confidențialitatea datelor și va depune eforturile necesare și va aloca resurse adecvate pentru a garanta acest rezultat. Departamentul va menține și va pune la dispoziția publicului o listă oficială a organizațiilor din SUA care au prezentat departamentului autocertificarea și și-au declarat angajamentul de a adera la principii („lista Cadrului privind confidențialitatea datelor"), pe care o va actualiza pe baza cererilor anuale de recertificare prezentate de organizațiile care participă la CCD UE-SUA și prin eliminarea organizațiilor atunci când acestea se retrag în mod voluntar sau nu finalizează recertificarea anuală în conformitate cu procedurile departamentului sau se constată că acestea încalcă în mod sistematic principiile. De asemenea, departamentul va menține și va pune la dispoziția publicului un registru oficial al organizațiilor din SUA care au fost eliminate de pe lista Cadrului privind confidențialitatea datelor și va identifica motivul eliminării fiecăreia dintre acestea. Registrul și lista oficiale menționate mai sus vor rămâne la dispoziția publicului pe site-ul web al departamentului destinat Cadrului privind confidențialitatea datelor. Site-ul web destinat Cadrului privind confidențialitatea datelor va include o explicație plasată în mod vizibil care va indica faptul că orice organizație eliminată din lista Cadrului privind confidențialitatea datelor trebuie să înceteze să mai declare că participă sau respectă CCD UE-SUA și că poate primi informații cu caracter personal în temeiul CCD UE-SUA. Cu toate acestea, o astfel de organizație trebuie să continue să aplice principiile informațiilor cu caracter personal pe care le-a primit în timpul participării sale la CCD UE-SUA atât timp aceasta păstrează informațiile respective. În scopul promovării angajamentului său amplu și continuu față de gestionarea și supravegherea eficace a programului aferent Cadrului privind confidențialitatea datelor, departamentul se angajează în mod specific să întreprindă acțiunile menționate în cele de mai jos:

Verificarea cerințelor de autocertificare

— Înainte de finalizarea autocertificării inițiale sau a recertificării anuale a unei organizații (denumite în mod colectiv „autocertificarea") și de plasarea sau menținerea unei organizații pe lista Cadrului privind confidențialitatea datelor, departamentul va verifica dacă organizația a îndeplinit cel puțin cerințele relevante prevăzute în principiul suplimentar privind autocertificarea în ceea ce privește informațiile pe care o organizație trebuie să le furnizeze în cererea sa de autocertificare înaintată departamentului și a furnizat, la momentul oportun, o politică de confidențialitate relevantă care informează persoanele cu privire la toate cele 13 elemente enumerate în principiul notificării. Departamentul va verifica dacă organizația:

— a precizat organizația care depune autocertificarea, precum și orice entități din SUA sau filiale din SUA ale acesteia care aderă, de asemenea, la principiile pe care organizația dorește să le acopere prin autocertificarea sa;

— a furnizat datele de contact necesare ale organizației [de exemplu, datele de contact ale persoanei (persoanelor) și/sau ale biroului (birourilor) specifice din cadrul organizației care se autocertifică responsabile pentru gestionarea plângerilor, a cererilor de acces și a oricăror alte aspecte care intervin în temeiul CCD UE-SUA];

— a descris scopul (scopurile) în care organizația ar urma să colecteze și să utilizeze informațiile cu caracter personal primite din Uniunea Europeană;

— a indicat informațiile cu caracter personal care ar urma să fie primite din Uniunea Europeană în temeiul CCD UE-SUA și, prin urmare, ar urma să facă obiectul autocertificării sale;

— în cazul în care organizația dispune de un site web public, a furnizat adresa URL la care este disponibilă politica de confidențialitate relevantă pe site-ul respectiv sau, în cazul în care organizația nu dispune de un site web public, a furnizat departamentului o copie a politicii de confidențialitate relevante și a comunicat locul în care textul politicii de confidențialitate este disponibil pentru consultare de către persoanele afectate (și anume angajații afectați, dacă politica de confidențialitate relevantă este o politică de confidențialitate privind resursele umane, sau publicul, dacă politica de confidențialitate relevantă nu este o politică de confidențialitate privind resursele umane);

— a inclus în politica sa de confidențialitate relevantă la momentul oportun (și anume inițial numai într-un proiect de politică de confidențialitate furnizat împreună cu cererea în cazul în care cererea vizează o autocertificare inițială și, în caz contrar, într-o politică de confidențialitate finală și, după caz, publicată) o declarație că aderă la principii și un hyperlink către site-ul web destinat Cadrului privind confidențialitatea datelor al departamentului sau adresa URL a acestuia (de exemplu, pagina principală sau pagina web a listei Cadrului privind confidențialitatea datelor);

— a inclus în politica sa de confidențialitate relevantă, la momentul oportun, toate celelalte 12 elemente enumerate în principiul notificării (de exemplu, posibilitatea, în anumite condiții, ca persoana din UE afectată să recurgă la o procedură de arbitraj obligatoriu, cerința de a divulga informații cu caracter personal ca răspuns la solicitări legale formulate de către autorități publice, inclusiv pentru respectarea cerințelor privind securitatea națională sau aplicarea legii și răspunderea sa în cazul transferurilor ulterioare către părți terțe);

— a precizat organismul statutar care are competența de a examina plângerile înaintate împotriva organizației referitoare la posibile practici neloiale sau frauduloase și încălcări ale legilor sau reglementărilor privind protecția vieții private (și care este menționat în principii sau într-o viitoare anexă la principii);

— a precizat orice program de protecție a vieții private la care participă organizația;

— a precizat dacă metoda relevantă (și anume procedurile de urmărire pe care trebuie să le asigure) pentru verificarea conformității sale cu principiile este „autoevaluarea” (și anume verificarea internă) sau „evaluarea externă a conformității” (și anume verificarea de către o parte terță) și, dacă a precizat că metoda relevantă este evaluarea externă a conformității, a precizat, de asemenea, partea terță care a realizat evaluarea respectivă;

— a precizat mecanismul independent de recurs corespunzător disponibil pentru soluționarea plângerilor depuse în temeiul principiilor și pentru a oferi o cale de atac adecvată și gratuită persoanei afectate.

— În cazul în care organizația a selectat un mecanism independent de recurs pus la dispoziție de un organism de soluționare alternativă a litigiilor din sectorul privat, aceasta a inclus în politica sa de confidențialitate relevantă un hyperlink către site-ul web relevant sau adresa URL a acestuia sau formularul de înaintare a plângerilor aferent mecanismului disponibil pentru investigarea plângerilor nesoluționate înaintate în temeiul principiilor.

— În cazul în care organizația fie este obligată (și anume în legătură cu datele privind resursele umane transferate din Uniunea Europeană în contextul unui raport de muncă), fie a ales să coopereze cu APD corespunzătoare în cadrul investigării și soluționării plângerilor înaintate în temeiul principiilor, aceasta și-a declarat angajamentul de a coopera cu APD și de a se conforma recomandărilor acestora de a întreprinde acțiuni specifice în vederea respectării principiilor.

— Departamentul va verifica, de asemenea, dacă respectiva cerere de autocertificare a organizației este în concordanță cu politica sa (politicile) (sale) de confidențialitate relevantă (relevante). În cazul în care o organizație de autocertificare dorește să includă oricare dintre entitățile sale din SUA sau filialele sale din SUA care au politici de confidențialitate relevante separate, departamentul va revizui, de asemenea, politicile de confidențialitate relevante ale acestor entități sau filiale vizate pentru a se asigura că acestea includ toate elementele necesare prevăzute în principiul notificării.

— Departamentul va colabora cu organismele statutare (de exemplu, FTC și DoT) pentru a verifica dacă organizațiile intră sub jurisdicția organismului statutar relevant identificat în cererile lor de autocertificare, în cazul în care departamentul are motive să se îndoiască de acest lucru.

— Departamentul va colabora cu organisme de soluționare alternativă a litigiilor din sectorul privat pentru a verifica dacă organizațiile sunt înregistrate în mod activ în ceea ce privește mecanismul independent de recurs identificat în cererile lor de autocertificare și pentru a verifica dacă organizațiile sunt înregistrate în mod activ pentru evaluarea externă a conformității identificată în documentele lor de autocertificare, în cazul în care organismele respective pot oferi ambele tipuri de servicii.

— Departamentul va colabora cu partea terță selectată de departament pentru a servi drept custode al fondurilor colectate prin intermediul taxei pentru comitetul APD (și anume taxa anuală menită să acopere costurile de funcționare ale comitetului APD) pentru a verifica dacă organizațiile au plătit taxa respectivă pentru anul relevant, în cazul în care organizațiile au identificat APD ca fiind mecanismul independent de recurs relevant.

— Departamentul va colabora cu partea terță selectată de departament pentru desfășurarea procedurilor de arbitraj în temeiul anexei I la principii și gestionarea fondului de arbitraj menționat în aceasta pentru a verifica dacă organizațiile au contribuit la fondul de arbitraj respectiv.

— În cazul în care departamentul identifică orice probleme în cursul examinării cererilor de autocertificare ale organizațiilor, acesta le va informa că trebuie să soluționeze toate aceste probleme în intervalul de timp adecvat desemnat de departament ([2]). Departamentul le va informa, de asemenea, cu privire la faptul că lipsa unui răspuns în termenele stabilite de departament sau orice altă omisiune de a-și finaliza autocertificarea în conformitate cu procedurile departamentului va conduce la concluzia că s-a renunțat la cererile de autocertificare respective, precum și cu privire la faptul că orice declarație falsă cu privire la participarea unei organizații la CCD UE-SUA sau la respectarea acestuia poate face obiectul unei măsuri de asigurare a respectării legii luate de FTC, de DoT sau de alt organism guvernamental relevant. Departamentul va informa organizațiile prin intermediul modalităților de contact pe care organizațiile le-au furnizat departamentului.

Facilitarea cooperării cu organismele de soluționare alternativă a litigiilor care oferă servicii legate de principii

— Departamentul va colabora cu organisme de soluționare alternativă a litigiilor din sectorul privat care oferă mecanisme independente de recurs și sunt disponibile pentru a investiga plângerile nesoluționate înaintate în temeiul principiilor pentru a verifica dacă acestea îndeplinesc cel puțin cerințele prevăzute în principiul suplimentar privind soluționarea litigiilor și punerea în aplicare a deciziilor. Departamentul va verifica dacă acestea:

  — includ pe site-urile lor web publice informații cu privire la principii și serviciile pe care acestea le furnizează în temeiul CCD UE-SUA, care trebuie să includă: (1) informații despre sau un hyperlink către cerințele principiilor referitoare la mecanismele independente de recurs, (2) un hyperlink către site-ul web al departamentului destinat Cadrului privind confidențialitatea datelor, (3) o explicație privind caracterul gratuit al serviciilor de soluționare a litigiilor în temeiul CCD UE-SUA, (4) o descriere a modului în care se poate înainta o plângere legată de principii, (5) termenul în care sunt prelucrate plângerile legate principii și (6) o descriere a gamei de soluții posibile. Departamentul va informa organismele respective în timp util cu privire la modificările semnificative în ceea ce privește supravegherea și gestionarea de către departament a programului aferent Cadrului privind confidențialitatea datelor, în cazul în care astfel de modificări sunt iminente sau au fost deja efectuate și sunt relevante pentru rolul pe care îl au organismele respective în temeiul CCD UE-SUA;

([2]) De exemplu, în ceea ce privește recertificarea, se așteaptă ca organizațiile să abordeze toate aceste aspecte în termen de 45 de zile, sub rezerva stabilirii de către departament a unui interval de timp diferit și corespunzător.

— publică un raport anual care să furnizeze statistici agregate privind serviciile lor de soluționare a litigiilor, care trebuie să includă: (1) numărul total de plângeri legate de principii primite în cursul anului de raportare, (2) tipurile de plângeri primite, (3) măsurile cu privire la calitatea procesului de soluționare a litigiilor, cum ar fi perioada de timp necesară pentru soluționarea plângerilor și (4) rezultatele plângerilor primite, în special numărul și tipul de măsuri reparatorii sau sancțiuni impuse. Departamentul va furniza organismelor respective orientări specifice și complementare cu privire la informațiile pe care ar trebui să le furnizeze în rapoartele anuale care detaliază cerințele respective (de exemplu, enumerarea criteriilor specifice pe care o plângere trebuie să le îndeplinească pentru a fi considerată o plângere legată de principii în scopul raportului anual), precum și identificarea altor tipuri de informații pe care ar trebui să le furnizeze (de exemplu, dacă organismul furnizează, de asemenea, un serviciu de verificare legat de principii, o descriere a modului în care organismul evită orice conflict de interese real sau potențial în situațiile în care furnizează unei organizații atât servicii de verificare, cât și servicii de soluționare a litigiilor). Orientările suplimentare furnizate de departament vor specifica, de asemenea, data până la care rapoartele anuale ale organismelor ar trebui să fie publicate pentru perioada de raportare relevantă.

Urmărirea organizațiilor care doresc să fie eliminate sau au fost eliminate de pe lista Cadrului privind confidențialitatea datelor

— Dacă o organizație dorește să se retragă din CCD UE-SUA, departamentul îi va solicita organizației respective să elimine din orice politică de confidențialitate relevantă orice trimiteri la CCD UE-SUA care implică faptul că organizația continuă să participe la CCD UE-SUA și că poate primi date cu caracter personal în temeiul CCD UE-SUA (a se vedea descrierea angajamentului departamentului de identificare a declarațiilor false de participare). De asemenea, departamentul îi va solicita organizației să completeze și să transmită departamentului un chestionar corespunzător pentru a verifica:

  — dorința acesteia de a se retrage;

  — care sunt acțiunile, din cele menționate mai jos, pe care le va întreprinde în legătură cu datele cu caracter personal primite în temeiul CCD UE-SUA în timpul participării sale la CCD UE-SUA, respectiv: (a) va păstra aceste date, va continua să aplice principiile în cazul acestor date și își va declara anual departamentului angajamentul de a aplica principiile în cazul acestor date, (b) va păstra aceste date și va asigura o protecție „adecvată” a acestor date prin alte mijloace autorizate sau (c) va returna sau va șterge toate aceste date până la o dată specificată și

  — care este punctul de contact permanent din cadrul organizației desemnat pentru orice întrebări legate de principii.

— În cazul în care o organizație a ales acțiunile menționate la litera (a) de mai sus, departamentul va solicita, de asemenea, ca aceasta să completeze și să transmită departamentului în fiecare an după retragere (și anume până la prima aniversare a retragerii sale, precum și până la fiecare aniversare ulterioară, cu excepția situației în care și până când organizația fie asigură o protecție „adecvată” a acestor date prin alte mijloace autorizate sau returnează sau șterge toate aceste date și informează departamentul în acest sens) un chestionar corespunzător pentru a stabili care sunt acțiunile pe care le-a întreprins în legătură cu datele cu caracter personal respective, care sunt acțiunile pe care le va întreprinde în legătură cu oricare dintre datele cu caracter personal pe care continuă să le păstreze și care este punctul de contact permanent din cadrul organizației desemnat pentru orice întrebări legate de principii.

