COMISIA
EUROPEANĂ

Bruxelles, 9.10.2024
COM(2024) 451 final

RAPORT AL COMISIEI CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU

privind prima evaluare periodică a funcționării Deciziei privind caracterul adecvat al nivelului de protecție asigurat de Cadrul UE-SUA privind confidențialitatea datelor

1. PRIMA EVALUARE PERIODICĂ – CONTEXT, PREGĂTIRE ȘI PROCES

În decizia sa din 10 iulie 2023 („Decizia privind caracterul adecvat al nivelului de protecție”), Comisia a constatat nivelul adecvat de protecție pe care Cadrul UE-SUA privind confidențialitatea datelor (CCD) îl oferă atunci când sunt transferate date cu caracter personal din Uniunea Europeană către organizații din Statele Unite ale Americii[1]. Decizia privind caracterul adecvat al nivelului de protecție prevede obligația Comisiei de a efectua evaluări periodice, prima fiind stabilită în termen de 1 an de la data notificării către statele membre a deciziei menționate anterior. Prezentul raport încheie această primă evaluare.

Astfel cum se prevede în considerentul 211 din Decizia privind caracterul adecvat al nivelului de protecție, această primă revizuire/evaluare, care are loc după primul an de funcționare a noului cadru, s-a axat pe a verifica dacă toate elementele prevăzute în cadru au fost puse în aplicare și funcționează în mod eficace. evaluarea a vizat toate aspectele funcționării cadrului, inclusiv având în vedere evoluțiile juridice care au avut loc de la adoptarea Deciziei privind caracterul adecvat al nivelului de protecție.

În etapa de pregătire a evaluării, Comisia a colectat informații de la părțile interesate relevante, în special de la organizațiile neguvernamentale (ONG-uri) cu expertiză în domeniul drepturilor digitale și al vieții private[2], de la organizațiile certificate în domeniul CCD, prin intermediul organismelor lor profesionale[3], precum și de la autoritățile SUA implicate în punerea în aplicare a cadrului. În plus, Comisia a colectat, de asemenea, feedback de la publicul larg prin intermediul unei cereri de contribuții specifice pe portalul „Exprimați-vă părerea”[4].

O reuniune de evaluare a avut loc în Washington D.C. pe 18 și 19 iulie 2024. Aceasta a fost deschisă de Comisarul UE pentru justiție și consumatori, Didier Reynders, și de Secretarul de stat pentru comerț al SUA, Gina Raimondo[5].

În ceea ce privește UE, evaluarea a fost efectuată de reprezentanți ai Direcției Generale Justiție și Consumatori din cadrul Comisiei Europene, împreună cu cinci reprezentanți desemnați de

[1] 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.

[2] Comisia a trimis un chestionar către nouă ONG-uri (Human Rights Watch, American Civil Liberties Union, Consumer Federation of America, Center for Digital Democracy, New America Open Technology Institute, Access Now, Electronic Frontier Foundation, Electronic Privacy Information Center și Center for Democracy and Technology), punând accentul pe evoluțiile relevante ale cadrului juridic al SUA, pe mecanismele de supraveghere și de asigurare a respectării legislației, precum și pe funcționarea mecanismelor de recurs. Serviciile Comisiei și reprezentanții CEPD s-au întâlnit, de asemenea, online cu aceste ONG-uri la 9 iulie 2024.

[3] Comisia a trimis un chestionar către nouă organisme profesionale (Software & Information Industry Association, U.S. Chamber of Commerce, Information Technology Industry Council, the Software Alliance, Centre for Information Policy Leadership, Interactive Advertising Bureau, United States Council for International Business, Computer and Communications Industry Association și Engine), punând accentul pe experiența societăților certificate în domeniul CCD, în special pe procesul de certificare, pe măsurile luate pentru a respecta principiile CCD, mecanismele de soluționare a cererilor și plângerilor din partea persoanelor fizice etc.

[4] Feedbackul primit poate fi consultat la următoarea adresă: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14379-Cadrul-UE-SUA-privind-confidentialitatea-datelor-raportul-Comisiei-referitor-la-functionarea-cadrului_ro.

[5] Reuniunea a fost organizată pe teme, fiecare punct specific de pe ordinea de zi fiind introdus de o scurtă prezentare din partea autorității din SUA, a reprezentantului UE sau a organizației relevante, urmată de o sesiune detaliată de întrebări și răspunsuri. În prima zi s-a discutat despre aspectele comerciale ale cadrului (și anume aplicarea și asigurarea respectării cerințelor aferente societăților certificate în temeiul CCD), iar în a doua zi – despre aspectele legate de accesul autorităților publice la datele cu caracter personal.

Comitetul european pentru protecția datelor (CEPD) și provenind de la diferite autorități naționale pentru protecția datelor (APD) și de la Autoritatea Europeană pentru Protecția Datelor[6]. Din partea SUA au participat reprezentanți ai Departamentului Comerțului (DoC), ai Departamentului de Stat, ai Comisiei Federale pentru Comerț (FTC), ai Departamentului Transporturilor (DoT), ai Biroului Directorului Serviciului Național de Informații (ODNI), ai Departamentului de Justiție (DoJ), ai inspectorului general al Comunității Serviciilor de Informații, precum și membri ai Comitetului de supraveghere în materie de protecție a vieții private și a libertăților civile (PCLOB). În plus, reprezentanții organizațiilor care oferă servicii independente de soluționare a litigiilor și Asociația Americană de Arbitraj au furnizat informații în cursul sesiunilor de evaluare relevante. În continuare, organizațiile certificate în domeniul CCD au prezentat modul în care au respectat cerințele cadrului.

La constatările Comisiei s-au adăugat informațiile furnizate de materialele disponibile pentru publicul larg, cum ar fi hotărâri judecătorești, norme de punere în aplicare și proceduri ale autorităților americane relevante, rapoarte și studii elaborate de organizații neguvernamentale, rapoarte privind transparența întocmite de societățile certificate în domeniul CCD, rapoartele anuale ale organismelor independente de supraveghere, precum și relatări din mass-media.

2. CONSTATĂRI

2.1. Aspecte comerciale

2.1.1. Procesul de certificare

Pentru a putea primi date cu caracter personal transferate din UE pe baza CCD, o societate din SUA trebuie să certifice și apoi să recertifice anual la DoC respectarea cerințelor specifice în materie de protecție a datelor („principiile CCD”). Certificarea impune ca o societate să facă obiectul exercitării competențelor FTC sau DoT în materie de investigare și de asigurare a respectării legislației, să își declare în mod public angajamentul de a respecta principiile CCD, precum și să își facă publică politica de confidențialitate și să pună pe deplin în aplicare aceste cerințe[7]. Înainte de finalizarea unei certificări, DoC verifică dacă societatea a îndeplinit toate cerințele de certificare[8].

În cadrul reuniunii de evaluare, DoC a explicat că, în acest prim an al CCD, accentul s-a pus pe instituirea procesului de certificare, inclusiv pe dezvoltarea de instrumente informatice specifice, pe actualizarea procedurilor, pe colaborarea cu întreprinderile și pe desfășurarea altor activități de informare/sensibilizare. La data reuniunii de evaluare, peste 2 800 de societăți au obținut certificări în domeniul CCD. Aceasta înseamnă că mai multe societăți au obținut certificări în domeniul CCD decât în cadrul anterior, Scutul de confidențialitate, în primul său an de funcționare[9]. Potrivit informațiilor furnizate de DoC, 70 % dintre participanți sunt IMM uri și un număr mare de societăți CCD (47 %) sunt din sectorul tehnologiei, informației și comunicațiilor (TIC). În plus, 60 % dintre societăți sunt certificate exclusiv pentru datele care nu privesc resursele umane, 2,5 % sunt certificate exclusiv pentru datele privind RU, iar

[6] Reprezentanții Comisiei și ai CEPD s-au reunit la 12 iunie și 10 iulie 2024 pentru a pregăti evaluarea, pentru a discuta contribuțiile primite și pentru a identifica aspectele care necesită colectarea de informații și clarificări suplimentare.

[7] Secțiunea I.2 din anexa I la Decizia privind caracterul adecvat al nivelului de protecție.

[8] Anexa III la Decizia privind caracterul adecvat al nivelului de protecție.

[9] În perioada echivalentă, 2 400 de societăți au fost certificate în temeiul Scutului de confidențialitate.

37,5 % sunt certificate atât pentru datele care privesc, cât și pentru cele care nu privesc resursele umane.

DoC a adoptat procedurile necesare pentru tratarea cererilor din partea societăților. Societățile trebuie să își depună cererile de certificare pe site-ul CCD al DoC (https://www.dataprivacyframework.gov/). Acesta conține informații cu privire la modalitățile de aderare la CCD[10] și la obligațiile ce revin societății în temeiul cadrului[11]. O echipă dedicată din cadrul DoC, sub conducerea unui director însărcinat cu Cadrul privind confidențialitatea datelor, este responsabilă de toate aspectele legate de gestionarea și administrarea CCD, inclusiv de procesul de certificare și de monitorizarea conformității. Fiecare cerere este atribuită unui anumit membru al personalului care deține responsabilitatea pentru societatea în cauză pe tot parcursul procesului de certificare.