— În cazul în care o organizație a permis expirarea autocertificării sale (și anume nici nu a finalizat recertificarea anuală a adeziunii sale la principii și nici nu a fost eliminată de pe lista Cadrului privind confidențialitatea datelor din alte motive, cum ar fi retragerea), departamentul o va îndruma să completeze și să transmită departamentului un chestionar corespunzător pentru a verifica dacă dorește să se retragă sau să se recertifice:

  — și, dacă dorește să se retragă, pentru a verifica în continuare care sunt acțiunile pe care le va întreprinde în legătură cu datele cu caracter personal primite în temeiul CCD UE-SUA în timpul participării sale la CCD UE-SUA (a se vedea descrierea anterioară a aspectelor pe care trebuie să le confirme o organizație dacă dorește să se retragă);

  — și, dacă dorește să se recertifice, pentru a verifica în continuare dacă, în timpul perioadei în care certificarea era expirată, aceasta a aplicat principiile în cazul datelor cu caracter personal primite în temeiul CCD UE-SUA și pentru a clarifica măsurile pe care aceasta le va lua pentru a aborda problemele nesoluționate care au determinat întârzierea recertificării.

— În cazul în care o organizație este eliminată de pe lista Cadrului privind confidențialitatea datelor din oricare dintre următoarele motive: (a) ca urmare a retragerii din CCD UE-SUA, (b) ca urmare a nefinalizării recertificării anuale a adeziunii sale la principii (și anume fie a început, dar nu a finalizat procesul de recertificare anuală în timp util, fie nici măcar nu a demarat procesul de recertificare anuală) sau (c) ca urmare a unei „încălcări sistematice", departamentul va trimite o notificare persoanei (persoanelor) de contact identificate în cererea de autocertificare a organizației, specificând motivul eliminării și explicând că aceasta trebuie să înceteze să mai facă afirmații explicite sau implicite că participă la sau respectă CCD UE-SUA și că poate primi date cu caracter personal în temeiul CCD UE-SUA. Notificarea, care poate include, de asemenea, un alt conținut adaptat motivului eliminării, va indica faptul că organizațiile care dau declarații false cu privire la participarea la sau respectarea CCD UE-SUA, inclusiv în cazul în care declară că participă la CCD UE-SUA după ce au fost eliminate de pe lista Cadrului privind confidențialitatea datelor, pot face obiectul unor măsuri de asigurare a respectării legii luate de către FTC, DoT sau un alt organism guvernamental relevant.

Identificarea și abordarea declarațiilor false de participare

— în permanență, atunci când o organizație: (a) renunță la participarea sa la CCD UE-SUA, (b) nu finalizează recertificarea anuală a adeziunii sale la principii (și anume fie a început, dar nu a finalizat procesul de recertificare anuală în timp util, fie nici măcar nu a demarat procesul de recertificare anuală) sau (c) este eliminată de pe lista organizațiilor care participă la CCD UE-SUA în principal ca urmare a unei „încălcări sistematice" sau (d) nu finalizează autocertificarea inițială a adeziunii sale la principii (și anume a început, dar nu a finalizat procesul de autocertificare inițială în timp util), departamentul va întreprinde acțiuni *ex officio* pentru a se asigura că nicio politică de confidențialitate publicată a organizației nu include trimiteri la CCD UE-SUA care implică faptul că organizația participă la CCD UE-SUA și că poate primi date cu caracter personal în temeiul CCD UE-SUA. În cazul în care departamentul constată existența unor astfel de trimiteri, acesta va informa organizația că, după caz, va sesiza agenția relevantă pentru eventuale măsuri de asigurare a respectării legii în cazul în care organizația continuă să facă declarații false privind participarea la CCD UE-SUA. Departamentul va informa organizația respectivă prin intermediul modalităților de contact pe care organizația le-a furnizat departamentului sau, după caz, prin intermediul altor mijloace corespunzătoare. În cazul în care organizația nu elimină trimiterile respective și nici nu își autocertifică respectarea principiilor în temeiul CCD UE-SUA în conformitate cu procedurile departamentului, acesta va sesiza *ex officio* FTC, DoT sau o altă agenție corespunzătoare de aplicare a legii sau va lua alte măsuri adecvate pentru a asigura utilizarea corespunzătoare a mărcii de certificare CCD UE-SUA;

— departamentul va depune alte eforturi pentru a identifica declarațiile false privind participarea la CCD UE-SUA și utilizarea necorespunzătoare a mărcii de certificare CCD UE-SUA, inclusiv de către organizații care, spre deosebire de organizațiile descrise mai sus, nici măcar nu au început vreodată procesul de autocertificare (de exemplu efectuarea de căutări corespunzătoare pe internet pentru a identifica trimiterile la CCD UE-SUA în politicile de confidențialitate ale organizațiilor). În situația în care, în urma acestor eforturi, departamentul identifică declarații false privind participarea la CCD UE-SUA și utilizarea necorespunzătoare a mărcii de certificare, departamentul va informa organizația că, după caz, departamentul va sesiza agenția relevantă pentru eventuale măsuri de asigurare a respectării legii în cazul în care organizația continuă să facă declarații false privind participarea la CCD UE-SUA. Departamentul va informa organizația respectivă prin intermediul modalităților de contact pe care organizația le-a furnizat departamentului, dacă există, sau, după caz, prin intermediul altor mijloace corespunzătoare. În cazul în care organizația nu elimină trimiterile respective și nici nu își autocertifică respectarea principiilor în temeiul CCD UE-SUA în conformitate cu procedurile departamentului, departamentul va sesiza *ex officio* FTC, DoT sau o altă agenție corespunzătoare de aplicare a legii sau va lua alte măsuri adecvate pentru a asigura utilizarea corespunzătoare a mărcii de certificare CCD UE-SUA;

— departamentul va examina și va soluționa cu celeritate plângerile specifice neabuzive cu privire la declarațiile false de participare la CCD UE-SUA pe care le primește (de exemplu, plângerile primite de la APD, mecanismele independente de recurs furnizate de organismele de soluționare alternativă a litigiilor din sectorul privat, persoanele vizate, întreprinderile din UE și SUA și alte tipuri de părți terțe) și

— departamentul poate lua alte măsuri de remediere adecvate. Orice declarație falsă adresată departamentului poate fi sancționată în temeiul Legii privind declarațiile false (titlul 18 articolul 1001 din U.S.C).

Efectuarea de evaluări periodice *ex officio* ale conformității și de evaluări ale programului aferent Cadrului privind confidențialitatea datelor

— în permanență, departamentul va depune eforturi pentru a monitoriza respectarea efectivă a cadrului de către organizațiile CCD UE-SUA pentru a identifica problemele care ar putea justifica acțiuni subsecvente. În special, departamentul va efectua *ex officio* controale de rutină prin sondaj asupra unor organizații CCD UE-SUA selectate aleatoriu, precum și controale ad-hoc prin sondaj asupra unor anumite organizații CCD UE-SUA în situația în care sunt identificate eventuale deficiențe de conformitate (de exemplu, eventuale deficiențe de conformitate aduse în atenția departamentului de către părți terțe) pentru a verifica: (a) dacă punctul (punctele) de contact responsabil(e) cu gestionarea plângerilor, a cererilor de acces și a altor aspecte care intervin în temeiul CCD UE-SUA sunt disponibile, (b) după caz, dacă politica de confidențialitate publică a organizației este ușor accesibilă consultării de către public, atât pe site-ul web public al organizației, cât și prin intermediul unui hyperlink care conduce la lista Cadrului privind confidențialitatea datelor, (c) dacă politica de confidențialitate a organizației continuă să respecte cerințele de autocertificare descrise în principii și (d) dacă mecanismul independent de recurs identificat de organizație este disponibil pentru soluționarea plângerilor depuse în temeiul CCD UE-SUA. De asemenea, departamentul va monitoriza în mod activ știrile pentru a identifica relatări care oferă dovezi credibile de neconformitate cu privire la organizațiile CCD UE-SUA.

— În cadrul procedurii de evaluare a conformității, departamentul va solicita unei organizații CCD UE-SUA să completeze și să transmită departamentului un chestionar detaliat atunci când: (a) departamentul a primit orice 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 CCD UE-SUA sau (c) există dovezi credibile că o organizație nu își respectă angajamentele asumate în temeiul CCD UE-SUA. În cazul în care departamentul a transmis un astfel de chestionar detaliat unei organizații, iar organizația nu răspunde în mod satisfăcător la chestionarul respectiv, departamentul va informa organizația că, după caz, va sesiza agenția relevantă pentru eventuale măsuri de asigurare a respectării legii în cazul în care departamentul nu primește în timp util un răspuns satisfăcător de la organizație. Departamentul va informa organizația respectivă prin intermediul modalităților de contact pe care organizația le-a furnizat departamentului sau, după caz, prin intermediul altor mijloace corespunzătoare. În cazul în care organizația nu oferă în timp util un răspuns satisfăcător, acesta va sesiza *ex officio* FTC, DoT sau o altă agenție competentă de aplicare a legii sau va lua alte măsuri adecvate în vederea asigurării conformității. Departamentul se va consulta, după caz, cu autoritățile competente pentru protecția datelor cu privire la astfel de evaluări ale conformității și

— departamentul va evalua periodic gestionarea și supravegherea programului aferent Cadrului privind confidențialitatea datelor, pentru a se asigura că eforturile sale de monitorizare, inclusiv orice astfel de eforturi întreprinse prin utilizarea unor instrumente de căutare (de exemplu, pentru a verifica dacă există linkuri întrerupte către politicile de confidențialitate ale organizațiilor CCD UE-SUA), sunt adecvate pentru abordarea problemelor existente și a oricăror probleme noi, pe măsură ce apar.

Adaptarea site-ului web destinat Cadrului privind confidențialitatea datelor la publicul vizat

Departamentul va adapta site-ul web destinat Cadrului privind confidențialitatea datelor pentru a viza următoarele categorii de public: persoane din UE, întreprinderi din UE, întreprinderi din SUA și APD. Includerea materialelor care vizează direct persoanele din UE și întreprinderile din UE va facilita transparența în mai multe moduri. În ceea ce privește persoanele din UE, site-ul web va explica în mod clar: (1) drepturile pe care CCD UE-SUA le oferă persoanelor din UE, (2) mecanismele de recurs disponibile persoanelor din 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 identifica informații referitoare la autocertificarea organizației în ceea ce privește CCD UE-SUA. În ceea ce privește întreprinderile din UE, acesta va facilita verificarea: (1) participării unei organizații la CCD UE-SUA, (2) a tipului de informații care fac obiectul autocertificării unei organizații în ceea ce privește CCD UE-SUA, (3) a politicii de confidențialitate care se aplică informațiilor care intră sub incidența acesteia și (4) a metodei utilizate de organizație pentru verificarea adeziunii acesteia la principii. În ceea ce privește întreprinderile din UE, acesta va explica în mod clar: (1) beneficiile participării la CCD UE-SUA, (2) modalitatea de aderare la CCD UE-SUA, precum și modalitatea de recertificare și de retragere din CCD UE-SUA și (3) modul de gestionare și punere în aplicare de către Statele Unite ale Americii a CCD UE-SUA. Includerea de materiale care vizează în mod direct APD (de exemplu, informații cu privire la punctul de contact specific al departamentului destinat APD și un hyperlink către conținutul legat de principii de pe site-ul web FTC) va facilita atât cooperarea, cât și transparența. De asemenea, departamentul va colabora ad-hoc cu Comisia și Comitetul european pentru protecția datelor („CEPD”) pentru a elabora materiale suplimentare punctuale (de exemplu, răspunsuri la întrebări frecvente) care să fie utilizate pe site-ul web destinat Cadrului privind confidențialitatea datelor, în cazul în care astfel de informații ar facilita gestionarea și supravegherea eficientă a programului aferent Cadrului privind confidențialitatea datelor.

Facilitarea cooperării cu APD

Pentru a spori posibilitățile de cooperare cu APD, departamentul va stabili un punct de contact specific în cadrul acestuia care să acționeze ca punct de legătură cu APD. În situațiile în care o APD consideră că o organizație CCD UE-SUA nu respectă principiile, inclusiv în urma unei plângeri din partea unei persoane din UE, APD va putea lua legătura cu punctul de contact specific din cadrul departamentului în vederea reexaminării acesteia. Departamentul va depune toate eforturile pentru a facilita soluționarea plângerii împreună cu organizația CCD UE-SUA. În termen de 90 de zile de la primirea plângerii, departamentul va furniza APD o actualizare. Punctul de contact specific va primi, de asemenea, sesizări cu privire la organizațiile care pretind în mod fals că participă la CCD UE-SUA. Punctul de contact specific va urmări toate sesizările de la APD primite de departament, iar departamentul va furniza în cadrul revizuirii comune descrise mai jos un raport în care se analizează în ansamblu plângerile pe care le primește în fiecare an. Punctul de contact specific va sprijini APD în activitatea acestora de identificare a informațiilor referitoare la autocertificarea sau participarea anterioară a unei anumite organizații la CCD UE-SUA și va răspunde solicitărilor de informații ale APD cu privire la punerea în aplicare a anumitor cerințe ale CCD UE-SUA. Departamentul va coopera, de asemenea, cu Comisia și cu CEPD cu privire la aspecte procedurale și administrative care vizează comitetul APD, inclusiv la stabilirea unor proceduri adecvate pentru distribuirea fondurilor colectate prin intermediul taxei comitetului APD. Potrivit înțelegerii noastre, Comisia va colabora cu departamentul pentru a facilita soluționarea oricăror probleme care ar putea apărea în legătură cu aceste proceduri. În plus, departamentul va oferi APD materiale privind CCD UE-SUA pentru a fi incluse pe propriile site-uri web în vederea sporirii transparenței pentru persoanele din UE și întreprinderile din UE. Creșterea gradului de conștientizare în ceea ce privește CCD UE-SUA și drepturile și responsabilitățile pe care le creează acesta ar trebui să faciliteze identificarea problemelor pe măsură ce acestea apar, astfel încât să poată fi abordate în mod adecvat.

Îndeplinirea angajamentelor asumate în temeiul anexei I la principii

Departamentul își va îndeplini angajamentele asumate în temeiul anexei I la principii, inclusiv menținerea unei liste de arbitri aleși împreună cu Comisia pe baza independenței, integrității și competențelor acestora și sprijinirea, după caz, a părții terțe selectate de departament pentru desfășurarea procedurilor de arbitraj în temeiul anexei I la principii și gestionarea fondului de arbitraj menționat în aceasta ([3]). Departamentul va colabora cu partea terță respectivă pentru a verifica, printre altele, dacă partea terță menține un site web pe care se regăsesc orientări privind procesul de arbitraj, inclusiv: (1) modul de inițiere a procedurilor și de depunere a documentelor, (2) lista arbitrilor menținută de departament și modul de selectare a arbitrilor din lista respectivă, (3) procedurile de arbitraj aplicabile și codul de conduită al arbitrilor adoptate de departament și de Comisie ([4]) și (4) colectarea și plata onorariilor arbitrilor. În plus, departamentul va coopera cu partea terță respectivă pentru a revizui periodic funcționarea fondului de arbitraj, inclusiv necesitatea de a ajusta valoarea contribuțiilor sau a plafoanelor (și anume a sumelor maxime) privind costurile procedurilor de arbitraj, ținând seama, printre altele, de numărul de arbitri, costurile și calendarul arbitrajelor și înțelegându-se că nu se va impune o sarcină financiară excesivă asupra organizațiilor CCD UE-SUA. Departamentul va informa Comisia cu privire la rezultatul acestor revizuiri realizate împreună cu partea terță și va transmite Comisiei o notificare prealabilă cu privire la orice ajustare a cuantumului contribuțiilor.

Realizarea de revizuiri comune ale funcționării CCD UE-SUA

Departamentul și alte agenții, după caz, vor organiza reuniuni periodice cu Comisia, cu APD interesate și cu reprezentanții corespunzători ai CEPD, în cadrul cărora departamentul va oferi informații actualizate cu privire la CCD UE-SUA. În cadrul reuniunilor, se va discuta cu privire la aspecte de actualitate legate de funcționarea, punerea în aplicare, supravegherea și asigurarea respectării programului aferent Cadrului privind confidențialitatea datelor. Reuniunile pot include, după caz, discuții pe teme conexe, cum ar fi alte mecanisme de transfer de date care beneficiază de garanțiile prevăzute de CCD UE-SUA.

([3]) Departamentul a selectat Centrul Internațional pentru Soluționarea Litigiilor (International Centre for Dispute Resolution) („ICDR”), divizia internațională a Asociației Americane de Arbitraj (American Arbitration Association) („AAA”), (denumite în mod colectiv „ICDR-AAA”), pentru desfășurarea procedurilor de arbitraj în conformitate cu anexa I la principii și pentru a gestiona fondul de arbitraj identificat în aceasta.

([4]) La 15 septembrie 2017, departamentul și Comisia au convenit cu privire la adoptarea unui set de norme de arbitraj care să reglementeze procedurile de arbitraj obligatoriu descrise în anexa I la principii, precum și a unui cod de conduită pentru arbitri care să fie în concordanță cu standardele etice general acceptate pentru arbitrii comerciali și cu anexa I la principii. Departamentul și Comisia au convenit să adapteze normele de arbitraj și codul de conduită pentru a reflecta actualizările în temeiul CCD UE-SUA, iar departamentul va colabora cu ICDR-AAA pentru a realiza aceste actualizări.

Actualizarea legislației

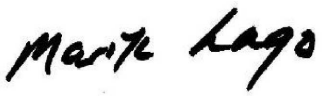
Departamentul va depune eforturi rezonabile pentru a informa Comisia cu privire la evoluții semnificative în legislația Statelor Unite ale Americii, în măsura în care acestea sunt relevante pentru CCD UE-SUA, în ceea ce privește protecția confidențialității datelor cu caracter personal și limitările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

Accesul autorităților SUA la datele cu caracter personal

Statele Unite ale Americii au emis Ordinul executiv nr. 14086 – „Enhancing Safeguards for US Signals Intelligence Activities" (Consolidarea garanțiilor pentru activitățile de colectare de informații de tip SIGINT desfășurate de Statele Unite ale Americii) și titlul 28 partea 201 din CFR de modificare a regulamentelor Departamentului de Justiție pentru instituirea „Curții de Reexaminare a Protecției Datelor", care oferă o protecție solidă a datelor cu caracter personal în ceea ce privește accesul autorităților la date în scopuri legate de securitatea națională. Protecția oferită include: consolidarea garanțiilor privind protecția vieții private și a libertăților civile care asigură faptul că activitățile de colectare de informații de tip SIGINT sunt necesare și proporționale din perspectiva urmăririi unor obiective definite de securitate națională, instituirea unui nou mecanism independent de recurs cu autoritate obligatorie și consolidarea supravegherii existente riguroase și pe mai multe niveluri a activităților de colectare de informații de tip SIGINT desfășurate de SUA. Prin intermediul acestor măsuri de protecție, persoanele din UE pot exercita căi de atac prin intermediul unui nou mecanism de recurs pe mai multe niveluri, care include o instanță DPRC independentă, compusă din persoane care nu fac parte din personalul autorităților SUA, cu competență deplină de a se pronunța asupra plângerilor și de a acorda în mod direct măsuri reparatorii, după cum este necesar. Departamentul va păstra o evidență a persoanelor din UE care depun plângeri eligibile în temeiul Ordinului executiv nr. 14086 și al titlului 28 partea 201 din CFR. La cinci ani de la data prezentei scrisori și, ulterior, o dată la cinci ani, departamentul va contacta agențiile relevante pentru a stabili dacă informațiile referitoare la examinarea plângerilor eligibile sau la reexaminarea oricăror cereri de reexaminare depuse la DPRC au fost declasificate. În cazul în care aceste informații au fost declasificate, departamentul va colabora cu APD relevantă pentru a informa persoana din UE în acest sens. Aceste îmbunătățiri confirmă faptul că datele cu caracter personal din UE transferate către Statele Unite ale Americii vor fi tratate în conformitate cu cerințele legale ale UE în ceea ce privește accesul autorităților la date.

Pe baza principiilor, a Ordinului executiv nr. 14086, a titlului 28 partea 201 din CFR și a scrisorilor și materialelor însoțitoare, inclusiv a angajamentelor departamentului privind gestionarea și supravegherea programului aferent Cadrului privind confidențialitatea datelor, ne așteptăm ca decizia Comisiei să stabilească că acest Cadru UE-SUA privind confidențialitatea datelor oferă o protecție adecvată în sensul legislației UE și ca transferurile de date din Uniunea Europeană să continue să se efectueze către organizațiile care participă la CCD UE-SUA. De asemenea, ne așteptăm ca transferurile către organizațiile din SUA efectuate pe baza clauzelor contractuale standard ale UE sau a regulilor corporatiste obligatorii ale UE să fie facilitate și mai mult de termenii acestor acorduri.

Cu stimă,



Marisa LAGO

ANEXA IV

STATELE UNITE ALE AMERICII
Comisia Federală pentru Comerț
Washington, D.C. 20580

Biroul președintelui

9 iunie 2023

Didier Reynders
Comisar pentru justiție
Comisia Europeană
Rue de la Loi/Wetstraat 200
1049 Bruxelles
Belgia

Stimate Domnule Comisar Reynders,

Comisia Federală pentru Comerț a Statelor Unite ale Americii („FTC") apreciază oportunitatea de a aborda rolul său de asigurare a respectării principiilor Cadrului UE-SUA privind confidențialitatea datelor („ CCD UE-SUA"). FTC s-a angajat de multă vreme să protejeze consumatorii și viața privată la nivel transfrontalier și ne angajăm să punem în aplicare aspectele legate de sectorul comercial ale acestui cadru. FTC a îndeplinit un astfel de rol începând cu anul 2000, în legătură cu Cadrul privind sfera de siguranță UE-SUA și, cel mai recent, din 2016, în legătură cu Cadrul privind Scutul de confidențialitate UE-SUA ([1]). La 16 iulie 2020, Curtea de Justiție a Uniunii Europene („CJUE") a declarat ca fiind nevalidă decizia Comisiei Europene privind caracterul adecvat al nivelului de protecție care stă la baza Cadrului privind Scutul de confidențialitate UE-SUA, pe temeiul altor aspecte decât principiile comerciale pe care le-a pus în aplicare FTC. Între timp, SUA și Comisia Europeană au negociat Cadrul UE-SUA privind confidențialitatea datelor pentru a ține seama de această hotărâre a CJUE.

Vă scriu pentru a confirma angajamentul FTC de a pune în aplicare cu fermitate principiile CCD UE-SUA. În special, ne afirmăm angajamentul în trei domenii principale: (1) gestionarea cu prioritate a sesizărilor și realizarea investigațiilor, (2) solicitarea și monitorizarea ordinelor și (3) cooperarea cu autoritățile UE pentru protecția datelor („APD") în vederea asigurării respectării legii.

I. **Introducere**

a. **Activitățile FTC în materie de politici și de asigurare a respectării legii în domeniul protecției vieții private**

FTC dispune de o competență amplă de asigurare a respectării legii în materie de drept civil pentru a promova protecția consumatorilor și concurența în domeniul comercial. În cadrul mandatului său de protecție a consumatorilor, FTC aplică o gamă largă de norme de protecție a vieții private și a securității consumatorilor și a datelor acestora. Legislația primară

([1]) Scrisoarea președintei Edith Ramirez către Věra Jourová, comisarul pentru justiție, consumatori și egalitate de gen al Comisiei Europene, în care se descrie punerea în aplicare de către Comisia Federală pentru Comerț a noului Cadru privind Scutul de confidențialitate UE-SUA (29 februarie 2016), *disponibilă la adresa* https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice-consumers-gender-equality-european. De asemenea, FTC s-a angajat anterior să pună în aplicare Programul privind sfera de siguranță UE-SUA. Scrisoarea președintelui FTC Robert Pitofsky către John Mogg, directorul DG Piața Internă a Comisiei Europene (14 iulie 2000), *disponibilă la adresa* https://www.federalregister.gov/documents/2000/07/24/00-18489/issuance-of-safe-harbor-principles-and-transmission-to-european-commission. Prezenta scrisoare înlocuiește angajamentele anterioare.

aplicată de FTC, Legea privind FTC, interzice actele sau practicile „neloiale" și „înșelătoare" în domeniul comerțului sau care afectează comerțul ([2]). FTC aplică, de asemenea, legi specifice care protejează informațiile referitoare la starea de sănătate, la credite și la alte aspecte financiare, precum și informațiile privind copii în mediul online și a publicat o serie de regulamente de punere în aplicare a fiecăruia dintre aceste legi ([3]).

De asemenea, FTC s-a implicat recent în numeroase inițiative de consolidare a activității noastre în domeniul protecției vieții private. În august 2022, FTC a anunțat că are în vedere norme împotriva supravegherii comerciale dăunătoare și securitatea laxă a datelor ([4]). Obiectivul proiectului este de a crea o evidență publică solidă pentru a fundamenta posibilitatea ca FTC să emită norme care să abordeze practicile de supraveghere comercială și de securitate a datelor, precum și modul în care ar trebui formulate aceste norme. Am salutat observațiile părților interesate din UE cu privire la această inițiativă și la alte inițiative.

Conferințele noastre „PrivacyCon" continuă să reunească cercetători de renume pentru a dezbate cele mai recente studii și tendințe în domeniul protecției vieții private a consumatorilor și securitatea datelor. De asemenea, am sporit capacitatea agenției noastre de a ține pasul cu evoluțiile tehnologice aflate în centrul unei mari părți a activității noastre în domeniul protecției vieții private, construind o echipă din ce în ce mai numeroasă de tehnicieni și cercetători interdisciplinari. De asemenea, după cum știți, am anunțat un dialog comun cu dumneavoastră și cu colegii dumneavoastră din cadrul Comisiei Europene, care include abordarea unor subiecte legate de protecția vieții private, cum ar fi interfețele înșelătoare și modelele de afaceri caracterizate prin colectarea generalizată de date ([5]). De asemenea, am publicat recent un raport către Congres, care avertizează cu privire la consecințele asociate utilizării inteligenței artificiale („IA") pentru a aborda problemele din mediul online identificate de Congres. Acest raport a ridicat semne de întrebare cu privire la inexactitatea, prejudecățile, discriminarea și denaturarea supravegherii comerciale ([6]).

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

CCD UE-SUA funcționează în contextul american mai amplu al protecției vieții private, care protejează, de asemenea, consumatorii din UE în mai multe moduri. Interdicția inclusă în Legea FTC privind actele sau practicile neloiale sau frauduloase nu se limitează la protecția consumatorilor din SUA de întreprinderile din SUA, întrucât aceasta include practicile care (1) cauzează sau pot cauza un prejudiciu previzibil în mod rezonabil în Statele Unite ale Americii sau (2) implică o serie de comportamente semnificative în Statele Unite ale Americii. De asemenea, FTC poate utiliza toate căile de atac disponibile pentru a proteja consumatorii de la nivel național atunci când protejează consumatorii străini ([7]).

De asemenea, FTC asigură aplicarea altor legi specifice ale căror măsuri de protecție se extind la consumatori care nu sunt cetățeni americani/rezidenți SUA, cum ar fi Legea privind respectarea vieții private a copiilor în mediul online („COPPA"). Printre altele, COPPA impune operatorilor de servicii online și site-uri web care vizează copiii sau de site-uri web care vizează publicul general și care colectează în cunoștință de cauză 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 web și serviciile

([2]) Titlul 15 articolul 45 litera (a) din U.S.C. FTC nu are competență în materie de asigurare a respectării dreptului penal sau cu privire la securitatea națională. De asemenea, FTC nu poate aplica majoritatea celorlalte măsuri aflate la dispoziția autorităților. În plus, există excepții de la competența FTC asupra activităților comerciale, respectiv în ceea ce privește activitățile bancare, companiile aeriene, activitățile de asigurare și activitățile transportatorilor comuni sau activitățile desfășurate de furnizorii de servicii de telecomunicații. De asemenea, FTC nu are competență în ceea ce privește cea mai mare parte a organizațiilor fără scop lucrativ, dar are competență în ceea ce privește organizațiile caritabile fictive sau alte organizații fără scop lucrativ care au, în realitate, scop lucrativ. De asemenea, FTC dispune de competență în ceea ce privește organizațiile fără scop lucrativ care funcționează în avantajul membrilor cu scop lucrativ, inclusiv prin furnizarea de beneficii economice pentru membrii respectivi. 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 cu autoritățile la nivel de stat și colaborăm îndeaproape cu acestea pentru a coordona investigații sau pentru a face sesizări, după caz.

([3]) *A se vedea* FTC, secțiunea privind protecția vieții private și securitatea, https://www.ftc.gov/business-guidance/privacy-security.

([4]) *A se vedea* comunicatul de presă al Comisiei Federale pentru Comerț privind explorarea de către FTC a unor norme împotriva practicilor de supraveghere comercială și de securitate laxă a datelor (11 august 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices.

([5]) *A se vedea* declarația de presă comună a lui Didier Reynders, comisar pentru justiție al Comisiei Europene și a Linei Khan, președinta Comisiei Federale pentru Comerț a Statelor Unite ale Americii (30 martie 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Joint%20FTC-EC%20Statement%20informal%20dialogue%20consumer%20protection%20issues.pdf.