Pentru a fi certificate în temeiul cadrului, societățile trebuie să depună o cerere care să includă și un proiect de politică de confidențialitate. DoC verifică dacă sunt respectate cerințele relevante ale CCD. Atunci când organizațiile doresc să certifice diferite entități din cadrul unui grup corporativ (de exemplu, filiale diferite), DoC solicită și evaluează fie o singură politică cuprinzătoare de confidențialitate care indică în mod clar toate entitățile care trebuie vizate, fie politici separate pentru fiecare entitate. DoC verifică, de asemenea, prin intermediul mecanismului independent de recurs (IRM)[12] indicat în cerere, dacă organizația figurează ca înregistrată. În ceea ce privește societățile care selectează grupul autorității pentru protecția datelor (de exemplu, pentru că prelucrează date privind resursele umane), DoC verifică dacă societatea a plătit taxele necesare pentru a utiliza grupul. Acolo unde este necesar, DoC verifică, de asemenea, dacă solicitantul se află în sfera de competență a FTC sau DoT (și, prin urmare, este eligibil să adere la CCD).

Dacă sunt îndeplinite toate condițiile, DoC informează organizația că își poate publica politica de confidențialitate referitoare la CCD pe site-ul său web. Odată ce politica de confidențialitate este publică, DoC confirmă certificarea și include societatea de pe lista CCD pe site-ul său web. CCD poate fi utilizat pentru a primi date cu caracter personal din partea UE de la data la care DoC include organizația pe lista respectivă[13].

Astfel cum s-a explicat în cursul reuniunii de evaluare, verificările efectuate de DoC până în prezent au condus la respingerea a 33 de cereri, pe fondul neîndeplinirii cerințelor CCD. În general, DoC colaborează cu societatea pentru a remedia eventualele deficiențe. În cazul în care DoC identifică deficiențe, acesta informează societatea că trebuie să le remedieze și că lipsa unui răspuns într-un anumit termen sau orice altă omisiune de a-și finaliza autocertificarea în conformitate cu procedurile DoC va conduce la concluzia că s-a renunțat la cererea respectivă. În cazul în care certificarea inițială nu este finalizată/modificată în termen de 12 luni, DoC consideră că s-a renunțat la aceasta.

Termenul pentru recertificarea anuală este specificat în lista CCD pentru fiecare societate. Pentru a reaminti întreprinderilor că este necesară solicitarea recertificării, DoC a creat un sistem de înștiințare a faptului că certificarea este pe punctul de a expira. Organizațiile primesc

[10] https://www.dataprivacyframework.gov/program-articles/How-to-Join-the-Data-Privacy-Framework-(DPF)-Program-(part%E2%80%931).

[11] https://www.dataprivacyframework.gov/key-requirements.

[12] Mecanisme de soluționare a litigiilor din sectorul privat prin care plângerile și litigiile fiecărei persoane sunt investigate și soluționate rapid, fără niciun cost pentru persoana în cauză.

[13] Secțiunea I paragraful 3 din anexa I la Decizia privind caracterul adecvat al nivelului de protecție.

o înștiințare cu o lună înainte, apoi cu două săptămâni înainte și apoi cu o zi înainte de data scadenței. Cele care permit expirarea certificării lor sunt eliminate de pe lista CCD. Astfel cum se descrie în anexa III la Decizia privind caracterul adecvat al nivelului de protecție, DoC are o secțiune specifică pe site-ul său web în care sunt enumerate organizațiile din SUA care nu mai sunt participanți activi și în care sunt identificate motivele pentru care (de exemplu, expirarea sau retragerea) societățile în cauză au fost eliminate de pe listă („lista inactivă”). Atunci când organizațiile sunt eliminate de pe lista CCD pentru că au permis expirarea certificării lor, DoC le contactează pentru a confirma dacă doresc să se retragă sau, în schimb, să se recertifice și, în acest din urmă caz, pentru a verifica dacă, în timpul perioadei în care certificarea era expirată, acestea au aplicat principiile CCD în cazul datelor cu caracter personal primite în temeiul CCD și pentru a clarifica măsurile pe care acestea le vor lua pentru a aborda problemele nesoluționate care au determinat întârzierea recertificării. Atunci când întreprinderile notifică DoC că doresc să se retragă din CCD, DoC le solicită să confirme dacă vor returna sau vor șterge datele primite în temeiul CCD; dacă le vor păstra și vor continua să aplice principiile CCD în cazul acestor date (care trebuie să fie confirmate anual); sau dacă le vor păstra și vor institui alte măsuri de protecție (cum ar fi clauzele contractuale standard adoptate de Comisia Europeană).

Feedbackul primit din partea organismelor profesionale și a societăților indică faptul că societățile certificate în domeniul CCD au luat o serie de măsuri pentru a asigura respectarea principiilor CCD. De exemplu, pentru a respecta *principiul existenței unui recurs, al asigurării respectării legislației și al asumării răspunderii*, organizațiile au efectuat verificări interne fie prin autoevaluare, fie prin intermediul unei evaluări externe a conformității. Cele două IRM uri din sectorul privat care au participat la reuniunea de evaluare au explicat că oferă, de asemenea, o evaluare externă a conformității prin evaluarea politicilor de confidențialitate, iar unul dintre IRM-urile din sectorul privat a explicat că oferă, de asemenea, audituri și verificări aleatorii, concentrându-se, de exemplu, pe principiile *accesului*, *alegerii* și *transferului ulterior*. În plus, întreprinderile certificate au elaborat programe interne de asigurare a conformității și mecanisme de supraveghere, au format angajați, au pus în aplicare mecanisme care să le permită persoanelor să își exercite drepturile, au efectuat evaluări ale impactului asupra vieții private și au verificat contractele existente.

2.1.2. Monitorizarea conformității, declarații false de participare și de asigurare a respectării legislației

În temeiul CCD, DoC este responsabil de monitorizarea respectării principiilor CCD prin utilizarea diferitelor instrumente, inclusiv verificări din oficiu (din proprie inițiativă), controale ad-hoc prin sondaj și chestionare de conformitate. Aceasta include căutarea și abordarea declarațiilor false de participare la cadru, de exemplu prin căutări pe internet[14].

Pentru a monitoriza respectarea principiilor de către societățile CCD, DoC s-a bazat în principal pe căutări ad-hoc pe internet și pe verificări (sociale) pe platformele de comunicare în ultimul an. DoC a raportat că nu a detectat probleme de conformitate cu principiile CCD în acest prim an și nu a transmis FTC sau DoT sesizări în privința vreunei societăți pentru eventuale măsuri de asigurare a respectării legislației. De asemenea, a instituit un punct de contact dedicat pentru a facilita cooperarea cu autoritățile pentru protecția datelor și pentru a primi plângeri din partea

[14] A se vedea Anexa III la Decizia privind caracterul adecvat al nivelului de protecție. Declarațiile false pot apărea, de exemplu, atunci când o societate pretinde că participă la CCD și fie nu a inițiat niciodată procesul de certificare, fie l-a inițiat, dar nu l-a dus până la capăt sau a permis expirarea certificării sale.

persoanelor fizice și sesizări din partea altor autorități (de exemplu, APD sau FTC). Cu toate acestea, în ultimul an nu s-au primit sesizări sau plângeri. În timp ce acest prim an de funcționare a CCD s-a axat pe instituirea cadrului și a procesului de certificare, DoC a explicat în cadrul reuniunii de evaluare că intenționează să efectueze verificări ale conformității prin mijloace automatizate pentru a le realiza într-un mod mai sistematic și dezvoltă în prezent instrumentele informatice necesare în acest scop.

Comisia recunoaște că DoC trebuie să își concentreze eforturile în acest prim an asupra instituirii cadrului și a procesului de certificare. În viitor, este important ca DoC să își intensifice eforturile de monitorizare și verificare a respectării principiilor, acest lucru fiind necesar pentru asigurarea unui nivel ridicat continuu de conformitate cu cadrul și pentru detectarea cazurilor care necesită măsuri suplimentare de asigurare a respectării legislației, inclusiv posibile declarații false de participare din partea societăților. În acest sens, Comisia salută faptul că DoC și-a confirmat intenția de a dezvolta și de a utiliza instrumente (automatizate) pentru a identifica într-un mod mai eficace și mai sistematic problemele de conformitate și declarațiile false și este de părere că acest lucru ar trebui să facă parte dintr-un efort mai amplu de a utiliza într-o mai mare măsură diferitele instrumente de care dispune (de exemplu, controale la fața locului, chestionare de examinare a conformității, cereri de informații etc.), inclusiv pentru a verifica conformitatea cu cerințele specifice în temeiul CCD[15].

Organizațiile CCD intră în jurisdicția FTC și DoT. În cursul reuniunii de evaluare, DoT a confirmat că dispune de toate procesele necesare pentru a lua măsuri adecvate de asigurare a respectării legislației. Acesta a explicat totodată că foarte puține societăți aflate sub jurisdicția sa au aderat la CCD (și anume câțiva agenți de bilete, dar nu și companii aeriene). FTC a confirmat că verifică în mod sistematic încălcările CCD în fiecare dintre investigațiile sale privind confidențialitatea. Până în prezent, FTC nu a primit sesizări din partea altor autorități. Comisia a primit câteva plângeri care menționează CCD, deși două dintre acestea vizau societăți aflate pe „lista inactivă”, două vizau societăți care nu participau la cadru, iar una nu se referea la datele cu caracter personal transferate din UE. La momentul redactării prezentului raport, FTC nu emisese decizii de asigurare a respectării CCD, deși a confirmat că mai multe societăți certificate în domeniul CCD fac în prezent obiectul investigației.