([6]) *A se vedea* comunicatul de presă al Comisiei Federale pentru Comerț privind raportul FTC care avertizează asupra utilizării inteligenței artificiale pentru a contracara problemele din mediul online (16 iunie 2022), https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems.

([7]) Titlul 15 articolul 45 litera (a) punctul 4 partea B din U.S.C. În plus, „actele sau practicile neloiale sau înșelătoare" includ astfel de acte sau practici privind comerțul internațional care (i) cauzează sau pot cauza un prejudiciu previzibil în mod rezonabil în Statele Unite ale Americii sau (ii) implică comportamente semnificative în Statele Unite ale Americii. Titlul 15 articolul 45 litera (a) punctul 4 partea A din U.S.C.

care fac obiectul COPPA și care colectează informații cu caracter personal de la copii străini sunt obligați să respecte dispozițiile COPPA. Site-urile web și serviciile online cu sediul 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 din Statele Unite ale Americii. De asemenea, în plus față de legislația federală a SUA aplicată de FTC, alte legi specifice federale și la nivel de stat de protecție a consumatorilor și a vieții private, precum și împotriva încălcărilor securității datelor pot aduce beneficii suplimentare pentru consumatorii din UE.

c. **Activitatea FTC de asigurare a respectării legii**

FTC a introdus acțiuni atât în temeiul Cadrului privind sfera de siguranță UE-SUA, cât și în temeiul Scutului de confidențialitate UE-SUA și a continuat să asigure respectarea Scutului de confidențialitate UE-SUA chiar și după ce CJUE a declarat nevalidă decizia privind caracterul adecvat al nivelului de protecție care stă la baza Cadrului privind Scutul de confidențialitate UE-SUA ([8]). Mai multe dintre plângerile recente ale FTC au inclus capete de acuzare care au vizat pretinsa încălcare a dispozițiilor Scutului de confidențialitate, inclusiv în cadrul unor proceduri împotriva Twitter, ([9]) CafePress, ([10]) și Flo ([11]). În cadrul acțiunii împotriva Twitter, FTC a obținut 150 de milioane USD de la Twitter pentru încălcarea unui ordin FTC anterior prin practici care au afectat peste 140 de milioane de clienți, inclusiv încălcarea principiului 5 al Scutului de confidențialitate UE-SUA (integritatea datelor și limitarea scopului). În plus, ordinul agenției impune Twitter să permită utilizatorilor să utilizeze metode securizate de autentificare multifactorială care nu impun utilizatorilor să furnizeze numerele lor de telefon.

În cazul *CafePress*, FTC a susținut că societatea respectivă nu a garantat securitatea informațiilor sensibile ale consumatorilor, a mușamalizat o încălcare majoră a securității datelor și a încălcat principiile 2 (opțiunea), 4 (securitatea) și 6 (accesul) din Scutul de confidențialitate UE-SUA. Ordinul FTC impune societății să înlocuiască măsurile de autentificare necorespunzătoare cu autentificarea multifactorială, să limiteze în mod substanțial volumul de date pe care le colectează și le păstrează, să cripteze numerele de securitate socială și să dispună evaluarea de către o parte terță a programelor de securitate a informațiilor și să furnizeze FTC o copie care poate fi făcută publică.

În cazul *Flo*, FTC a susținut că aplicația de urmărire a fertilității a divulgat informații privind sănătatea utilizatorilor furnizorilor terți de analize de date, după ce s-a angajat să păstreze confidențialitatea acestor informații. FTC face referire în special la interacțiunile societății cu consumatorii din UE și la faptul că Flo a încălcat principiile 1 (notificarea), 2 (opțiunea), 3 (responsabilitatea pentru transferurile ulterioare) și 5 (integritatea datelor și limitarea scopului) din Scutul de confidențialitate UE-SUA. Printre altele, ordinul agenției impune societății Flo să informeze utilizatorii afectați cu privire la divulgarea informațiilor lor cu caracter personal și să solicite oricărei părți terțe care a primit informații privind sănătatea utilizatorilor să distrugă datele respective. Este important de menționat că ordinele FTC protejează toți consumatorii din întreaga lume care interacționează cu o întreprindere din SUA, și nu doar consumatorii care au depus plângeri.

Multe dintre cazurile anterioare care vizează asigurarea respectării Cadrului privind sfera de siguranță UE-SUA și a Scutului de confidențialitate UE-SUA au implicat organizații care au finalizat o autocertificare inițială prin intermediul Departamentului Comerțului, dar nu și-au menținut autocertificarea anuală, deși au continuat să se reprezinte ca participanți la acestea. Alte cazuri au implicat declarații false de participare din partea organizațiilor care nu au finalizat niciodată o autocertificare inițială prin intermediul Departamentului Comerțului. Pe viitor, ne așteptăm să ne concentrăm eforturile proactive de asigurare a respectării legii asupra tipurilor de încălcări de fond ale principiilor CCD UE-SUA în cazuri precum Twitter, CafePress și Flo. Între timp, Departamentul Comerțului va gestiona și va supraveghea procesul de autocertificare, va menține lista oficială a participanților la CCD UE-SUA și va aborda alte aspecte legate de cererile de participare la program ([12]). Este important de precizat că organizațiile care solicită participarea la CCD UE-SUA pot face obiectul unor acțiuni substanțiale de asigurare a respectării principiilor CCD UE-SUA în cazul în care nu se autocertifică sau nu mențin autocertificarea prin intermediul Departamentului Comerțului.

([8]) *A se vedea* apendicele A, care include o listă a cazurilor FTC care vizează sfera de siguranță și Scutul de confidențialitate.

([9]) *A se vedea* comunicatul de presă al Comisiei Federale pentru Comerț privind cazul în care FTC acuză Twitter de utilizarea înșelătoare a datelor de securitate a contului pentru a vinde publicitate direcționată (25 mai 2022), https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads.

([10]) *A se vedea* comunicatul de presă al Comisiei Federale pentru Comerț privind cazul în care FTC se îndreaptă împotriva CafePress pentru încercarea de mușamalizare a încălcării securității datelor (15 martie 2022), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover.

([11]) *A se vedea* comunicatul de presă al Comisiei Federale pentru Comerț privind cazul în care FTC finalizează ordinul pentru Flo Health, o aplicație de monitorizare a fertilității care a divulgat date sensibile cu caracter personal privind sănătatea cu Facebook, Google și alte părți (22 iunie 2021), https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google.

([12]) Scrisoarea Subsecretarului pentru comerț internațional Marisa Lago către onorabilul Didier Reynders, comisar pentru justiție, Comisia Europeană (12 decembrie 2022).

II. **Gestionarea cu prioritate a sesizărilor și realizarea investigațiilor**

Astfel cum am procedat în temeiul Cadrului privind sfera de siguranță UE-SUA și al Cadrului privind Scutul de confidențialitate UE-SUA, FTC se angajează să acorde prioritate sesizărilor referitoare la principiile CCD UE-SUA transmise de Departamentul Comerțului și statele membre ale UE. De asemenea, vom acorda prioritate examinării sesizărilor în ceea ce privește nerespectarea principiilor CCD UE-SUA transmise de organizații de autoreglementare în domeniul protecției vieții private și de alte organisme independente de soluționare a litigiilor.

Pentru a facilita sesizările în temeiul CCD UE-SUA de la statele membre ale UE, FTC a creat un proces de sesizare standard și a oferit orientări pentru statele membre cu privire la tipul de informații care ar sprijini cel mai mult FTC în investigația sa în legătură cu o sesizare. Ca parte a acestui efort, FTC a desemnat 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 investigație preliminară în legătură cu presupusa încălcare și să poată coopera cu FTC în cadrul unei investigații.

După primirea unei sesizări din partea Departamentului Comerțului, a unui stat membru al UE, a unui organism de autoreglementare sau a unui alt organism independent de soluționare a litigiilor, FTC poate lua o serie de măsuri pentru a soluționa aspectele invocate. De exemplu, se pot revizui politicile de confidențialitate ale organizației, se pot obține informații suplimentare direct de la organizație sau de la părți terțe, se poate asigura o monitorizare împreună cu entitatea de trimitere, se poate evalua dacă există mai multe încălcări sau un număr semnificativ de consumatori afectați, se poate determina dacă sesizarea implică aspecte ce țin de competența Departamentul Comerțului, se poate evalua dacă ar fi utile eforturi suplimentare pentru informarea participanților pe piață și, după caz, se poate iniția o procedură de asigurare a respectării legii.

În plus față de gestionarea cu prioritate a sesizărilor referitoare la principiile CCD UE-SUA transmise de Departamentul Comerțului, statele membre ale UE și organizațiile de autoreglementare în domeniul protecției vieții private sau de alte organisme independente de soluționare a litigiilor ([13]), FTC va continua să investigheze încălcări ale principiilor CCD UE-SUA din proprie inițiativă, după caz, prin utilizarea unei serii de instrumente. În cadrul programului FTC de investigare a aspectelor legate de protecția vieții private și de securitate care implică organizații comerciale, agenția a examinat în mod regulat dacă entitatea în cauză a emis declarații privind Scutul de confidențialitate UE-SUA. Dacă entitatea a emis astfel de declarații și investigația a scos la iveală încălcări clare ale principiilor Scutului de confidențialitate, FTC a inclus în acțiunile sale de asigurare a respectării legii acuzații de încălcări ale Scutului de confidențialitate UE-SUA. Vom continua această abordare proactivă și în prezent în ceea ce privește CCD UE-SUA.

III. **Solicitarea și monitorizarea ordinelor**

FTC își afirmă, de asemenea, angajamentul de a solicita și monitoriza ordinele de asigurare a respectării legii pentru a asigura respectarea principiilor CCD UE-SUA. Vom impune respectarea principiilor CCD UE-SUA prin diverse dispoziții reparatorii corespunzătoare în ordine viitoare ale FTC care vizează principiile CCD UE-SUA. Încălcările ordinelor administrative ale FTC pot conduce la sancțiuni civile de până la 50 120 USD pentru fiecare încălcare sau 50 120 USD pe zi pentru o încălcare persistentă ([14]), 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 vizate de un ordin trebuie să păstreze documentele care le demonstrează conformitatea timp de un anumit număr de ani. Ordinele trebuie, de asemenea, să fie transmise angajaților responsabili pentru asigurarea conformității cu acestea.

FTC monitorizează sistematic respectarea ordinelor care vizează principiile Scutului de confidențialitate UE-SUA, astfel cum procedează în cazul tuturor ordinelor sale, și întreprinde acțiuni de asigurare a respectării acestora în situațiile necesare ([15]). Este important de menționat că ordinele FTC vor continua să protejeze toți consumatorii din întreaga lume care interacționează cu o întreprindere din SUA, și nu doar consumatorii care au depus plângeri. În sfârșit, FTC va menține o listă online a societăților care fac obiectul ordinelor obținute în legătură cu asigurarea respectării principiilor CCD UE-SUA ([16]).

([13]) Deși FTC nu soluționează sau mediază plângeri ale consumatorilor individuali, FTC afirmă că va acorda prioritate sesizărilor legate de principiile CCD UE-SUA primite din partea APD din UE. De asemenea, FTC utilizează plângerile din baza de date Consumer 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 legii și pentru a identifica posibilele obiective de investigare. Persoanele din UE pot utiliza același sistem de plângeri de care dispun consumatorii din SUA pentru a depune o plângere la FTC, disponibil la adresa https://reportfraud.ftc.gov/. Cu toate acestea, pentru plângerile individuale în temeiul principiilor CCD UE-SUA, ar putea fi mai util pentru persoanele din UE să depună plângeri la APD a statului lor membru sau la organismul independent de soluționare a litigiilor.

([14]) Titlul 15 articolul 45 litera (m) din U.S.C., titlul 16 secțiunea 1.98 din CFR. Această sumă este ajustată periodic în funcție de inflație.

([15]) Anul trecut, FTC a votat pentru simplificarea procesului de investigare în cazul recidivelor. *A se vedea* comunicatul de presă al Comisiei Federale pentru Comerț privind autorizarea de către FTC a investigațiilor privind principalele priorități în materie de asigurare a respectării legii (1 iulie 2021), https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-authorizes-investigations-key-enforcement-priorities.

([16]) *Cf.* FTC, Scutul de confidențialitate, https://www.ftc.gov/business-guidance/privacy-security/privacy-shield.

IV. **Cooperarea cu APD din UE**

FTC recunoaște rolul important pe care îl joacă APD din UE cu privire la respectarea principiilor CCD UE-SUA și încurajează sporirea consultării și cooperarea în vederea asigurării respectării legii. Într-adevăr, o abordare coordonată a provocărilor generate de evoluțiile actuale ale pieței digitale și de modelele de afaceri care utilizează intensiv date este din ce în ce mai importantă. FTC va face schimb de informații cu privire la sesizări cu autoritățile de aplicare a legii de trimitere, inclusiv cu privire la stadiul sesizărilor, sub rezerva legilor 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 invocate, precum și orice măsuri luate în vederea soluționării cazurilor de încălcare a legii, 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 aplicare a legii de trimitere solicită informații privind stadiul unei anumite sesizări în scopul desfășurării propriei proceduri de asigurarea a respectării legii, FTC va răspunde, ținând cont de numărul de sesizări în curs de examinare și cu condiția respectării cerințelor de confidențialitate și a altor cerințe juridice.

De asemenea, FTC va colabora îndeaproape cu APD din UE pentru a oferi asistență pentru asigurarea respectării legii. În cazurile corespunzătoare, aceasta ar putea include schimbul de informații și asistență pentru investigații în conformitate cu Legea SAFE WEB din SUA, care autorizează FTC să acorde asistență agențiilor străine de aplicare a legii atunci când agenția străină pune în aplicare legi care interzic practici în mare măsură similare cu cele interzise de legislația aplicată de FTC ([17]). În cadrul acestei asistențe, FTC poate transmite informații obținute în legătură cu o investigație FTC, poate emite un ordin obligatoriu de depoziție în numele APD din UE care desfășoară propria investigație și poate solicita depoziții orale ale martorilor sau inculpaților în legătură cu procedurile APD de asigurare a respectării legii, sub rezerva îndeplinirii cerințelor Legii SAFE WEB din SUA. FTC utilizează periodic această competență pentru a asista alte autorități din întreaga lume în cazuri care vizează protecția vieții private și a consumatorilor.

Pe lângă consultările cu APD din UE cu privire la aspecte specifice cazurilor, FTC se angajează să participe la reuniuni periodice cu reprezentanții desemnați ai Comitetului european pentru protecția datelor („CEPD") pentru a discuta 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 reprezentanți ai CEPD, la revizuirea periodică a CCD UE-SUA pentru a discuta punerea sa în aplicare. FTC încurajează, de asemenea, dezvoltarea unor instrumente care vor consolida cooperarea cu APD din UE în vederea asigurării respectării legii, precum și cu alte autorități de aplicare a legii în domeniul protecției vieții private din întreaga lume. FTC are plăcerea de a-și afirma angajamentul în direcția punerii în aplicare a aspectelor ce țin de sectorul comercial din CCD UE-SUA. Considerăm că parteneriatul nostru cu colegii din UE este o esențial pentru asigurarea protecției vieții private atât pentru cetățenii noștri, cât și pentru ai dumneavoastră.