Comisia salută faptul că FTC verifică în mod sistematic încălcările CCD în toate investigațiile sale privind confidențialitatea. Întrucât eficacitatea continuă a CCD depinde de aplicarea riguroasă a acestuia, se preconizează că FTC își va exercita în continuare competențele de investigare în temeiul cadrului, inclusiv prin desfășurarea proactivă a unor acțiuni de verificare care să se axeze pe respectarea cerințelor specifice ale CCD și/sau a anumitor sectoare.

2.1.3. Gestionarea plângerilor

CCD oferă persoanelor fizice din UE diferite posibilități de recurs pentru cazurile de nerespectare a principiilor CCD de către organizații certificate[16]. Aceasta include urmărirea rezoluției prin contacte directe cu o organizație CCD, care trebuie să ofere un răspuns persoanei afectate în termen de 45 de zile. De asemenea, persoanele fizice pot depune o plângere la un IRM desemnat de o organizație pentru a investiga și a soluționa plângerile. În funcție de

[15] De exemplu, în ceea ce privește transferurile ulterioare, prin utilizarea posibilității, în temeiul principiului 3 litera (b) din CCD, de a solicita un rezumat sau o copie reprezentativă a dispozițiilor relevante privind confidențialitatea incluse în contractele pentru transferurile ulterioare.

[16] A se vedea secțiunea 2.4 din decizia de inițiere a procedurii.

circumstanțe, aceasta ar putea fi un organism de soluționare alternativă a litigiilor sau o autoritate pentru protecția datelor[17]. În cele din urmă, în cazul în care plângerea persoanei vizate nu a fost soluționată în mod satisfăcător prin niciuna dintre celelalte modalități de recurs disponibile, persoanele fizice pot iniția un arbitraj obligatoriu în fața comisiei de arbitraj CCD UE-SUA ca recurs în „ultimă instanță”.

2.1.3.1. Tratarea plângerilor de către societăți

Răspunsurile primite din partea organismelor profesionale și a societăților la chestionarele trimise de Comisie indică faptul că societățile certificate în domeniul CCD au primit foarte puține plângeri – în cazul în care există – din partea persoanelor fizice cu privire la nerespectarea principiilor CCD. În același timp, societățile au instituit diferite mecanisme și instrumente pentru a le permite persoanelor fizice să își exercite drepturile și să depună plângeri, inclusiv prin formulare online, e-mail și telefon.

2.1.3.2. *Mecanisme independente de recurs (IRM)*

Feedbackul primit în cursul reuniunii și informațiile furnizate de organismele profesionale indică faptul că plângerile adresate mecanismelor independente de soluționare au fost în număr foarte mic. IRM care au fost selectate de societăți includ programele naționale BBB, JAMS, TRUSTe și VeraSafe. CCD impune ca IRM-urile să publice un raport anual cu statistici agregate privind utilizarea serviciilor lor de soluționare a litigiilor. La momentul adoptării prezentului raport, toate IRM vizate și-au publicat rapoartele anuale[18].

În plus, în cadrul reuniunii de evaluare, BBB și VeraSafe și-au prezentat în mod detaliat activitățile desfășurate în ultimul an. Aceștia au raportat o creștere a numărului de participanți din mediul de afaceri care și-au ales serviciile în comparație cu cadrele anterioare și au menționat că au primit unele plângeri, deși acestea erau neeligibile în cea mai mare parte. De exemplu, BBB a primit 87 de plângeri din partea unor persoane fizice din UE, doar două dintre acestea fiind eligibile pentru soluționare. Deși BBB a explicat că plângerile sunt, în medie, prelucrate în 5 zile lucrătoare în general, aceste două plângeri au fost în cele din urmă clasate din cauza lipsei unui răspuns din partea persoanelor fizice. VeraSafe a primit 26 de plângeri, dintre care șase au fost eligibile pentru soluționare. Două dintre acestea – vizând cereri de acces și de ștergere – au fost soluționate, în timp ce două au rămas pendinte, iar două

[17] Organizațiile CCD 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.

[18] ANA - https://www.ana.net/content/show/id/accountability-dpf-consumers;
Programe naționale BBB - https://assets.bbbprograms.org/docs/default-source/eu-privacy-shield/dpf_periodicalreport_072024.pdf; ICDR – AAA - https://go.adr.org/rs/294-SFS-516/images/Data%20Privacy%20Framework%20IRM%20Program%20Report%202023-2024%20FINAL.pdf?version=0;
Asociație de informare (*insights*) - https://www.insightsassociation.org/Portals/INSIGHTS/Insights%20Association%20DPF%20Services%20Program%202024%20Annual%20Report_Final_1.pdf;
JAMS - https://www.jamsadr.com/files/Uploads/Documents/2024-Annual-Report-DPF-Cases.pdf ;
Privacy Trust DPF Services – https://privacytrust.com/fserve/PrivacyTrust_Dispute_Resolution_Report_2023_2024.pdf ;
Mecanismul de soluționare a litigiilor TRUSTe - https://trustarc.com/wp-content/uploads/2024/07/2024-Independent-Recourse-Mechanism-Annual-Report.pdf ;
Verasafe - https://verasafe.com/wp-content/uploads/2020/06/VeraSafe-DPF-Dispute-Resolution-Program-Annual-Report-2024.pdf

au fost fie retrase, fie clasate din cauza lipsei unui răspuns din partea persoanei fizice. Ambele IRM-uri au explicat că urmăresc să răspundă plângerilor în limba vorbită de persoana în cauză.

Societățile CCD care prelucrează date privind resursele umane transferate din UE trebuie să selecteze autoritățile pentru protecția datelor din UE drept IRM pentru datele respective, în timp ce o societate CCD poate selecta, în mod voluntar, autoritățile pentru protecția datelor din UE drept IRM pentru alte tipuri de date cu caracter personal transferate în baza CCD. În fapt, mai mult de jumătate dintre societățile certificate în temeiul CCD la momentul evaluării au optat pentru această soluție[19], ceea ce este binevenit. De la adoptarea Deciziei privind caracterul adecvat al nivelului de protecție, CEPD a adoptat regulamentul de procedură pentru „Comitetul informal al APD din UE". Comitetul are competența de a oferi consiliere obligatorie organizațiilor din SUA în urma plângerilor nesoluționate în domeniul CCD din partea persoanelor fizice cu privire la prelucrarea datelor cu caracter personal care au fost transferate din UE în temeiul CCD. În conformitate cu regulamentul său de procedură, comitetul este format dintr-o APD care acționează în calitate de APD principală și alte APD desemnate pentru a efectua evaluarea în comun[20]. Acesta oferă consiliere obligatorie în termen de 60 de zile de la primirea unei plângeri în domeniul CCD. CEPD a publicat, de asemenea, un model de formular de plângere pentru depunerea plângerilor la autoritățile pentru protecția datelor[21], precum și întrebări frecvente pentru persoanele fizice[22] și întreprinderile[23] europene cu privire la CCD. Comitetul nu primise nicio plângere la momentul evaluării.

2.1.3.3. Mecanismul de arbitraj obligatoriu

Pentru administrarea mecanismului de arbitraj obligatoriu, DoC a selectat Centrul Internațional pentru Soluționarea Litigiilor (*International Centre for Dispute Resolution* – ICDR), care este divizia internațională a Asociației Americane de Arbitraj (*American Arbitration Association*). În urma adoptării Deciziei privind caracterul adecvat al nivelului de protecție, DoC, împreună cu Comisia, a selectat 11 arbitri cu experiență în materie de confidențialitate și din diferite medii, inclusiv arbitrajul, sistemul judiciar, mediul academic și societatea civilă[24]. În plus, au fost adoptate normele de arbitraj[25] pentru comisia de arbitraj CCD și un cod de conduită pentru arbitri[26], toate acestea fiind disponibile pe site-ul ICDR. La momentul evaluării, mecanismul de arbitraj nu fusese încă declanșat de nicio persoană fizică din UE.

2.1.4. Orientare, cooperare și sensibilizare

De la intrarea în vigoare a CCD, DoC a desfășurat diverse activități de sensibilizare prin organizarea de campanii de informare, seminare online și conferințe, stabilind contacte cu

[19] La scurt timp după data reuniunii de evaluare, site-ul CCD a indicat că 1 511 dintre cei 2 892 de participanți dispuneau de o autoritate a UE pentru protecția datelor ca mecanism de recurs.
[20] La 17 aprilie 2024, CEPD a adoptat Regulamentul de procedură pentru „Comitetul informal al APD din UE", în conformitate cu Cadrul UE-SUA privind confidențialitatea datelor. Regulamentul poate fi accesat la adresa: https://www.edpb.europa.eu/system/files/2024-04/dpf_rules-of-procedure_informal-panel-dpas_en.pdf.
[21] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-template-complaint-form_en.
[22] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-individuals_en.
[23] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-businesses_en.
[24] https://go.adr.org/DPF_Arbitrator_Bios.html.
[25] https://go.adr.org/rs/294-SFS-516/images/IC.DR-AAA_EU-US_DPF_AnnexI_Arbitration_Rules.pdf.
[26] https://go.adr.org/rs/294-SFS-516/images/Code_of_Conduct_for_Arbitrators_Appointed_to_EU-US_DPF_AnnexI_Arbitrations.pdf.

organisme profesionale și interacționând în mod direct cu peste 3 000 de societăți pentru a furniza informații cu privire la CCD. De asemenea, a publicat orientări, inclusiv sub formă de întrebări frecvente adresate persoanelor fizice, precum și întreprinderilor din UE și SUA[27]. CEPD a elaborat, la rândul său, formulare de plângere și întrebări frecvente adresate persoanelor fizice și juridice. În mod similar, Comisia a publicat o fișă cu întrebări și răspunsuri și o fișă informativă privind CCD atunci când a adoptat Decizia privind caracterul adecvat al nivelului de protecție[28].

În același timp, în urma reuniunii de evaluare a reieșit că se impune depunerea unor eforturi suplimentare pentru a sensibiliza persoanele fizice și pentru a oferi orientări întreprinderilor. Contribuțiile primite din partea întreprinderilor și a IRM-urilor, precum și numărul foarte scăzut) de plângeri sugerează că este posibil ca persoanele fizice să nu fie întotdeauna conștiente de drepturile lor și/sau de mecanismul de exercitare a acestora. În cursul reuniunii de evaluare, DoC și-a exprimat interesul de a colabora cu autoritățile pentru protecția datelor din UE pentru a spori gradul de conștientizare a cadrului în rândul persoanelor din UE. Comisia încurajează astfel de inițiative și ia totodată măsuri pentru o mai bună informare a persoanelor fizice, inclusiv prin furnizarea de informații suplimentare cu privire la CCD pe site-ul său web, de exemplu prin includerea de linkuri și trimiteri la documentele de orientare relevante adoptate de CEPD, DoC și alte autorități SUA.

În ceea ce privește orientările privind principiile CCD, reprezentanții CEPD au convenit, în cursul reuniunii de evaluare, să coopereze în lunile următoare pentru a oferi clarificări suplimentare cu privire la noțiunea de date privind resursele umane în temeiul CCD și la obligațiile specifice care se aplică prelucrării unor astfel de date. Au fost analizate diferite elemente care trebuie incluse în aceste orientări. De exemplu, aceste orientări ar putea aborda anumite scenarii practice în care datele angajaților ar fi prelucrate în temeiul CCD (de exemplu, de către un furnizor de servicii de cloud) și ar putea explica obligațiile în temeiul CCD care ar fi relevante în cazul unor astfel de scenarii. În plus, acestea ar putea sugera societăților care primesc date privind angajații persoane fizice din UE (dar nu utilizează neapărat astfel de date în contextul unui raport de muncă) să aleagă comitetul APD ca IRM. Acest lucru ar asigura faptul că persoanele respective se pot adresa unei autorități care este „aproape de casă” și, dacă este necesar, este mai familiarizată cu legislația națională aplicabilă datelor privind resursele umane.

În plus, un aspect specific în raport cu care se pare că ar fi utile orientări mai detaliate (și pe baza contribuțiilor primite de la organismele profesionale) se referă la cerințele CCD pentru transferurile ulterioare. Mai mult decât atât, DoC a indicat că ar fi util să se analizeze dacă unele sectoare ar putea beneficia de orientări suplimentare privind aplicarea principiilor CCD în activitățile lor, de exemplu în sfera cercetării în domeniul sănătății și a serviciilor financiare.

Comisia salută disponibilitatea ambelor părți de a elabora orientări și se așteaptă ca lucrările privind subiectele menționate mai sus să înceapă în curând.

La un nivel mai general, au fost instituite o serie de mecanisme pentru a asigura schimburile și cooperarea dintre autoritățile SUA și autoritățile pentru protecția datelor, inclusiv prin

[27] A se vedea, de exemplu, https//www.dataprivacyframework.gov/US-Businesses.
[28] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_ro.

desemnarea unor puncte de contact specifice în cadrul FTC și DoC care să se ocupe de solicitările și sesizările din partea APD.

2.1.5. Evoluții relevante în sistemul juridic al SUA

De la adoptarea Deciziei privind caracterul adecvat al nivelului de protecție, s-au înregistrat o serie de evoluții în cadrul juridic al SUA în domeniul vieții private. Printre acestea se numără evoluțiile în materie de legislație, de reglementare și de jurisprudență. În general, acestea indică o convergență sporită între abordările UE și SUA în ceea ce privește anumite provocări la adresa vieții private, inclusiv prin utilizarea unor concepte juridice similare. Unele dintre aceste evoluții sunt în curs și vor trebui monitorizate în continuare.

La nivel federal, președintele a emis mai multe ordine executive (OE) care sunt relevante pentru utilizarea datelor cu caracter personal. În special, Ordinul executiv 14117 din 28 februarie 2024[29] interzice sau limitează tranzacțiile care implică anumite categorii de date cu caracter personal sensibile (de exemplu, date privind sănătatea, elemente biometrice de identificare, date genomice umane) cu entități din unele „țări care prezintă motive de îngrijorare”[30]. Ordinul adoptat solicită procurorului general să propună regulamente – care urmează să fie emise la momentul adoptării prezentului raport – pentru a detalia punerea sa în aplicare. În plus, Ordinul executiv 14110 din 30 octombrie 2023 privind inteligența artificială[31] se axează pe dezvoltarea unei inteligențe artificiale sigure, securizate și de încredere. Acesta impune mai multor agenții federale să elaboreze standarde și orientări de siguranță legate de IA, inclusiv cu privire la riscurile specifice legate de IA la adresa vieții private și la tehnicile de protecție a vieții private.

În ceea ce privește activitatea legislativă, în timp ce legile federale privind protecția vieții private au fost introduse în Congres în ultimii ani, 20 de state din SUA au adoptat legi cuprinzătoare privind protecția vieții private începând din iulie 2024, dintre care opt au intrat în vigoare: California, Colorado, Oregon, Virginia, Connecticut, Utah, Texas și Florida. În plus, 17 state din SUA au adoptat acte legislative care abordează prelucrarea automată (sau, cel puțin,

[29] https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related.

[30] Printre acestea se numără, astfel cum a propus procurorul general într-o notificare prealabilă privind propunerea de regulament emis la 3 mai 2024, China, Cuba, Hong Kong și Macao, Iran, Coreea de Nord și Venezuela. A se vedea https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and.

[31] https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

unele forme ale acesteia) și permit, în general, renunțarea în cazul anumitor tipuri de decizii bazate pe „crearea de profiluri”[32].

În ceea ce privește evoluția jurisprudenței, mai mulți reprezentanți ai societății civile au subliniat recenta hotărâre a Curții Supreme în cauza *Loper Bright Enterprises/Raimondo* (din 28 iunie 2024). Această hotărâre anulează jurisprudența anterioară privind doctrina *Chevron*, potrivit căreia instanțele aplică principiul deferenței în cazul interpretării rezonabile a legii de către o agenție de reglementare în caz de ambiguitate într-o lege pusă în aplicare de această agenție. În special, unele ONG-uri și-au exprimat îngrijorarea cu privire la impactul acestei hotărâri a Curții Supreme asupra autorității de reglementare a FTC în domeniul vieții private, recunoscând, în același timp, că este posibil să nu existe niciun impact sau să existe un impact limitat asupra competențelor sale de asigurare a respectării legislației. În cadrul reuniunii de evaluare, FTC a informat că este încă prea devreme pentru a se cunoaște implicațiile exacte ale acestei hotărâri. În același timp, aceasta a explicat că elaborarea de norme de către FTC se realizează în temeiul unei competențe prevăzute în Legea privind FTC, diferită de cea a altor agenții administrative și pentru care doctrina *Chevron* este mai puțin relevantă. Prin urmare, hotărârea recentă poate avea un impact limitat în acest domeniu.

În plus, FTC a informat cu privire la evoluțiile recente ale abordării sale privind prelucrarea automată și inteligența artificială. Aceasta include adoptarea unei declarații comune împreună cu alte autorități de aplicare a legii împotriva discriminării și a prejudecăților în sistemele automatizate[33], precum și a mai multor acțiuni de asigurare a respectării legislației – în care FTC se axează, printre altele, pe transparență, pe echitatea prelucrării automate și pe capacitatea persoanelor fizice de a contesta rezultatele. Cazul cel mai important în această privință este decizia FTC împotriva *Rite Aid* din martie 2024, care a impus o interdicție de 5 ani privind utilizarea tehnologiei de recunoaștere facială în scopuri de securitate de către societatea respectivă[34]. În special, FTC a constatat că *Rite Aid* nu a luat măsuri rezonabile pentru a preveni rezultatele eronate și pentru a informa consumatorii cu privire la tehnologia utilizată. La un nivel mai general, în cadrul reuniunii de evaluare, FTC a abordat prioritățile sale actuale și, în special, domeniile în raport cu care consideră că merită ca o abordare mai proactivă în materie de asigurare a respectării legislației să înregistreze progrese. Aceasta include protecția datelor

[32] Deși există diferențe între diferitele state în ceea ce privește noțiunea de „creare de profiluri”, crearea de profiluri este definită, în general, ca orice formă de prelucrare automată a datelor cu caracter personal pentru a evalua, a analiza sau a prevedea aspecte personale referitoare la situația economică, starea de sănătate, preferințele personale, interesele, fiabilitatea, comportamentul, locația sau deplasările unei persoane fizice identificate sau identificabile. Consumatorii sunt, de regulă, cei care pot opta să renunțe la crearea de profiluri. Următoarele state au elaborat acte legislative privind crearea de profiluri: Colorado (Colo. Rev. Stat. Ann. § 6-1-1306), Connecticut (Conn. Gen. Stat. Ann. § 42-518), Delaware (Del. Code Ann. tit. 6, § 12D-104), Florida (Fla. Stat. Ann. § 501.705), Indiana (Ind. Code Ann. § 24-15-3-1), Kentucky (Ky. Rev. Stat. Ann. § 367.3615), Maryland (Legea din 2024 privind confidențialitatea datelor în mediul online din Maryland, adoptată la 9 mai 2024), Minnesota (Minn. Stat. Ann. § 325O.07), Montana (Mont. Code Ann. § 30-14-2808), Nebraska (Neb. Rev. Stat. Ann. § 87-1107), New Hampshire (N.H. Rev. Stat. Ann. § 507-H:4), New Jersey (N.J. Stat. Ann. § 56:8-166.8), Oregon (Or. Rev. Stat. Ann. § 646A.574), Rhode Island (Legea privind protecția confidențialității și transparența datelor din Rhode Island, adoptată la 29 iunie 2024), Tennessee (Tenn. Code Ann. § 47-18-3304), Texas (Tex. Bus. & Com. Code Ann. § 541.051) și Virginia (Va. Code Ann. § 59.1-577).