Cu stimă,

Lina Khan

Lina M. KHAN
Președinta Comisiei Federale pentru Comerț

([17]) Atunci când decide dacă să își exercite competența în temeiul Legii SAFE WEB din SUA, FTC are în vedere, printre altele: „(A) dacă agenția solicitantă a fost de acord să ofere sau va oferi Comisiei asistență reciprocă, (B) dacă îndeplinirea cererii ar aduce atingere interesului public al Statelor Unite ale Americii și (C) dacă investigația sau procedura de asigurare a respectării legii a agenției solicitante se referă la acte sau practici care cauzează sau pot cauza un prejudiciu unui număr semnificativ de persoane." Titlul 15 articolul 46 litera (j) punctul 3. Această competență nu se aplică în ceea ce privește asigurarea respectării legislației în domeniul concurenței.

Apendicele A

Asigurarea respectării Scutului de confidențialitate și a programului privind sfera de siguranță

	Nr. de înregistrare pe rol/nr. dosar FTC	**Cazul**	**Linkul**
1	Dosar FTC nr. 2023062 Cazul nr. 3:22-cv-03070 (N.D. Cal.)	SUA/**Twitter, Inc.**	Twitter
2	Dosar FTC nr. 192 3209	Residual Pumpkin Entity, LLC, anterior desfășurându-și activitatea sub denumirea **CafePress** și PlanetArt, LLC, anterior desfășurându-și activitatea sub denumirea **CafePress**	CafePress
3	Dosar FTC nr. 192 3133 Nr. de înregistrare pe rol – C-4747	Flo Health, Inc.	Flo Health
4	Dosar FTC nr. 192 3050 Nr. de înregistrare pe rol – C-4723	Ortho-Clinical Diagnostics, Inc.	Ortho-Clinical
5	Dosar FTC nr. 192 3092 Nr. de înregistrare pe rol – C-4709	T&M Protection, LLC	T&M Protection
6	Dosar FTC nr. 192 3084 Nr. de înregistrare pe rol – C-4704	TDARX, Inc.	TDARX
7	Dosar FTC nr. 192 3093 Nr. de înregistrare pe rol – C-4706	Global Data Vault, LLC	Global Data
8	Dosar FTC nr. 192 3078 Nr. de înregistrare pe rol – C-4703	Incentive Services, Inc.	Incentive Services
9	Dosar FTC nr. 192 3090 Nr. de înregistrare pe rol – C-4705	Click Labs, Inc.	Click Labs
10	Dosar FTC nr. 182 3192 Nr. de înregistrare pe rol – C-4697	Medable, Inc.	Medable
11	Dosar FTC nr. 182 3189 Nr. de înregistrare pe rol – 9386	NTT Global Data Centers Americas, Inc., în calitate de succesor în drepturi a **RagingWire Data Centers, Inc.**	RagingWire
12	Dosar FTC nr. 182 3196 Nr. de înregistrare pe rol – C-4702	Thru, Inc.	Thru
13	Dosar FTC nr. 182 3188 Nr. de înregistrare pe rol – C-4698	DCR Workforce, Inc.	DCR Workforce
14	Dosar FTC nr. 182 3194 Nr. de înregistrare pe rol – C-4700	LotaData, Inc.	LotaData
15	Dosar FTC nr. 182 3195 Nr. de înregistrare pe rol – C-4701	EmpiriStat, Inc.	EmpiriStat

16	Dosar FTC nr. 182 3193 Nr. de înregistrare pe rol – C-4699	214 Technologies, Inc., anterior desfășurându-și activitatea sub denumirea **Trueface.ai**	Trueface.ai
17	Dosar FTC nr. 182 3107 Nr. de înregistrare pe rol – 9383	Cambridge Analytica, LLC	Cambridge Analytica
18	Dosar FTC nr. 182 3152 Nr. de înregistrare pe rol – C-4685	SecureTest, Inc.	SecurTest
19	Dosar FTC nr. 182 3144 Nr. de înregistrare pe rol – C-4664	VenPath, Inc.	VenPath
20	Dosar FTC nr. 182 3154 Nr. de înregistrare pe rol – C-4666	SmartStart Employment Screening, Inc.	SmartStart
21	Dosar FTC nr. 182 3143 Nr. de înregistrare pe rol – C-4663	**mResourceLLC,** anterior desfășurându-și activitatea sub denumirea Loop Works LLC	mResource
22	Dosar FTC nr. 182 3150 Nr. de înregistrare pe rol – C-4665	Idmission LLC	IDmission
23	Dosar FTC nr. 182 3100 Nr. de înregistrare pe rol – C-4659	ReadyTech Corporation	ReadyTech
24	Dosar FTC nr. 172 3173 Nr. de înregistrare pe rol – C-4630	Decusoft, LLC	Decusoft
25	Dosar FTC nr. 172 3171 Nr. de înregistrare pe rol – C-4628	Tru Communication, Inc.	Tru
26	Dosar FTC nr. 172 3172 Nr. de înregistrare pe rol – C-4629	Md7, LLC	Md7
30	Dosar FTC nr. 152 3198 Nr. de înregistrare pe rol – C-4543	Jhayrmaine Daniels (anterior desfășurându-și activitatea sub denumirea California Skate-Line)	Jhayrmaine Daniels
31	Dosar FTC nr. 152 3190 Nr. de înregistrare pe rol – C-4545	Dale Jarrett Racing Adventure, Inc.	Dale Jarrett
32	Dosar FTC nr. 152 3141 Nr. de înregistrare pe rol – C-4540	Golf Connect, LLC	Golf Connect
33	Dosar FTC nr. 152 3202 Nr. de înregistrare pe rol – C-4546	Inbox Group, LLC	Inbox Group
34	Dosar nr. 152 3187 Nr. de înregistrare pe rol – C-4542	IOActive, Inc.	IOActive
35	Dosar FTC nr. 152 3140 Nr. de înregistrare pe rol – C-4549	Jubilant Clinsys, Inc.	Jubilant
36	Dosar FTC nr. 152 3199 Nr. de înregistrare pe rol – C-4547	Just Bagels Manufacturing, Inc.	Just Bagels

37	Dosar FTC nr. 152 3138 Nr. de înregistrare pe rol – C-4548	NAICS Association, LLC	NAICS
38	Dosar FTC nr. 152 3201 Nr. de înregistrare pe rol – C-4544	One Industries Corp.	One Industries
39	Dosar FTC nr. 152 3137 Nr. de înregistrare pe rol – C-4550	Pinger, Inc.	Pinger
40	Dosar FTC nr. 152 3193 Nr. de înregistrare pe rol – C-4552	SteriMed Medical Waste Solutions	SteriMed
41	Dosar FTC nr. 152 3184 Nr. de înregistrare pe rol – C-4541	Contract Logix, LLC	Contract Logix
42	Dosar FTC nr. 152 3185 Nr. de înregistrare pe rol – C-4551	Forensics Consulting Solutions, LLC	Forensics Consulting
43	Dosar FTC nr. 152 3051 Nr. de înregistrare pe rol – C-4526	American Int'l Mailing, Inc.	AIM
44	Dosar FTC nr. 152 3015 Nr. de înregistrare pe rol – C-4525	TES Franchising, LLC	TES
45	Dosar FTC nr. 142 3036 Nr. de înregistrare pe rol – C-4459	American Apparel, Inc.	American Apparel
46	Dosar FTC nr. 142 3026 Nr. de înregistrare pe rol – C-4469	Fantage.com, Inc.	Fantage
47	Dosar FTC nr. 142 3017 Nr. de înregistrare pe rol – C-4461	Apperian, Inc.	Apperian
48	Dosar FTC nr. 142 3018 Nr. de înregistrare pe rol – C-4462	Atlanta Falcons Football Club, LLC	Atlanta Falcons
49	Dosar FTC nr. 142 3019 Nr. de înregistrare pe rol – C-4463	Baker Tilly Virchow Krause, LLP	Baker Tilly
50	Dosar FTC nr. 142 3020 Nr. de înregistrare pe rol – C-4464	BitTorrent, Inc.	BitTorrent
51	Dosar FTC nr. 142 3022 Nr. de înregistrare pe rol – C-4465	Charles River Laboratories, Int'l	Charles River
52	Dosar FTC nr. 142 3023 Nr. de înregistrare pe rol – C-4466	DataMotion, Inc.	DataMotion
53	Dosar FTC nr. 142 3024 Nr. de înregistrare pe rol – C-4467	**DDC Laboratories, Inc.**, anterior desfășurându-și activitatea sub denumirea DNA Diagnostics Center	DDC
54	Dosar FTC nr. 142 3028 Nr. de înregistrare pe rol – C-4470	Level 3 Communications, LLC	Level 3

55	Dosar FTC nr. 142 3025 Nr. de înregistrare pe rol – C-4468	**PDB Sports, Ltd.**, anterior desfășurându-și activitatea sub denumirea Denver Broncos Football Club, LLP	Broncos
56	Dosar FTC nr. 142 3030 Nr. de înregistrare pe rol – C-4471	Reynolds Consumer Products, Inc.	Reynolds
57	Dosar FTC nr. 142 3031 Nr. de înregistrare pe rol – C-4472	Receivable Management Services Corporation	Receivable Mgmt
58	Dosar FTC nr. 142 3032 Nr. de înregistrare pe rol – C-4473	Tennessee Football, Inc.	Tennessee Football
59	Dosar FTC nr. 102 3058 Nr. de înregistrare pe rol – C-4369	Myspace LLC	Myspace
60	Dosar FTC nr. 092 3184 Nr. de înregistrare pe rol – C-4365	Facebook, Inc.	Facebook
61	Dosar FTC nr. 092 3081 Acțiunea civilă nr. 09-CV-5276 (C. D. Cal.)	FTC/Javian Karnani și **Balls of Kryptonite, LLC**, anterior desfășurându-și activitatea sub denumirea Bite Size Deals, LLC și Best Priced Brands, LLC	Balls of Kryptonite
62	Dosar FTC nr. 102 3136 Nr. de înregistrare pe rol – C-4336	Google, Inc.	Google
63	Dosar FTC nr. 092 3137 Nr. de înregistrare pe rol – C-4282	World Innovators, Inc.	World Innovators
64	Dosar FTC nr. 092 3141 Nr. de înregistrare pe rol – C-4271	Progressive Gaitways LLC	Progressive Gaitways
65	Dosar FTC nr. 092 3139 Nr. de înregistrare pe rol – C-4270	Onyx Graphics, Inc.	Onyx Graphics
66	Dosar FTC nr. 092 3138 Nr. de înregistrare pe rol – C-4269	ExpatEdge Partners, LLC	ExpatEdge
67	Dosar FTC nr. 092 3140 Nr. de înregistrare pe rol – C-4281	Directors Desk LLC	Directors Desk
68	Dosar FTC nr. 092 3142 Nr. de înregistrare pe rol – C-4272	Collectify LLC	Collectify

ANEXA V

THE SECRETARY OF TRANSPORTATION
WASHINGTON, DC 20590

6 iulie 2023

Comisarul Didier Reynders
Comisia Europeană
Rue de la Loi/Wetstraat 200
1049 1049 Bruxelles
Belgia

Stimate Domnule Comisar Reynders,

Departamentul Transporturilor al Statelor Unite ale Americii („departamentul" sau „DoT") apreciază posibilitatea de a descrie rolul său în asigurarea respectării principiilor Cadrului UE-SUA privind confidențialitatea datelor („CCD UE-SUA"). CCD UE-SUA va juca un rol esențial în protecția datelor cu caracter personal furnizate în cursul tranzacțiilor comerciale 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.

Departamentul Transporturilor și-a exprimat pentru prima dată, în mod public, angajamentul față de asigurarea respectării Cadrului privind sfera de siguranță UE-SUA într-o scrisoare adresată Comisiei Europene cu peste 22 de ani în urmă, iar acest angajament a fost reluat și extins în scrisoarea din 2016 referitoare la Cadrul privind Scutul de confidențialitate UE-SUA. În scrisorile respective, Departamentul Transporturilor s-a angajat să asigure respectarea cu strictețe a principiilor privind protecția vieții private ale sferei de siguranță UE-SUA și, ulterior, a principiilor Scutului de confidențialitate UE-SUA. DoT își extinde angajamentul la principiile CCD UE-SUA, iar prezenta scrisoare consacră acest angajament.

În special, DoT își confirmă angajamentul în următoarele domenii esențiale: (1) realizarea cu prioritate a investigațiilor unor presupuse încălcări ale principiilor CCD UE-SUA, (2) acțiuni adecvate de asigurare a respectării legii împotriva entităților care fac afirmații false sau înșelătoare cu privire la participarea la CCD UE-SUA și (3) monitorizarea și publicarea ordinelor de asigurare a respectării legii privind încălcările CCD UE-SUA. Prezentăm informații cu privire la fiecare dintre aceste angajamente și, pentru contextul necesar, istoricul pertinent privind rolul DoT în protecția vieții private a consumatorilor și asigurarea respectării principiilor CCD UE-SUA.

1. **Context**

A. Competența în materie de confidențialitate a DoT

Departamentul este ferm hotărât să asigure confidențialitatea informațiilor furnizate de consumatori companiilor aeriene și agenților de bilete.

Autoritatea DoT de a lua măsuri în acest domeniu se întemeiază pe titlul 49 articolul 41712 din U.S.C., care interzice unui transportator sau unui agent de bilete să desfășoare orice „practică neloială sau frauduloasă" în cadrul activității de transport aerian sau pentru vânzarea de servicii de transport aerian. Articolul 41712 este formulat după modelul secțiunii 5 din Legea Comisiei Federale pentru Comerț (titlul 15 articolul 45 din U.S.C.).

Recent, DoT a emis reglementări care definesc practicile neloiale și înșelătoare, în concordanță atât cu precedentele DoT, cât și FTC (titlul 14 articolul 399.79 din CFR). Mai exact, o practică este considerată „neloială" în cazul în care cauzează sau poate cauza un prejudiciu semnificativ consumatorilor, care nu poate fi evitat în mod rezonabil și care nu este compensat de beneficiile pentru consumatori sau concurență.