[33] https://files.consumerfinance.gov/f/documents/cfpb_joint-statement-enforcement-against-discrimination-bias-automated-systems_2023-04.pdf.

[34] https://www.ftc.gov/legal-library/browse/cases-proceedings/2023190-rite-aid-corporation-ftc-v.

sensibile cu caracter personal (de exemplu, date privind sănătatea, date biometrice, geolocalizare)[35], protecția copiilor[36] și a minorilor în mediul online și securitatea datelor[37].

Comisia va continua să urmărească îndeaproape aceste evoluții și alte evoluții din SUA, în special orice măsuri suplimentare în direcția unei legi federale cuprinzătoare privind protecția vieții private și posibilul impact al jurisprudenței recente a Curții Supreme asupra rolului FTC în domeniul vieții private.

Comisia salută informațiile furnizate de FTC cu privire la activitățile sale recente de asigurare a respectării legislației și la prioritățile actuale care corespund în mare măsură tendințelor și priorităților în materie de asigurare a respectării legislației în domeniul protecției datelor în Europa. De asemenea, FTC participă activ la rețeaua care reunește țări ce beneficiază de o decizie a UE privind caracterul adecvat al nivelului de protecție, pe care Comisia a lansat-o în martie 2024[38]. Această convergență sporită ar trebui să încurajeze și să faciliteze o cooperare mai strânsă între autoritățile responsabile cu asigurarea respectării vieții private de ambele părți ale Atlanticului, în special în ceea ce privește aspectele relevante pentru funcționarea CCD.

2.2. Aspecte referitoare la accesarea și utilizarea datelor cu caracter personal transferate în temeiul Cadrului UE-SUA privind confidențialitatea datelor de către autoritățile publice din SUA

Decizia privind caracterul adecvat al nivelului de protecție conține o evaluare detaliată a normelor care reglementează colectarea și utilizarea datelor cu caracter personal transferate din UE către societăți certificate în domeniul CCD de către autoritățile publice din SUA, în special în scopuri de asigurare a respectării dreptului penal și de securitate națională. De la adoptarea Deciziei privind caracterul adecvat al nivelului de protecție, astfel cum a fost confirmată de autoritățile SUA în cursul reuniunii de evaluare, nu au existat evoluții relevante în ceea ce privește cadrul juridic care se aplică accesului la date în scopuri de asigurare a respectării legislației sau de reglementare în primul an al CCD. Din acest motiv, constatările de mai jos se referă numai la evoluțiile din domeniul securității naționale.

Concluziile la care s-a ajuns în Decizia privind caracterul adecvat al nivelului de protecție în ceea ce privește accesul la date al serviciilor de informații se bazează pe analiza condițiilor și a limitărilor care se aplică operațiunilor de colectare a informațiilor de tip SIGINT în cadrul mai multor autorități juridice relevante – în special articolul 702 din Legea privind

---

[35] A se vedea, de exemplu, Ordinul recent al FTC împotriva X-Mode privind vânzarea și partajarea de informații sensibile de localizare (https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf) și împotriva Monument privind divulgarea de date sensibile privind starea de sănătate către părți terțe în scopuri de marketing (https://www.ftc.gov/system/files/ftc_gov/pdf/MonumentOrderFiled.pdf).

[36] De exemplu, FTC a anunțat recent o anchetă care a condus la un proces împotriva TikTok și a societății-mamă a acestuia, ByteDance, pentru presupusa încălcare a legislației privind viața privată a copiilor. Se susține că niciuna dintre cele două societăți nu a respectat cerința de a notifica și de a obține acordul părinților înainte de a colecta și de a utiliza informații cu caracter personal de la copiii cu vârsta sub 13 ani (https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law).

[37] A se vedea prezentarea generală a activităților recente în materie de asigurare a respectării legislației din „*The FTC 2023 Privacy and Data Security Update*” (Actualizarea FTC din 2023 privind confidențialitatea și securitatea datelor). https://ec.europa.eu/commission/presscorner/detail/en/mex_24_1307.

[38] A se vedea https://ec.europa.eu/commission/presscorner/detail/en/mex_24_1307. În urma reuniunii din martie 2024, s-a decis organizarea unei serii de sesiuni tematice. Prima a avut loc în iulie 2024 și s-a axat pe dezvoltarea de instrumente care pot sprijini întreprinderile mici și mijlocii în ceea ce privește respectarea legislației privind protecția vieții private.

supravegherea activităților străine de spionaj (FISA) și Ordinul executiv nr. 12333[39] – astfel cum au fost completate și consolidate prin Ordinul executiv nr. 14086 privind consolidarea garanțiilor pentru activitățile de colectare de informații de tip SIGINT desfășurate de Statele Unite ale Americii (OE nr. 14086), adoptat de președintele SUA la 7 octombrie 2022. Garanțiile prevăzute în OE nr. 14086 se aplică tuturor activităților de colectare de informații de tip SIGINT desfășurate de Statele Unite ale Americii, indiferent de competența juridică pe care se bazează aceste activități și de locul în care se desfășoară și protejează datele persoanelor care nu sunt cetățeni americani/rezidenți SUA (inclusiv ale europenilor)[40]. OE nr. 14086 a instituit, de asemenea, un nou mecanism de recurs prin care aceste garanții obligatorii pot fi invocate și puse în aplicare de către persoane din UE.

Următoarele secțiuni descriu măsurile luate de autoritățile SUA de la adoptarea Deciziei privind caracterul adecvat al nivelului de protecție pentru a se conforma OE nr. 14086, precum și evoluțiile relevante în ceea ce privește cadrul juridic menționat anterior.

2.2.1. Evoluții relevante în ceea ce privește cadrul juridic al SUA

2.2.1.1. Punerea în aplicare a Ordinului executiv nr. 14086 de către serviciile de informații

Limitările și garanțiile introduse prin OE nr. 14086 le completează pe cele prevăzute în articolul 702 din FISA și OE nr. 12333. Acestea sunt obligatorii pentru toate serviciile de informații și au fost operaționalizate în continuare prin politici și proceduri adoptate de fiecare serviciu.

În cadrul primei reexaminări, autoritățile SUA au confirmat că nu au existat modificări ale OE nr. 14086 de la adoptare. În plus, s-a clarificat faptul că președintele SUA nu a făcut uz de competența prevăzută la articolul 2 litera (b) punctul (i) subpunctul (B) și la articolul 2 litera (b) punctul (ii) litera (C) din OE nr. 14086 pentru a actualiza lista obiectivelor legitime care pot fi urmărite prin sistemul de colectare a informațiilor de tip SIGINT sau lista scopurilor în care pot fi utilizate datele colectate în masă[41]. Pentru a stabili priorități mai specifice în materie de informații pentru care pot fi efectiv colectate informații de tip SIGINT, OE nr. 14086 a instituit o procedură specifică. În special, responsabilul pentru protecția libertăților civile din cadrul ODNI (CLPO ODNI) trebuie consultat pentru a evalua, pentru fiecare prioritate, dacă (1) promovează unul sau mai multe obiective legitime enumerate în OE; (2) aceasta nu a fost concepută pentru colectarea de informații pe baza semnalelor electromagnetice pentru un obiectiv interzis enumerat în ordinul executiv și nici nu ar trebui să aibă ca rezultat 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[42]. În cursul reuniunii de evaluare, CLPO ODNI a

[39] Alte măsuri care pot fi luate în temeiul FISA în ceea ce privește datele transferate din UE sunt supravegherea electronică individualizată (articolul 105 din FISA), percheziții fizice (articolul 302 din FISA), utilizarea dispozitivelor de interceptare și de captare și urmărire (articolul 402 din FISA) și colectarea documentelor comerciale de la anumite societăți (transportatori comuni, unități publice de cazare, unități de închiriere de vehicule sau unități de depozitare, articolul 501 din FISA). Aceste temeiuri juridice diferite sunt analizate în detaliu în Decizia privind caracterul adecvat al nivelului de protecție (considerentele 142-152).

[40] Pentru informații suplimentare, a se vedea secțiunea 3.2.1.2 din Decizia privind caracterul adecvat al nivelului de protecție.

[41] Aceste obiective/scopuri legitime includ, de exemplu, protecția împotriva spionajului, a sabotajului, a asasinatelor sau a altor activități ale serviciilor de informații desfășurate de către sau în numele ori cu sprijinul unui guvern, al unei organizații sau al unei persoane străine; 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.