O practică este „înșelătoare” pentru consumatori în cazul în care poate să inducă în eroare un consumator care acționează în mod rezonabil în circumstanțele date cu privire la un aspect semnificativ. Un aspect este semnificativ dacă este probabil ca acesta să fie afectat comportamentul sau decizia consumatorului cu privire la un produs sau un serviciu. Pe lângă aceste principii generale, DoT interpretează în mod specific articolul 41712 ca interzicând transportatorilor și agenților de bilete: (1) să încalce dispozițiile politicii sale de confidențialitate, (2) să încalce orice normă emisă de departament care identifică practici specifice de protecție a vieții private ca neloiale sau frauduloase sau (3) să încalce Legea privind respectarea vieții private a copiilor în mediul online („COPPA”) sau normele FTC de punere în aplicare a COPPA sau (4) în calitate de participant la CCD UE-SUA, să încalce principiile CCD UE SUA ([1]).

Astfel cum se menționează anterior, în temeiul legii federale, DoT dispune de competențe exclusive de reglementare a practicilor 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 de bilete la vânzarea serviciilor de transport aerian.

Astfel, după ce un transportator sau un vânzător de servicii de transport aerian se angajează public să respecte principiile CCD UE-SUA, departamentul poate să recurgă la competențele legale 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 de bilete care și-a luat angajamentul să respecte principiile CCD UE-SUA, orice nerespectare a acestui angajament de către transportatorul sau agentul de bilete respectiv ar constitui o încălcare a articolului 41712.

B. Practici de asigurare a respectării legii

Biroul pentru protecția consumatorilor în domeniul aviației (*Office of Aviation Consumer Protection*) („OACP”) ([2]) din cadrul departamentului investighează cazuri și introduce acțiuni în legătură cu acestea 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 negociere, pregătirea ordinelor administrative de încetare și elaborarea de ordine privind sancțiunile civile. Biroul ia cunoștință de încălcările potențiale, în mare măsură, ca urmare a plângerilor pe care le primește din partea persoanelor, a agenților de turism, a companiilor aeriene și a agențiilor guvernamentale din Statele Unite ale Americii și din străinătate. Consumatorii pot utiliza site-ul web al DoT pentru a depune plângeri în materie de confidențialitate împotriva companiilor aeriene și agenților de bilete ([3]).

În situația în care nu se ajunge la o tranzacție rezonabilă și adecvată într-un caz, OACP are competența de a iniția o procedură de asigurare a respectării legii care implică o audiere probatorie în fața unui judecător de drept administrativ („JDA”) al DoT. JDA are competența de a emite ordine administrative de încetare și de a impune sancțiuni civile. Nerespectarea dispozițiilor articolului 41712 poate avea ca rezultat emiterea de ordine administrative de încetare și impunerea de sancțiuni civile de până la 37 377 USD pentru fiecare încălcare a articolului 41712.

Departamentul nu are competența de a acorda daune sau despăgubiri pecuniare reclamantului. Cu toate acestea, departamentul are competența de a aproba tranzacțiile rezultate în urma investigațiilor desfășurate de OACP care aduc beneficii directe consumatorilor (de exemplu, în numerar, tichete) pentru a compensa sancțiunile monetare datorate în alt mod autorităților SUA. Acest lucru s-a întâmplat în trecut și este posibil, de asemenea, în contextul principiilor CCD UE-SUA 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 funcționare și, în consecință, riscă să-și piardă licența de funcționare.

Până în prezent, DoT a primit relativ puține plângeri care implică presupuse încălcări ale confidențialității de către agenții de bilete sau de către companiile aeriene. Atunci când apar, acestea sunt investigate în conformitate cu principiile enunțate mai sus.

C. Măsuri de protecție juridică ale DoT în beneficiul consumatorilor din UE

În temeiul articolului 41712, interdicția cu privire la practicile neloiale sau frauduloase în transportul aerian sau vânzarea serviciilor de transport aerian se aplică agenților de bilete, precum și companiilor aeriene americane și străine. DoT ia frecvent măsuri împotriva companiilor aeriene americane și străine pentru practici 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. DoT 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.

([1]) https://www.transportation.gov/individuals/aviation-consumer-protection/privacy.

([2]) Denumit anterior Biroul pentru proceduri și asigurarea respectării legii în domeniul aviației (*Office of Aviation Enforcement and Proceedings*).

([3]) http://www.transportation.gov/airconsumer/privacy-complaints.

De asemenea, în ceea ce privește companiile aeriene, DoT asigură aplicarea altor legi specifice ale căror măsuri de protecție se extind la consumatori care nu sunt cetățeni americani/rezidenți SUA, cum ar fi Legea privind respectarea vieții private a copiilor în mediul online („COPPA"). Printre altele, COPPA impune operatorilor de servicii online și site-uri web care vizează copiii sau de site-uri web care vizează publicul general și care colectează în cunoștință de cauză 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 web și serviciile care fac obiectul COPPA și care colectează informații cu caracter personal de la copii străini sunt obligați să respecte dispozițiile COPPA. Site-urile web și serviciile online cu sediul 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 din Statele Unite ale Americii. În măsura în care companiile aeriene americane sau străine care își desfășoară activitatea în Statele Unite ale Americii încalcă COPPA, DoT ar avea competența de a întreprinde acțiuni de asigurare a respectării legii.

II. **Asigurarea respectării principiilor CCD UE-SUA**

În cazul în care o companie aeriană sau un agent de bilete alege să participe la CCD UE-SUA, iar departamentul primește o plângere potrivit căreia o astfel de companie aeriană sau un astfel de agent de bilete ar fi încălcat principiile CCD UE-SUA, departamentul ia următoarele măsuri pentru a asigura respectarea cu strictețe a principiilor CCD UE-SUA.

A. Realizarea cu prioritate a investigării pretinselor încălcări

OACP din cadrul Departamentului va investiga fiecare plângere referitoare la pretinse încălcări ale principiilor CCD UE-SUA, inclusiv plângerile primite de la autorități pentru protecția datelor („APD") din UE și va întreprinde acțiuni de asigurare a respectării legii în cazul în care există dovezi ale unei încălcări.

În plus, OACP va coopera cu FTC și Departamentul Comerțului și va acorda prioritate plângerilor legate de nerespectarea de către entitățile reglementate a angajamentelor în materie de confidențialitate asumate în temeiul CCD UE-SUA.

La primirea unei plângeri privind o încălcare a principiilor CCD UE-SUA, OACP poate lua o serie de măsuri în cadrul investigației sale. De exemplu, acesta poate revizui politicile de confidențialitate ale companiei aeriene sau ale agentului de bilete, poate obține informații suplimentare din partea companiei aeriene sau a agentului de bilete sau de la terți, poate asigura o monitorizare împreună cu entitatea de trimitere și poate evalua dacă există mai multe încălcări sau un număr semnificativ de consumatori afectați. În plus, acesta poate stabili dacă problema se referă la aspecte care intră în domeniul de competență al Departamentului Comerțului sau FTC, poate evalua dacă ar fi utilă educarea consumatorilor sau a mediului de afaceri și, după caz, poate iniția o procedură de asigurare a respectării legii.

În cazul în care departamentul ia cunoștință de posibile încălcări ale principiilor CCD UE-SUA comise de agenți de bilete, acesta își va coordona acțiunile cu FTC în această privință. De asemenea, comunicăm FTC și Departamentului Comerțului rezultatul oricăror acțiuni de asigurare a respectării principiilor CCD UE-SUA.

B. Abordarea declarațiilor false sau frauduloase de participare

Departamentul își menține angajamentul de a investiga încălcările principiilor CCD UE-SUA, inclusiv declarațiile false sau frauduloase de participare la CCD UE-SUA. Vom acorda prioritate examinării sesizărilor din partea Departamentului Comerțului în ceea ce privește organizațiile identificate de acesta ca declarând în mod nejustificat că participă la CCD UE-SUA sau ca utilizând marca de certificare CCD UE-SUA fără a deține autorizarea în acest sens.

În plus, observăm că, dacă politica de confidențialitate a unei organizații afirmă că respectă principiile CCD UE SUA, incapacitatea acesteia de a efectua sau de a menține o autocertificare prin intermediul Departamentului Comerțului nu va scuti, în sine, organizația de la impunerea angajamentelor respective de către DoT.

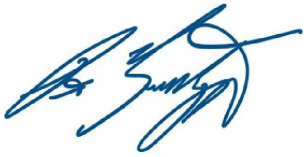
C. Monitorizarea și publicarea ordinelor de asigurare a respectării legii privind încălcările CCD UE-SUA

OACP din cadrul departamentului își reafirmă, de asemenea, angajamentul de a monitoriza ordinele de asigurare a respectării legii după cum este necesar pentru a asigura respectarea principiilor CCD UE-SUA. Mai precis, în cazul în care biroul emite un ordin de încetare prin care se indică unei companii aeriene sau unui agent de bilete să nu mai comită în viitor nicio încălcare a principiilor CCD UE-SUA și a articolului 41712, acesta va monitoriza respectarea de către entitatea respectivă a dispoziției de încetare din ordinul respectiv. În plus, biroul se va asigura că ordinele care decurg din cazuri care vizează principiile CCD UE-SUA sunt disponibile pe site-ul său web.

Așteptăm cu interes continuarea activității noastre cu partenerii de la nivel federal și cu părțile interesate din UE cu privire la aspecte legate de CCD UE-SUA.

Sper că aceste informații vă vor fi utile. Vă stau la dispoziție pentru orice informații suplimentare.

Cu stimă,



Pete BUTTIGIEG

ANEXA VI

Departamentul de Justiție al SUA

Divizia penală

Biroul Procurorului General Adjunct Washington, D.C. 20530

23 iunie 2023

Dna Ana Gallego Torres
Director general justiție și consumatori
Comisia Europeană
Rue Montoyer/Montoyerstraat 59
1049 Bruxelles
Belgia

Stimată Doamnă Director General Gallego Torres,

Prezenta scrisoare cuprinde o scurtă prezentare generală a principalelor instrumente de investigare utilizate pentru obținerea de date comerciale și alte informații din registre de la societățile din Statele Unite ale Americii în scopul asigurării respectării dreptului penal sau în interes public (civil și de reglementare), inclusiv a limitărilor cu privire la acces prevăzute de mecanismele respective ([1]). Toate procesele juridice descrise în prezenta scrisoare sunt nediscriminatorii prin faptul că sunt utilizate pentru obținerea de informații de la societățile din Statele Unite ale Americii, inclusiv de la societăți care se vor autocertifica prin intermediul Cadrului UE-SUA privind confidențialitatea datelor, fără a ține cont de cetățenia sau locul de reședință al persoanei vizate. În plus, societățile care beneficiază de calitate procesuală în Statele Unite ale Americii o pot contesta în instanță, astfel cum este descris mai jos ([2]).

În ceea ce privește confiscarea datelor de către autoritățile publice, trebuie remarcat 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 SUA, 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 acestui amendament, astfel cum este recunoscut în numeroase hotărâri ale Curții, este să protejeze viața privată și securitatea persoanelor împotriva invaziei arbitrare din partea funcționarilor guvernamentali.” (388 U.S. 41, 53 (1967) [citând hotărârea Camara/Tribunalul Municipal din San Francisco, 387 U.S. 523, 528 (1967)]. În investigările interne, cel de al patrulea amendament impune, în general, agenților de aplicare a legii să obțină un mandat judecătoresc înainte de a efectua o percheziție. A se vedea hotărârea Katz/Statele Unite ale Americii, 389 U.S. 347, 357

([1]) Această prezentare generală nu descrie instrumentele de investigare în materie de securitate națională utilizate de autoritățile de aplicare a legii în investigații cu privire la terorism și alte investigații privind securitatea națională, inclusiv scrisorile privind securitatea națională (*National Security Letters* – NSL) – pentru anumite informații din rapoartele de credit, evidențele financiare și evidențele electronice privind abonații și tranzacțiile, a se vedea titlul 12 articolul 3414 din U.S.C., titlul 15 articolul 1681u din U.S.C., titlul 15 articolul 1681v din U.S.C., titlul 18 articolul 2709 din U.S.C., titlul 50 articolul 3162 din U.S.C., iar pentru măsurile de supraveghere electronică, mandatele de percheziție, documentele comerciale și alte colectări de informații efectuate în temeiul Legii privind supravegherea activităților străine de spionaj, a se vedea titlul 50 articolul 1801 și urm. din U.S.C.

([2]) Această scrisoare discută aplicarea legii federale și autoritățile de reglementare. Încălcările legislației statale sunt investigate de autoritățile statale de aplicare a legii și sunt judecate în instanțele statale. Autoritățile statale de aplicare a legii utilizează mandatele și citațiile emise conform legislației statale, în esență în același mod descris în prezentul document, dar cu posibilitatea ca procesul juridic la nivel de stat să poată face obiectul unor măsuri de protecție suplimentare prevăzute de constituțiile sau statutele statelor, care le depășesc pe cele din Constituția SUA. Măsurile de protecție din legislația statală trebuie să fie cel puțin egale cu cele din Constituția SUA, inclusiv cu al patrulea amendament, dar fără a se limita la acesta.

(1967). Standardele pentru emiterea unui mandat, cum ar fi cerințele privind cauza probabilă și caracterul particular, se aplică mandatelor pentru percheziții fizice și confiscări, precum și mandatelor pentru conținutul stocat al comunicațiilor electronice emise în temeiul Legii privind comunicațiile stocate, astfel cum se discută în cele ce urmează. Atunci când cerința privind mandatul nu se aplică, activitatea autorității publice este supusă, totuși, unui test privind caracterul rezonabil în temeiul celui de al patrulea amendament. Prin urmare, se garantează chiar prin Constituție faptul că, în SUA, autoritatea publică nu are putere nelimitată sau arbitrară de a reține informații cu caracter privat ([3]).

Autoritățile de aplicare a dreptului penal:

Procurorii federali, care sunt funcționari ai Departamentului de Justiție (DOJ) și agenți federali de investigații, inclusiv agenții din cadrul Biroului Federal de Investigații (FBI), agenție de aplicare a legii din cadrul DOJ, sunt în măsură să impună societăților din Statele Unite ale Americii să prezinte documente și alte informații din registre în scopuri de cercetare penală prin intermediul mai multor tipuri de procese juridice obligatorii, inclusiv prin citații pentru a apărea în fața marelui juriu, citații administrative și mandate de percheziție, și pot obține alte comunicări în baza mecanismelor federale de interceptare a comunicațiilor în temeiul legislației penale.

Citațiile pentru a apărea în fața marelui juriu sau la proces: Citațiile penale sunt utilizate pentru a sprijini anchete specifice 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 investigație a marelui juriu în cazul unei anumite presupuse încălcări a dreptului penal. Marile jurii reprezintă ramura de investigare a instanței și sunt alcătuite de un judecător sau magistrat. O citație poate impune unei persoane să depună mărturie în cadrul unei proceduri sau să producă sau să pună la dispoziție documente comerciale, informații stocate electronic sau alte elemente tangibile. Informațiile trebuie să fie relevante pentru investigație, iar citația nu poate fi nerezonabilă, fiind excesiv de cuprinzătoare, abuzivă sau împovărătoare. Persoana citată poate depune o propunere de a contesta o citație întemeiată pe aceste motive. A se vedea Codul federal de procedură penală, p. 17. În anumite circumstanțe, citațiile referitoare la 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 prezenta sau a pune la dispoziție documente comerciale, informații stocate electronic sau alte elemente tangibile relevante pentru investigațiile care implică fraudarea serviciilor de sănătate, abuzuri împotriva copiilor, protecția Serviciului Secret, cazuri referitoare la substanțe controlate și investigații ale inspectorului general care implică agenții 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 nerezonabilă deoarece este excesiv de cuprinzătoare sau pentru că este abuzivă sau împovărătoare.