[42] Articolul 2 litera (b) punctul (iii) din OE nr. 14086.

confirmat că a verificat prioritățile propuse de directorul Serviciului Național de Informații în Cadrul național privind prioritățile în materie de informații din 2023, a concluzionat că acestea respectă cerințele de mai sus și a împărtășit concluzia sa directorului Serviciului Național de Informații (DNI), care, la rândul său, a prezentat președintelui prioritățile în vederea validării. CLPO ODNI a oferit, de asemenea, formare cu privire la cerințele OE nr. 14086 unor părți ale Comunității Serviciilor de Informații implicate în dezvoltarea priorităților în materie de informații.

În plus, autoritățile SUA au luat măsuri practice suplimentare în ultimul an pentru a pune în aplicare OE nr. 14 086 în operațiunile lor de zi cu zi. În special, serviciile de informații au instituit politici și orientări interne suplimentare privind aplicarea OE, de exemplu procese interne (prin cerințe interne de autorizare, controale documentate ale accesului, astfel încât numai persoanele care au fost instruite în mod corespunzător și care au cerințele de misiune necesare au acces la informații etc.) pentru a se asigura că cerințele în materie de necesitate și proporționalitate sunt respectate atât în contextul colectării direcționate, cât și al colectării în masă[43]. În plus, personalul din cadrul diverselor servicii de informații (de exemplu, NSA, CIA, FBI) a beneficiat de formare cu privire la OE nr. 14086, inclusiv de sesiuni de formare anuale și ad-hoc organizate de CLPO ODNI și de cursuri de formare obligatorii pentru toți noii membri ai personalului care se alătură ODNI.

Comisia salută diferitele măsuri instituite pentru punerea în aplicare și asigurarea conformității cu OE nr. 14086. Întrucât se câștigă din ce în ce mai multă experiență odată cu aplicarea practică a garanțiilor OE, Comisia ar aprecia oportunitatea de a discuta exemple concrete privind modul în care OE este aplicat în practică (respectând în același timp considerentele în materie de confidențialitate aplicabile) în evaluările viitoare.

2.2.1.2. Reautorizarea articolului 702 din FISA

Articolul 702 din FISA permite 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 pentru a obține informații operative externe. Achiziția are loc pe baza unor certificări anuale prezentate Curții de Supraveghere a Activităților Străine de Spionaj (FISC) și aprobate de aceasta. Aceste certificări identifică categorii specifice de informații operative externe care trebuie colectate. La 21 iulie 2023, ODNI a anunțat că există trei certificări aprobate în temeiul articolului 702 din FISA, care acoperă următoarele categorii de informații externe: (1) guverne străine și entități conexe, (2) combaterea terorismului și (3) combaterea proliferării[44]. Certificările trebuie, de asemenea, să includă proceduri de vizare și de minimizare care sunt aprobate de FISC[45]. În special, vizarea este efectuată prin solicitarea ca societățile din SUA care îndeplinesc definiția FISA a „furnizorului de servicii de comunicații electronice” să divulge datele transmise în cadrul comunicațiilor electronice pentru comunicațiile trimise către sau de la „termeni de selecție”, care identifică un cont specific de comunicare, de exemplu un număr de telefon sau o adresă de e-mail. Guvernul SUA a publicat o serie de materiale privind

[43]A se vedea https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguardsin-executive-order-14086, publicat la 3 iulie 2023.

[44] https://www.intelligence.gov/ic-on-the-record-database/results/1307-release-of-documents-related-to-the-2023-fisa-section-702-certifications.

[45] Astfel de proceduri limitează colectarea datelor cu privire la un scop specific legat de obținerea de informații externe, restricționează accesul la bazele de date în care sunt stocate informațiile obținute în temeiul articolului 702 din FISA (inclusiv prin controale de acces) și impun limite privind utilizarea, păstrarea și diseminarea unor astfel de informații.

articolul 702 din FISA pentru a informa publicul cu privire la funcționarea programelor de supraveghere, la cerințele aplicabile și la protecția vieții private, precum și cu privire la rolul FISC[46].

Pe fondul unei clauze de încetare a efectelor, articolul 702 din FISA urma să expire la sfârșitul anului 2023, cu excepția cazului în care era reautorizată de Congres. După o reautorizare temporară fără modificări, Congresul a adoptat Legea privind reforma serviciilor de informații și a securității în America (*Reforming Intelligence and Securing America Act* – RISAA) la 19 aprilie 2024, reactivând articolul 702 din FISA pentru o perioadă de 2 ani și introducând mai multe modificări. În linii mari, acestea pot fi împărțite în două categorii: (1) modificări ale domeniului de aplicare al activităților de supraveghere permise în temeiul articolului 702 din FISA și (2) modificări instituționale și procedurale.

Modificări ale domeniului de aplicare al activităților de supraveghere permise în temeiul articolului 702 din FISA

RISAA a introdus trei modificări principale ale domeniului de aplicare al activităților de supraveghere care pot fi desfășurate în temeiul articolului 702 din FISA.

În primul rând, colectarea „informațiilor despre” a fost interzisă definitiv[47]. Aceasta se referă la colectarea de comunicări în cazul cărora termenul de selecție prevăzut în articolul 702 (cum ar fi o adresă de e-mail) nu este de forma „către” sau „de la” în cadrul comunicărilor, ci conține mai degrabă o trimitere la un astfel de termen de selecție în comunicare (de exemplu, comunicările prin e-mail care nu sunt trimise către sau de la adresa de e-mail selectată, ci includ adresa de e-mail selectată în textul sau în cuprinsul e-mailului). Deși o astfel de colectare a fost deja exclusă în urma unei modificări a FISA în 2018, FISA a prevăzut în continuare posibilitatea de a reîncepe colectarea „informațiilor despre” în viitor, în urma unei proceduri specifice de autorizare care implică FISC și Congresul. Cea mai recentă modificare introdusă de RISAA a eliminat această posibilitate.

În al doilea rând, definiția informațiilor operative externe a fost extinsă pentru a include informații referitoare la combaterea drogurilor[48]. În cursul reuniunii de evaluare, autoritățile SUA au explicat că aceasta a fost introdusă având în vedere actuala criză de fentanil și amenințarea tot mai mare la adresa securității naționale din partea traficanților și producătorilor internaționali de stupefiante. În acest context, s-a confirmat că această noțiune se încadrează în mai multe dintre obiectivele legitime enumerate în OE nr. 14086, și anume înțelegerea sau evaluarea capacităților, intențiilor sau activităților organizațiilor străine care reprezintă o amenințare actuală sau potențială la adresa securității naționale a SUA sau a aliaților săi; înțelegerea sau evaluarea amenințărilor transnaționale care au un impact asupra securității globale, inclusiv a riscurilor pentru sănătatea publică și protecția împotriva amenințărilor infracționale transnaționale[49].

În al treilea rând, RISAA a extins definiția „furnizorului de servicii de comunicații electronice” (ECSP), extinzând astfel obiectul de activitate al întreprinderilor care pot fi obligate să furnizeze informații în temeiul articolului 702 din FISA[50]. Definiția include în prezent alți furnizori de servicii care au „acces la echipamente care sunt sau pot fi utilizate pentru a

[46] https://www.intel.gov/foreign-intelligence-surveillance-act.
[47] Articolul 22 din RISAA.
[48] Articolul 23 din RISAA.
[49] Articolul 2 litera (b) punctul (ii) partea A alineatele (2), (3) și (10) din OE nr. 14086.
[50] Articolul 25 din RISAA.

transmite sau a stoca comunicații telefonice sau electronice", excluzând în mod explicit unități publice de cazare, locuințe, infrastructuri comunitare și unități de servicii alimentare. Într-o scrisoare adresată Congresului, DoJ a menționat această modificare ca fiind o modificare tehnică menită să acopere un număr „extrem de mic" de societăți tehnologice care, în conformitate cu deciziile recente ale FISC și ale Curții de Reexaminare a Supravegherii Activităților Străine de Spionaj (FISCR), nu au fost incluse în definiția anterioară a ECSP[51]. În aceeași scrisoare, DoJ s-a angajat să restrângă domeniul prin aplicarea acestei definiții exclusiv pentru a acoperi tipul de prestator de servicii în cauză în litigiul care a condus la decizia FISC. În consecință, societățile vizate sunt menționate într-o anexă clasificată pentru Congres. Mai multe ONG-uri, inclusiv cele care au furnizat feedback în cadrul evaluării, și-au exprimat îngrijorarea cu privire la această extindere, susținând că aceasta ar putea acoperi numeroase întreprinderi din SUA (întrucât multe dintre acestea furnizează un anumit tip de servicii și au acces la echipamente de comunicații). Având în vedere aceste preocupări, a fost propusă o nouă modificare cu sprijinul Comunității Serviciilor de Informații într-un proiect de lege privind autorizarea serviciilor de informații pentru anul fiscal 2025, care se află în prezent în dezbaterea Congresului. Dacă ar fi adoptată de Congres, această modificare ar asigura faptul că societățile suplimentare incluse în definiția ECSP ar fi limitate numai la cele menționate în hotărârile FISC menționate mai sus. Proiectul de lege prevede, de asemenea, că fiecare directivă adresată unei astfel de societăți ar trebui să fie raportată către FISC, pentru a permite acesteia din urmă să verifice dacă societatea ar intra într-adevăr în domeniul de aplicare. În scrisoarea sa adresată Congresului, DoJ s-a angajat să raporteze Congresului o dată la șase luni cu privire la orice aplicare a definiției actualizate, pentru a permite Congresului să exercite supravegherea adecvată în ceea ce privește aplicarea restrictivă a definiției.