Ordine judecătorești pentru interceptare și capturare și trasabilitate: În temeiul dispozițiilor privind interceptarea și capturarea și trasabilitatea în materie penală, autoritățile de aplicare a legii pot obține un ordin judecătoresc de a obține, în timp real, disimularea, rutarea, adresarea și semnalarea de informații cu privire la un număr de telefon sau la o adresă de e-mail, pe baza certificării faptului că informațiile furnizate sunt relevante pentru o investigare în curs. A se vedea titlul 18 articolele 3121-3127 din U.S.C. 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 (*internet service providers* – ISP), de companiile de telefonie și de alți furnizori de servicii terți, în temeiul titlului II din ECPA, denumită și Legea privind comunicațiile stocate (*Stored Communications Act* – SCA), titlul 18 articolele 2701-2712 din U.S.C. SCA stabilește un sistem de drepturi legale la viață privată care limitează accesul autorităților de aplicare a legii la alte date decât cele necesare în temeiul dreptului constituțional ale clienților și abonaților ai furnizorilor de servicii de internet. SCA prevede creșterea nivelului de protecție

([3]) În ceea ce privește principiile celui de al patrulea amendament privind protecția vieții private și a intereselor de securitate care sunt discutate mai sus, instanțele din SUA aplică în mod regulat aceste principii noilor tipuri de instrumente de investigare în materie de aplicare a legii care sunt facilitate de evoluțiile tehnologice. De exemplu, în 2018, Curtea Supremă a statuat că obținerea de către autoritatea publică, în cadrul unei anchete de aplicare a legii, a istoricului datelor privind localizarea unui telefon mobil de la o societate de telefonie mobilă pentru o perioadă îndelungată constituie o „percheziție" care face obiectul cerinței privind mandatul prevăzută în cel de al patrulea amendament. Carpenter/Statele Unite ale Americii, 138 S. Ct. 2206 (2018).

a vieții private în funcție de caracterul intruziv al colectării. Pentru informațiile de înregistrare ale abonaților, adresele IP și mărcile temporale asociate, precum și informațiile privind facturarea, autoritățile de aplicare a dreptului penal trebuie să obțină o citație. Pentru majoritatea celorlalte informații fără conținut stocate, cum ar fi antete de 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 importante pentru o investigare în curs. Pentru a obține conținutul stocat al comunicațiilor, în general, autoritățile de aplicare a dreptului penal trebuie să obțină un mandat de la un judecător pe baza unei cauze probabile de a crede că acel cont conține dovezi ale unei infracțiuni. SCA prevede, de asemenea, răspunderea civilă și sancțiuni penale ([4]).

Ordine judecătorești de supraveghere în temeiul Legii federale privind interceptarea convorbirilor: În plus, autoritățile de aplicare a legii pot intercepta în timp real comunicații prin cablu, comunicații orale sau electronice în scopuri de cercetare penală, în conformitate cu Legea federală privind interceptarea comunicațiilor. A se vedea titlul 18 articolele 2510-2523 din U.S.C. Această competență este disponibilă numai în temeiul unui ordin judecătoresc, prin care un judecător constată, printre altele, că există o cauză probabilă 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.

Mandat de percheziție – Codul federal de procedură penală, articolul 41: Autoritățile de aplicarea legii pot să percheziționeze fizic spații din Statele Unite în cazul în care sunt autorizate în acest sens de un judecător. Autoritățile de aplicare a legii trebuie să demonstreze judecătorului, pe baza unei cauze probabile, că o infracțiune a fost comisă sau este pe cale să fie comisă și că obiectele legate de infracțiune sunt susceptibile de a fi găsite în locul specificat în mandat. Această competență este utilizată adesea în cazul în care 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 societății i se trimite o citație sau un alt tip de ordin de prezentare. O persoană care face obiectul unei percheziții sau ale cărei bunuri fac obiectul unei percheziții poate solicita invalidarea elementelor de probă obținute sau rezultate în urma unei percheziții ilegale în cazul în care se aduc astfel de probe împotriva persoanei respective în cursul unui proces penal. A se vedea hotărârea Mapp/Ohio, 367 U.S. 643 (1961). În cazul în care un deținător de date este obligat să divulge date în temeiul unui mandat, partea obligată poate contesta cerința de divulgare a datelor ca fiind nejustificat de împovărătoare. A se vedea hotărârea cu privire la o cerere înaintată de Statele Unite ale Americii, 610 F.2d 1148, 1157 (al treilea circuit, 1979) (în care s-a statuat că, „pentru respectarea garanțiilor procedurale, este necesar să aibă loc o audiere cu privire la caracterul împovărător al unei măsuri înainte de a obliga o societate de telefonie să furnizeze" asistență în baza unui mandat de percheziție); hotărârea cu privire la o cerere înaintată de Statele Unite ale Americii, 616 F.2d 1122 (al nouălea circuit, 1980) (care a ajuns la aceeași concluzie pe baza competenței de supraveghere a instanței).

Orientările și politicile DOJ: Pe lângă aceste limitări constituționale, statutare și bazate pe norme privind accesul autorității publice la date, procurorul general a emis orientări care stabilesc limite suplimentare pentru accesul autorităților de aplicare a legii la date și care conțin, de asemenea, măsuri de protecție a vieții private și a libertăților 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 investigare pentru a căuta informații cu privire la anchetele care implică infracțiuni federale. Aceste orientări prevăd ca FBI să utilizeze metodele de anchetă cele mai puțin invazive, luând în considerare impactul asupra vieții private și a libertăților civile și eventualele daune aduse reputației. De asemenea, acestea prevăd că „este incontestabil 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." Orientările AG FBI 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%28DIOG%29, un manual cuprinzător care include limite detaliate privind utilizarea unor instrumente de investigare și orientări pentru a se asigura că libertățile publice și viața privată sunt protejate în fiecare anchetă. Norme și politici suplimentare care prevăd limitări ale activităților de investigare ale procurorilor federali sunt stabilite în Manualul justiției, disponibil, de asemenea, online la adresa https://www.justice.gov/jm/justicemanual.

Autoritățile civile și de reglementare (interesul public):

([4]) În plus, secțiunea 2705 litera (b) din SCA autorizează autoritatea publică să obțină un ordin judecătoresc, pe baza unei nevoi demonstrate de protecție împotriva divulgării, prin care se interzice unui furnizor de servicii de comunicații să notifice în mod voluntar utilizatorilor săi demararea procesului juridic în temeiul SCA. În octombrie 2017, procurorul general adjunct Rod Rosenstein a emis un memorandum adresat avocaților și agenților DOJ, care prevede orientări pentru asigurarea faptului că cererile pentru astfel de ordine de protecție sunt adaptate faptelor și preocupărilor specifice investigației și care stabilește un plafon general de un an pentru perioada cu care o cerere poate încerca să amâne notificarea. În mai 2022, procurorul general adjunct Lisa Monaco a emis orientări suplimentare pe această temă, care, printre alte aspecte, au stabilit cerințe interne de aprobare de către DOJ pentru cererile de prelungire a unui ordin de protecție dincolo de perioada inițială de un an și au solicitat încetarea ordinelor de protecție la încheierea unei investigații.

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 societăților pentru documente comerciale, informații stocate electronic sau alte elemente tangibile. Aceste agenții sunt limitate în ceea ce privește exercitarea competenței administrative sau civile de citare nu numai prin legile lor organice, ci și prin controlul jurisdicțional independent al unor citații emise înainte de punerea în aplicare a unor potențiale decizii judiciare. A se vedea, de exemplu Codul federal de procedură civilă 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 citații administrative poate contesta executarea acestei citații în instanță, prezentând dovada că agenția nu a acționat în conformitate cu standardele de bază privind caracterul rezonabil, astfel cum s-a arătat anterior.

Există alte temeiuri juridice pentru ca societățile să conteste cererile de date din partea agențiilor administrative, pe baza sectoarelor lor specifice de activitate și a tipurilor de date pe care le dețin. De exemplu, instituțiile financiare pot contesta citațiile administrative care urmăresc anumite tipuri de informații ca fiind încălcări ale Legii privind secretul bancare și ale regulamentelor de punere în aplicare ale acesteia. Titlul 31 articolul 5318 din U.S.C.; titlul 31 capitolul X din C.F.R. Alte întreprinderi pot invoca Legea privind raportarea echitabilă a creditelor (*Fair Credit Reporting Act*), a se vedea titlul 15 articolul 1681b din U.S.C., sau o serie de alte legi sectoriale specifice. Utilizarea abuzivă a autorității de citare a unei agenții poate antrena răspunderea agenției sau răspunderea personală a agenților agenției. A se vedea, de exemplu, Legea privind dreptul la confidențialitate financiară (*Right to Financial Privacy Act*), titlul 12 articolele 3401-3423 din U.S.C. Astfel, instanțele din Statele Unite apără împotriva solicitărilor neadecvate de reglementare și asigură supravegherea independentă a acțiunilor agențiilor federale.

În cele din urmă, orice competență legală de care dispun autoritățile administrative pentru a confisca fizic evidențele unei societăți din Statele Unite ale Americii în urma unei percheziții administrative trebuie să îndeplinească cerințele stabilite în temeiul celui de al patrulea amendament. A se vedea hotărârea 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, statutele, normele și reglementările. 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 de a obține informații de la societățile din Statele Unite – indiferent dacă informațiile se referă la cetățeni americani/rezidenți în SUA sau cetățeni ai unor țări străine – și, în plus, permite controlul jurisdicțional al tuturor solicitărilor de date ale autorităților publice în conformitate cu aceste competențe.

Bruce C. Swartz
Deputy Assistant Attorney General and
Counselor for International Affairs

ANEXA VII

BIROUL DIRECTORULUI SERVICIULUI NAȚIONAL DE INFORMAȚII AL CONSILIERULUI GENERAL

WASHINGTON, DC 20511

9 decembrie 2022

Consilier general
Leslie B. Kiernan
Departamentul Comerțului din
SUA 1401 Constituție Ave.,
NW Washington, DC 20230

Stimată Doamnă Kiernan,

La 7 octombrie 2022, Președintele Biden a semnat Ordinul executiv nr. 14086, *„Enhancing Safeguards for US Signals Intelligence Activities”* (Consolidarea garanțiilor pentru activitățile de colectare de informații de tip SIGINT desfășurate de Statele Unite ale Americii), care consolidează gama riguroasă de garanții privind viața privată și libertățile civile care se aplică activităților SUA de colectare a informațiilor de tip SIGINT. Aceste garanții includ: impunerea obligației ca activitățile de colectare de informații de tip SIGINT să îndeplinească obiectivele legitime enumerate; interzicerea explicită a unor astfel de activități în scopul unor obiective specifice interzise; instituirea unor proceduri noi pentru a se asigura că activitățile de colectare de informații de tip SIGINT promovează aceste obiective legitime, și nu alte obiective, interzise; impunerea obligației ca activitățile de colectare de informații de tip SIGINT să fie efectuate numai după ce s-a stabilit, pe baza unei evaluări rezonabile a tuturor factorilor relevanți, că activitățile sunt necesare pentru a promova o prioritate validată în materie de informații și numai în măsura și într-un mod proporțional cu prioritatea validată în materie de informații pentru care au fost autorizate și direcționarea elementelor comunității serviciilor de informații (CI) pentru a-și actualiza politicile și procedurile astfel încât să reflecte garanțiile impuse de ordinul executiv în materie de SIGINT. Cel mai important aspect este faptul că ordinul executiv introduce și un mecanism independent și obligatoriu care permite persoanelor din „statele care îndeplinesc condițiile”, astfel cum au fost desemnate în temeiul ordinului executiv, să solicite reparații în cazul în care consideră că au făcut obiectul unor activități de colectare de informații de tip SIGINT ilegale ale SUA, inclusiv activități care încalcă măsurile de protecție identificate în ordinul executiv.

Emiterea de către Președintele Biden a Ordinului executiv nr. 14086 a marcat încununarea a mai mult de un an de negocieri detaliate între reprezentanți ai Comisiei Europene (CE) și ai Statelor Unite ale Americii și ghidează măsurile pe care le vor lua Statele Unite ale Americii pentru a-și pune în aplicare angajamentele asumate în temeiul Cadrului UE-SUA privind confidențialitatea datelor. În concordanță cu spiritul de cooperare care a produs cadrul, înțeleg că ați primit două seturi de întrebări din partea CE cu privire la modul în care CI va pune în aplicare ordinul executiv. Am plăcerea de a răspunde acestor întrebări prin prezenta scrisoare.

Secțiunea 702 din Legea privind supravegherea activităților străine de spionaj din 1978 (secțiunea 702 din FISA)

Primul set de întrebări se referă la secțiunea 702 din FISA, care permite colectarea de informații operative externe prin vizarea unor persoane care nu sunt cetățeni americani/rezidenți în SUA și despre care se crede în mod rezonabil că se află în afara Statelor Unite ale Americii, cu asistența obligatorie a furnizorilor de servicii de comunicații electronice. Mai precis, întrebările privesc interacțiunea dintre această dispoziție și Ordinul executiv nr. 14086, precum și celelalte garanții care se aplică activităților desfășurate în temeiul secțiunii 702 din FISA.

Pentru început, putem confirma că CI va aplica garanțiile prevăzute în Ordinul executiv nr. 14086 activităților desfășurate în temeiul secțiunii 702 din FISA.

În plus, numeroase alte garanții se aplică utilizării de către guvern a secțiunii 702 din FISA. De exemplu, toate certificările în temeiul secțiunii 702 din FISA trebuie să fie semnate atât de procurorul general, cât și de directorul Serviciului Național de Informații (*Director of National Intelligence* – DNI), iar guvernul trebuie să prezinte toate aceste certificări spre aprobare de către Curtea de Supraveghere a Activităților Străine de Spionaj (*Foreign Intelligence Surveillance Court* – FISC), care este formată din judecători independenți, numiți pe viață, care îndeplinesc un mandat de șapte ani ce nu poate fi reînnoit. Certificările identifică categoriile de informații secrete externe care urmează să fie colectate, care trebuie să corespundă definiției legale a informațiilor operative externe, prin vizarea unor persoane care nu sunt cetățeni americani/rezidenți în SUA despre care se crede în mod rezonabil că se află în afara Statelor Unite ale Americii. Certificările au inclus informații privind terorismul internațional și alte subiecte, cum ar fi obținerea de informații privind armele de distrugere în masă. Fiecare certificare anuală trebuie prezentată FISC spre aprobare într-un pachet de cereri de certificare care include certificările procurorului general și ale DNI, declarații sub jurământ ale unor șefi ai serviciilor de informații, precum și proceduri de vizare, proceduri de minimizare și proceduri de interogare care sunt obligatorii pentru guvern. Procedurile de vizare impun, printre altele, ca CI să evalueze în mod rezonabil, pe baza tuturor circumstanțelor, că vizarea va conduce probabil la colectarea de informații externe identificate într-o certificare în conformitate cu secțiunea 702 din FISA.