Este important de remarcat faptul că, în cadrul reuniunii de evaluare desfășurate de autoritățile SUA și de PCLOB, s-a confirmat că toate garanțiile prevăzute de OE nr. 14086 continuă să se aplice pe deplin colectării și utilizării tuturor datelor în temeiul articolului 702 din FISA, inclusiv în urma acestor modificări. Astfel, deși RISAA extinde într-o oarecare măsură sfera întreprinderilor care pot primi un ordin, aceasta nu limitează exercitarea drepturilor. Cu toate acestea, monitorizarea evoluțiilor ulterioare (legislative și de raportare) și primirea informațiilor cu privire la aplicarea în practică a acestor noi norme vor avea un caracter important. Aceasta include, de exemplu, impactul extinderii definițiilor informațiilor externe și ale ECSP asupra numărului de obiective prevăzute în articolul 702 din FISA (astfel cum au fost comunicate anual de ODNI, a se vedea mai jos privind transparența). Viitorul raport de monitorizare a recentului raport PCLOB privind articolul 702 din FISA (a se vedea mai jos) ar trebui să aibă un caracter deosebit de informativ în această privință.

Modificări instituționale și procedurale

În ceea ce privește modificările instituționale și procedurale, RISAA a codificat mai multe proceduri care au fost deja urmate în practică și a introdus noi garanții. În timp ce unele dintre acestea se referă numai la persoane din SUA, mai multe modificări sporesc nivelul de protecție atât pentru cei care sunt, cât și pentru cei care nu sunt cetățeni americani/rezidenți SUA, ale

[51] https://www.justice.gov/opa/media/1348621/dl?inline. A se vedea hotărârea FISC din 2022 (https://www.intel.gov/assets/documents/702%20Documents/declassified/2022-FISC-ECSP-OPINION.pdf) și hotărârea Curții de Reexaminare a Supravegherii Activităților Străine de Spionaj prin care se confirmă această decizie (https://www.intel.gov/assets/documents/702%20Documents/declassified/2023_FISC-R_ECSP_Opinion.pdf).

căror date pot fi colectate în temeiul articolului 702 din FISA[52] și, prin urmare, sunt relevante pentru funcționarea CCD.

În primul rând, au fost instituite o serie de cerințe suplimentare în materie de responsabilitate, supraveghere și raportare. În special, personalul FBI trebuie acum să fie instruit anual cu privire la normele care se aplică interogării informațiilor obținute în temeiul articolului 702 din FISA[53]. FBI are, de asemenea, obligația de a raporta Congresului cu privire la activitățile sale de interogare (de exemplu, numărul de interogări care utilizează „tehnologii pentru ocuparea unui loc de muncă pe loturi", adică utilizarea mai multor termeni de interogare ca parte a unei singure interogări) și cu privire la măsurile de responsabilizare instituite pentru a asigura conformitatea cu cerințele legale în materie de interogare (articolele 11-12 din RISAA). În plus, inspectorul general al DoJ este însărcinat să elaboreze un raport privind conformitatea FBI cu cerințele în materie de interogare (articolul 9 din RISAA). La un nivel mai general, pentru a spori transparența procedurilor în fața FISC, ODNI și procurorul general au acum obligația de a finaliza analiza de declasificare a deciziilor FISC în termen de 180 de zile (articolul 7 din RISAA). În plus, transcrierile tuturor audierilor în fața FISC și a Curții de Reexaminare a Supravegherii Activităților Străine de Spionaj (FISCR, unde deciziile FISC pot fi atacate) trebuie păstrate și transmise Congresului (articolul 8 din RISAA).

În al doilea rând, RISAA a introdus limitări suplimentare privind utilizarea de către FBI a datelor colectate în temeiul articolului 702 din FISA. Articolul 2 litera (d) din RISAA prevede că o interogare care utilizează „tehnologia pe loturi" poate fi efectuată numai după obținerea aprobării din partea unui avocat din cadrul FBI, cu excepția cazului în care există circumstanțe urgente. În plus, FBI are acum interdicția de a verifica automat informațiile nereduse la minimum obținute în temeiul articolului 702 din FISA și, în schimb, trebuie să se asigure că analiștii trebuie să aleagă în mod afirmativ pentru a efectua căutări pe baza unor astfel de informații. RISAA a interzis, de asemenea, FBI să efectueze interogări care sunt concepute exclusiv pentru a găsi și a extrage probe privind o activitate infracțională (cu excepția cazului în care există convingerea rezonabilă că acestea ar putea contribui la atenuarea sau eliminarea unei amenințări la adresa vieții sau a vătămării corporale grave sau, dacă este necesar, pentru a respecta obligațiile de divulgare în cadrul litigiilor)[54]. În plus, FBI are interdicție de a introduce date nereduse la minimum în registre analitice, cu excepția cazului în care persoana vizată este relevantă pentru o investigație de securitate națională existentă[55].

În al treilea rând, anumite dispoziții referitoare la statutul și la rolul *amici curiae* în fața FISC au fost modificate[56]. *Amici* sunt desemnați ca experți pentru a asista Curtea (și FISCR) în chestiuni legate de viața privată și libertățile civile sau pentru a contribui la clarificarea

[52] În plus, RISAA a introdus unele modificări în ceea ce privește supravegherea electronică individualizată tradițională în temeiul articolului 105 din FISA (pe baza mandatului FISC emis în cazul în care se respectă un standard de cauză probabilă). O cerere depusă de un serviciu de informații la procurorul general pentru un ordin de efectuare a supravegherii electronice individualizate necesită în prezent o declarație pe proprie răspundere care să justifice convingerea că sunt îndeplinite condițiile prevăzute la articolul 105 din FISA [articolul 6 litera (a) din RISAA]. Durata posibilă a supravegherii electronice în ceea ce privește puterile străine sau agenții puterilor străine a fost prelungită de la 120 de zile la 1 an [articolul 6 litera (g) din RISAA].

[53] Articolul 2 litera (d) din RISAA.

[54] Articolul 3 litera (a) din RISAA.

[55] Articolul 3 litera (b) din RISAA. Dacă este necesar pe fondul unor circumstanțe urgente, directorul FBI poate decide cu privire la o excepție de la această dispoziție, care trebuie notificată Congresului.

[56] Din motive de claritate, aceste modificări nu afectează statutul și rolul avocaților speciali în fața DPRC, astfel cum a confirmat SUA în cadrul reuniunii de evaluare.

aspectelor tehnologice atunci când tratează o anumită cerere din partea unui guvern. Deși FISA impunea anterior ca *amici* să aibă expertiză în ceea ce privește viața privată și libertățile civile, colectarea de informații, tehnologia comunicațiilor sau alte domenii relevante, în prezent este nevoie, în principiu, de expertiză în ceea ce privește viața privată/libertățile civile și colectarea de informații. Curtea a avut deja posibilitatea de a numi un *amicus* în orice caz pe care îl considera adecvat, având obligația de a acționa în acest sens în condițiile în care se confruntă cu o interpretare nouă sau semnificativă a legii. În urma reautorizării, FISC trebuie acum să numească un *amicus* de fiecare dată când i se solicită aprobarea unei certificări în temeiul articolului 702 din FISA și a procedurilor aferente (de exemplu, proceduri de vizare), cu excepția cazului în care constată că acest lucru nu ar fi adecvat sau ar conduce probabil la întârzieri nejustificate[57]. În plus, în loc să numească doar unul, Curtea poate decide acum să numească unul sau mai mulți *amici*. De asemenea, se clarifică faptul că informațiile care urmează să fie furnizate de *amici* trebuie „să se limiteze la abordarea problemelor specifice identificate de instanță”, deși domeniile în care *amici* pot prezenta observații au rămas largi (și anume argumente juridice și informații legate de protecția vieții private și a libertăților civile ale persoanelor din Statele Unite, colectarea de informații și tehnologia comunicațiilor sau orice alt domeniu relevant).

În cele din urmă, articolul 18 din RISAA instituie o Comisie de reformă a FISA – formată, printre altele, din membri ai Congresului, președintele PCLOB, directorul adjunct principal al Serviciului Național de Informații și Procurorul General adjunct, precum și din alți membri care urmează să fie numiți de Congres[58] – pentru a recomanda reforme suplimentare ale FISA.

Comisia va monitoriza îndeaproape evoluțiile ulterioare în ceea ce privește articolul 702 din FISA, inclusiv în contextul activităților de supraveghere ale PCLOB (a se vedea mai jos), al activității Comisiei pentru reformă și al viitoarei evaluări a FISA după 2 ani.

2.2.1.3. Activități de supraveghere în practică: cifre și tendințe

Raportul anual al ODNI privind transparența statistică referitor la utilizarea de către comunitatea serviciilor de informații a autorităților de supraveghere a securității naționale pentru anul calendaristic 2023 (publicat în aprilie 2024)[59] arată că numărul obiectivelor prevăzute în articolul 702 din FISA a crescut de la 245 073 în anul calendaristic 2022 la 268 590 în anul calendaristic 2023. Raportul explică faptul că fluctuațiile numărului de obiective pot fi legate de o varietate de motive, inclusiv modificări ale priorităților operaționale, evenimente mondiale, capacități tehnice, comportamente-țintă și schimbări în sectorul telecomunicațiilor. Raportul indică, de asemenea, că nicio persoană care nu este cetățean american/rezident în SUA (comparativ cu 1 în 2021 și 0 în 2022) nu a fost vizată în temeiul articolului 402 din FISA (interceptare și capturare și trasabilitate), în timp ce șase ordine (comparativ cu 11 ordine atât în 2021, cât și în 2022), pentru șase obiective (comparativ cu 13 în 2021 și 11 în 2022), au fost emise în temeiul articolului 501 din FISA (accesul la documentele comerciale ale transportatorilor comuni, la unitățile de închiriere de vehicule sau la unitățile de depozitare fizică), care acoperă 5 412 identificatori unici (față de 23 157 în 2021 și 55 431 în 2022) utilizați pentru a comunica informațiile colectate în temeiul unor astfel de ordine.