În plus, atunci când colectează informații în conformitate cu secțiunea 702 din FISA, CI trebuie: să furnizeze o explicație scrisă a elementelor pe baza cărora evaluează, în momentul vizării, că se preconizează că ținta va deține, va primi sau că este probabil să comunice informațiile operative externe identificate într-o certificare în conformitate cu secțiunea 702 din FISA; să confirme că standardul de vizare, astfel cum este prevăzut în secțiunea 702 din FISA, este în continuare îndeplinit și să înceteze colectarea în cazul în care standardul nu mai este respectat. *A se vedea* documentul prezentat de guvernul SUA Curții de Supraveghere a Activităților Străine de Spionaj, *Sinteza din 2015 a principalelor cerințe în temeiul secțiunii 702*, punctele 2-3 (15 iulie 2015).

Cerința ca CI să înregistreze în scris și să afirme în mod regulat validitatea evaluării sale potrivit căreia obiectivele din secțiunea 702 a FISA îndeplinesc standardele de vizare aplicabile facilitează supravegherea de către FISC a activităților de vizare ale CI. Fiecare evaluare și justificare a vizării înregistrate este revizuită bilunar de către avocații însărcinați cu supravegherea serviciilor de informații din cadrul Departamentului de Justiție (DOJ), care exercită această funcție de supraveghere independent de operațiunile de informații externe. Secțiunea din cadrul DOJ care îndeplinește această funcție are apoi responsabilitatea, în temeiul unei norme FISC stabilite cu mult timp în urmă, de a raporta către FISC orice încălcare a procedurilor aplicabile. Această raportare, împreună cu reuniunile periodice dintre FISC și această secțiune din cadrul DOJ privind supravegherea procedurii de vizare în conformitate cu secțiunea 702 din FISA, permite FISC să asigure respectarea procedurii de vizare conform secțiunii 702 din FISA și a altor proceduri și, în caz contrar, să se asigure că activitățile guvernului sunt legale. În special, FISC poate face acest lucru în mai multe moduri, inclusiv prin emiterea unor decizii de remediere obligatorii pentru sista competența guvernului de a colecta date în raport cu o anumită țintă sau pentru a modifica sau a întârzia colectarea de date conform secțiunii 702 din FISA. De asemenea, FISC poate solicita guvernului să furnizeze rapoarte sau informări suplimentare cu privire la respectarea de către acesta a procedurilor de vizare și a altor proceduri sau poate solicita modificări ale acestor proceduri.

Colectarea SIGINT „în masă”

Al doilea set de întrebări se referă la colectarea SIGINT „în masă”, care este definită prin Ordinul executiv nr. 14086 ca fiind „colectarea autorizată a unor cantități mari de SIGINT care, din motive tehnice sau operaționale, sunt obținute fără a se recurge la factori de diferențiere (de exemplu, fără utilizarea unor identificatori sau a unor termeni de selecție specifici).”

În ceea ce privește aceste întrebări, observăm mai întâi că nici FISA, nici scrisorile privind securitatea națională nu autorizează colectarea în masă. În ceea ce privește FISA:

— Titlurile I și III din FISA, care autorizează supravegherea electronică și, respectiv, percheziții fizice, impun un ordin judecătoresc (cu câteva excepții, de exemplu în situații de urgență) și necesită întotdeauna o cauză probabilă de a crede că ținta este o putere străină sau un agent al unei puteri străine. *A se vedea* titlul 50 articolele 1805, 1824 din U.S.C.

— Legea FREEDOM din 2015 a SUA a modificat titlul IV din FISA, care autorizează utilizarea dispozitivelor de interceptare și de captare și urmărire, în baza unui ordin judecătoresc (cu excepția situațiilor de urgență), pentru a solicita guvernului să își întemeieze cererile pe un „termen de selecție specific”. *A se vedea* titlul 50 articolul 1842 litera (c) punctul 3 din U.S.C.

— Titlul V din FISA, care permite Biroului Federal de Investigații (FBI) să obțină anumite tipuri de documente comerciale, impune emiterea unui ordin judecătoresc pe baza unei cereri în care se precizează că „există fapte specifice și articulabile care susțin convingerea că persoana la care se referă evidențele este o putere străină sau un agent al unei puteri străine." *A se vedea* titlul 50 articolul 1862 litera (b) punctul 2 partea B din U.S.C ([1]).

— În cele din urmă, secțiunea 702 din FISA autorizează „vizarea unor persoane despre care se crede în mod rezonabil că se află în afara Statelor Unite ale Americii, pentru a obține informații operative externe". *A se vedea* titlul 50 articolul 1881a litera (a) din U.S.C. Astfel, după cum a remarcat Consiliul de supraveghere a vieții private și a libertăților civile, colectarea de date de către guvern în temeiul secțiunii 702 din FISA „constă în întregime în vizarea persoanelor fizice și în obținerea de comunicații asociate acestor persoane, de la care guvernul are motive să se aștepte să obțină anumite tipuri de informații externe", astfel încât „programul nu funcționează prin colectarea în masă a comunicațiilor." Consiliul de supraveghere a vieții private și a libertăților civile, *„Raport privind programul de supraveghere care funcționează în conformitate cu secțiunea 702 din Legea privind supravegherea activităților străine de spionaj"* punctul 103 (2 iulie 2014) ([2]).

În ceea ce privește scrisorile privind securitatea națională, Legea FREEDOM din 2015 a SUA impune „un termen de selecție specific" privind utilizarea unor astfel de scrisori. *A se vedea* titlul 12 articolul 3414 litera (a) punctul 2 din U.S.C., titlul 15 articolul 1681u din U.S.C., titlul 15 articolul 1681v litera (a) din U.S.C., titlul 18 articolul 2709 litera (b) din U.S.C.

În plus, Ordinul executiv nr. 14086 prevede că „[c]olectarea direcționată trebuie să aibă prioritate" și că, atunci când CI efectuează colectare în masă, „colectarea în masă a SIGINT este autorizată numai după ce s-a stabilit [...] că informațiile necesare pentru a promova o prioritate validată în materie de informații nu pot fi obținute în mod rezonabil prin colectare țintită." *A se vedea* Ordinul executiv nr. 14086, articolul 2 litera (c) punctul (ii) partea A.

În plus, atunci când CI stabilește că colectarea în masă respectă aceste standarde, Ordinul executiv nr. 14086 prevede garanții suplimentare. În special, ordinul executive impune ca, atunci când efectuează colectare în masă, CI să aplice „metode și măsuri tehnice pentru a limita datele colectate numai la ceea ce este necesar pentru promovarea unei priorități validate în materie de informații, reducând în același timp la minimum colectarea de informații nepertinente". *A se vedea id*. Ordinul precizează, de asemenea, că activitățile de colectare de informații de tip SIGINT, „care includ interogarea informațiilor de tip SIGINT obținute prin colectare în masă, să fie efectuate numai după ce s-a stabilit, pe baza unei evaluări rezonabile a tuturor factorilor relevanți, că activitățile sunt necesare pentru a promova o prioritate validată în materie de informații". *A se vedea id*. articolul 2 litera (a) punctul (ii) partea A. Ordinul pune în aplicare în continuare acest principiu, afirmând că CI poate să efectueze doar interogări nereduse la minimum de SIGINT obținute în masă în vederea atingerii a șase obiective permise și că astfel de interogări trebuie efectuate în conformitate cu politici și proceduri care „iau în considerare în mod corespunzător impactul [interogărilor] asupra vieții private și a libertăților civile ale tuturor persoanelor, indiferent de cetățenie sau de locul de reședință al acestora". *A se vedea id*. articolul 2 litera (c) punctul (iii) partea D. În cele din urmă, ordinul prevede măsuri de control privind gestionarea, securitatea și accesul la datele colectate. *A se vedea id*. articolul 2 litera (c) punctul (iii) partea A și articolul 2 litera (c) punctul (iii) partea B.

* * * * *

Sperăm că aceste clarificări vor fi utile. Vă rugăm să nu ezitați să ne contactați dacă aveți întrebări suplimentare cu privire la modul în care CI SUA intenționează să pună în aplicare Ordinul executiv nr. 14086.

([1]) Din 2001 până în 2020, titlul V din FISA a permis FBI să solicite autorizația FISC pentru a obține „lucruri tangibile" care sunt relevante pentru anumite investigații autorizate. *A se vedea* Legea PATRIOT a SUA, Pub. L. Nr. 107-56, 115 Stat. 272 articolul 215 (2001). Această formulare, care a devenit caducă și, prin urmare, nu mai reprezintă legea, a constituit autoritatea în temeiul căreia guvernul a colectat la un moment dat metadate de telefonie în masă. Cu toate acestea, chiar înainte de expirarea dispoziției, Legea FREEDOM a SUA o modificase pentru a impune guvernului să își întemeieze cererea către FISC pe un „termen de selecție specific". *A se vedea* Legea FREEDOM a SUA, Pub. L. Nr. 114-23, 129 Stat. 268 articolul I 03 (2015).

([2]) Secțiunile 703 și 704, care autorizează CI să vizeze cetățeni americani/rezidenți în SUA situați în străinătate, impun un ordin judecătoresc (cu excepția situațiilor de urgență) și necesită întotdeauna o cauză probabilă de a crede că ținta este o putere străină, un agent al unei puteri străine sau un funcționar sau un angajat al unei puteri străine. *A se vedea titlul 50 articolele* 1881b, 1881c din U.S.C.

Sincerely,

Christopher C. FONZONE
Consilier general

ANEXA VIII

Lista abrevierilor

În prezenta decizie apar următoarele abrevieri:

AAA	American Arbitration Association (Asociația Americană de Arbitraj)
Regulamentul PG	Regulamentul procurorului general de instituire a unei instanțe de reexaminare a protecției datelor
AGG-DOM	Orientările procurorului general cu privire la operațiunile interne ale FBI
APA	Administrative Procedure Act (Legea privind procedura administrativă)
CIA	Central Intelligence Agency
CNSS	Committee on National Security Systems (Comitetul privind sistemele de securitate națională)
Curtea de Justiție	Curtea de Justiție a Uniunii Europene
Decizie	Decizia de punere în aplicare a Comisiei de constatare, în conformitate cu Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului, a nivelului adecvat de protecție a datelor cu caracter personal asigurat de Cadrul UE-SUA privind confidențialitatea datelor
DHS	Department of Homeland Security (Departamentul de Securitate Internă)
DNI	Directorul Serviciului Național de Informații
DoC	Departamentul Comerțului al SUA
DoJ	Departamentul de Justiție al SUA
DoT	Departamentul Transporturilor al SUA
APD	Autoritate pentru protecția datelor
Lista CCD	Lista Cadrului privind confidențialitatea datelor
DPRC	Data Protection Review Court (Curtea de Reexaminare a Protecției Datelor)
ECOA	Equal Credit Opportunity Act (Legea privind egalitatea de șanse în materie de credit)
ECPA	Electronic Communications Privacy Act (Legea privind confidențialitatea comunicațiilor electronice)
SEE	Spațiul Economic European
OE nr. 12333	Ordinul executiv nr. 12333 „United States Intelligence Activities” (Activitățile de colectare de informații ale Statelor Unite ale Americii)
OE nr. 14086, OE	Ordinul executiv nr. 14086 „Enhancing Safeguards for US Signals Intelligence Activities” (Consolidarea garanțiilor pentru activitățile de colectare de informații de tip SIGINT desfășurate de Statele Unite ale Americii)
CCD UE-SUA sau CCD	Cadrul UE-SUA privind confidențialitatea datelor
Comisia de arbitraj CCD UE-SUA	Comisia de arbitraj pentru Cadrul UE-SUA privind confidențialitatea datelor
FBI	Federal Bureau of Investigation (Biroul Federal de Investigații)
FCRA	Fair Credit Reporting Act (Legea privind raportarea echitabilă a creditelor)
FISA	Foreign Intelligence Surveillance Act (Legea privind supravegherea activităților străine de spionaj)
FISC	Foreign Intelligence Surveillance Court (Curtea de Supraveghere a Activităților Străine de Spionaj)
FISCR	Foreign Intelligence Surveillance Court of Review (Curtea de Reexaminare a Supravegherii Activităților Străine de Spionaj)
FOIA	Freedom of Information Act (Legea privind libertatea de informare)
FRA	Federal Records Act (Legea privind registrele federale)

FTC	U.S. Federal Trade Commission (Comisia Federală pentru Comerț din SUA)
HIPAA	Health Insurance Portability and Accountability Act (Legea privind portabilitatea și răspunderea în materie de asigurări de sănătate)
ICDR	International Centre for Dispute Resolution (Centrul Internațional pentru Soluționarea Litigiilor)
IOB	Intelligence Oversight Board (Comitetul pentru supravegherea serviciilor de informații)
NIST	National Institute of Standards and Technology (Institutul Național pentru Standarde și Tehnologie)
NSA	National Security Agency (Agenția Națională de Securitate)
NSL	National Security Letter(s) (scrisori privind securitatea națională)
ODNI	Office of the Director of National Intelligence (Biroul Directorului Serviciului Național de Informații)
ODNI CLPO, CLPO	Civil Liberties Protection Officer of the Director of National Intelligence (responsabilul pentru protecția libertăților civile din cadrul Biroului Directorului Serviciului Național de Informații)
OMB	Office of Management and Budget (Biroul pentru Administrare și Buget)
OPCL	Office of Privacy and Civil Liberties of the Department of Justice (Biroul pentru protecția vieții private și a libertăților civile din cadrul Departamentului de Justiție)
PCLOB	Privacy and Civil Liberties Oversight Board (Comitetul de supraveghere în materie de protecție a vieții private și a libertăților civile)
PIAB	President's Intelligence Advisory Board (Consiliul consultativ privind serviciile de informații al președintelui)
PPD-28	Presidential Policy Directive 28 (Directiva nr. 28 privind politica prezidențială)
Regulamentul (UE) 2016/679	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
SAOP	Senior Agency Official for Privacy (înalt funcționar al agenției pentru protecția vieții private)
Principiile	Principiile Cadrului UE-SUA privind confidențialitatea datelor
SUA	Statele Unite ale Americii
Uniunea	Uniunea Europeană