Raportul anual al DoJ către Congres referitor la Legea privind supravegherea activităților străine de spionaj indică faptul că, în cursul anului calendaristic 2023, au fost depuse 327 de

[57] Articolul 5 litera (b) din RISAA.
[58] Articolul 18 prevede în mod specific reprezentarea din afara Congresului.
[59] https://www.dni.gov/files/CLPT/documents/2024_ASTR_for_CY2023.pdf.

cereri la FISC pentru a efectua supravegherea electronică și/sau percheziții fizice în scopuri legate de obținerea de informații externe în temeiul articolului 105 și, respectiv, al articolului 302 din FISA[60]. Numărul total de persoane vizate a fost cuprins între 500 și 999. În ceea ce privește scrisorile privind securitatea națională (NSL), raportul prevede că 10 115 cereri (excluzând doar cererile de informații privind abonații) au fost emise pentru informații privind persoanele care nu sunt cetățeni americani/rezidenți în SUA, solicitând informații referitoare la 3 033 de persoane diferite care nu sunt cetățeni americani/rezidenți în SUA[61].

Mai multe societăți certificate în domeniul CCD (de exemplu, Google, Meta) utilizează posibilitatea prevăzută în legislația SUA de a publica rapoarte privind transparența care să informeze cu privire la numărul de cereri FISA și NSL pe care le-au primit în cursul unei anumite perioade de raportare. La momentul redactării prezentului raport, statisticile privind cererile FISA după iulie 2023 nu erau încă disponibile. Google a raportat, de exemplu, că a primit între 500 și 999 de cereri NSL, afectând între 2 000 și 2 499 de conturi, în perioada iulie decembrie 2023[62]. Meta a raportat că a primit între 0 și 499 de cereri NSL, afectând între 500 și 999 de conturi, în aceeași perioadă de raportare[63]. Cifrele au rămas relativ stabile în ultimii ani. Pentru a spori și mai mult transparența, unele societăți (de exemplu, Google) publică în mod proactiv NSL primite după ridicarea restricțiilor de nedivulgare[64].

2.2.1.4. Alte evoluții

În contextul pregătirii evaluării, o serie de ONG-uri au formulat întrebări cu privire la noile forme de achiziție de date de către serviciile de informații din SUA prin achiziționarea de date de la entități comerciale, în special de la brokeri de date. Acestea au explicat că, deși datele colectate pe această bază trebuie să fie prelucrate în continuare în conformitate cu alte cerințe, inclusiv, de exemplu, în temeiul OE nr. 12333[65], o astfel de achiziție are loc în afara cadrului FISA și OE nr. 14086.

În acest sens, ar trebui reamintit faptul că orice tip de partajare voluntară de date cu părți terțe face obiectul mai multor condiții detaliate în cadrul CCD. În primul rând, organizația certificată nu poate face schimb de date cu o parte terță (care nu acționează în calitate de agent/persoană împuternicită de operator) fără a informa și a alege persoanele în cauză[66]. În al doilea rând, în conformitate cu *principiul responsabilității pentru transferurile ulterioare*, transferurile ulterioare pot fi efectuate numai (1) în scopuri limitate și specificate, (2) pe baza unui contract încheiat între organizația CCD UE-SUA și partea terță și (3) numai în cazul în care contractul respectiv îi impune părții terțe în cauză să asigure același nivel de protecție precum cel garantat de principii[67].

---

[60] https://www.justice.gov/nsd/media/1350236/dl?inline.

[61] Aceste cifre s-au menținut în mare parte la un nivel stabil în comparație cu anul de raportare precedent (2022). Prin comparație, în 2022 au existat 317 cereri finale depuse la FISC pentru a efectua supravegherea electronică și/sau percheziții fizice în scopuri legate de obținerea de informații externe. Numărul total de persoane vizate de ordinele de supraveghere electronică a fost cuprins între 0 și 499. FBI a formulat 9 103 cereri de informații NSL privind persoane care nu sunt cetățeni americani/rezidenți în SUA în 2022 (cu excepția cererilor de informații privind abonații). Sursă: https://irp.fas.org/agency/doj/fisa/2022rept.pdf

[62] https://transparencyreport.google.com/user-data/us-national-security.

[63] https://transparency.meta.com/reports/government-data-requests/country/US/.

[64] https://transparencyreport.google.com/user-data/us-national-security.

[65] A se vedea, de exemplu, articolul 2.4 din OE nr. 12333 privind tehnicile de colectare.

[66] A se vedea considerentul 40 din decizia de inițiere a procedurii.

[67] A se vedea considerentul 38 din decizia de inițiere a procedurii.

În plus, astfel cum s-a discutat și în cadrul reuniunii de evaluare, FTC a luat măsuri de asigurare a respectării legislației împotriva brokerilor de date care vând date sensibile privind consumatorii. De exemplu, într-o cauză împotriva *X-Mode* și a succesorului său *Outlogic*, FTC a adoptat, la 9 ianuarie 2024, un ordin prin care interzice societății să vândă date de geolocalizare unor părți terțe și să șteargă datele pe care le-a utilizat și le-a partajat în mod ilegal. Ancheta FTC a constatat, printre altele, că societatea nu a informat pe deplin persoanele fizice cu privire la utilizarea și vânzarea datelor lor de geolocalizare, nu a pus în aplicare măsuri care să le permită persoanelor fizice să renunțe la urmărire, a permis utilizarea datelor în scopuri potențial discriminatorii și nu a limitat utilizarea acestor informații de către terți[68]. Comisia se așteaptă ca FTC să adopte aceeași abordare în cazul în care societățile certificate în domeniul CCD ar face schimb de date, încălcând dispozițiile menționate mai sus.

În cele din urmă, trebuie menționat faptul că, în mai 2024, ODNI a emis Cadrul de politică al comunității serviciilor de informații pentru informațiile disponibile în mod comercial[69]. Prezentul cadru stabilește o serie de principii și cerințe pe care serviciile de informații ar trebui să le respecte, inclusiv pentru a reduce la minimum riscurile la adresa vieții private și a libertăților civile, atunci când achiziționează și utilizează informații în contextul unei tranzacții comerciale.

2.2.2. Supravegherea independentă

Activitățile serviciilor de informații ale SUA fac obiectul supravegherii de către diferite organisme, inclusiv responsabili pentru protecția vieții private și a libertăților civile, inspectori generali, Congres și PCLOB. În special, 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. 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[70]. 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.

Consilierul general al biroului inspectorului general al comunității serviciilor de informații (ICIG) din cadrul ODNI – care are competență generală asupra întregii Comunități a Serviciilor

[68] https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data.

[69] https://www.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Framework-May2024.pdf. Serviciile de informații au obligația de a respecta cadrul începând din august 2024.

[70] Fiecare serviciu de informații are un inspector general independent din punct de vedere legal și responsabil pentru efectuarea de audituri și investigații privind activitățile desfășurate de serviciul respectiv în scopuri legate de securitate națională. Aceștia au acces la toate materialele relevante (inclusiv clasificate), dacă este necesar, prin intermediul unei citații și pot lua declarații ale martorilor. Inspectorii generali trimit spre urmărire penală cazurile de presupuse încălcări penale și formulează recomandări de măsuri de remediere către șefii de serviciu. Deși recomandările lor nu au caracter obligatoriu, în general, rapoartele lor, inclusiv cu privire la acțiunile subsecvente (sau lipsa acestora), sunt făcute publice și transmise Congresului. A se vedea, în acest sens, nota de subsol 136 din Decizia privind caracterul adecvat al nivelului de protecție cu privire la rolul inspectorului general.

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 – a participat la reuniunea de evaluare. El a confirmat că ICIG verifică în mod sistematic respectarea OE nr. 14086 ca parte a activităților sale de supraveghere. El s-a referit, de asemenea, la activitățile recente de supraveghere ale altor inspectori generali ai comunității serviciilor de informații, astfel cum sunt detaliate în rapoartele periodice. De exemplu, în raportul său semestrial către Congres pentru perioada aprilie-septembrie 2023[71], inspectorul general al NSA a informat cu privire la o evaluare a unui cadru intern de control al NSA pentru deciziile și cererile de vizare. Acesta a concluzionat că respectivul cadru funcționează în mod corespunzător pentru a asigura respectarea legilor, directivelor și politicilor care protejează libertățile civile și viața privată. Același raport menționează, de asemenea, o investigație care a dezvăluit utilizarea abuzivă a unui instrument de colectare a informațiilor de tip SIGINT în scopuri neautorizate de către un angajat al NSA.

În temeiul OE nr. 14086, PCLOB[72] are funcții de supraveghere specifice[73]. Președintele PCLOB și cei trei membri ai săi au participat la reuniunea de evaluare și au informat că PCLOB a oferit consiliere serviciilor de informații cu privire la proiectele lor de politici și proceduri de punere în aplicare a OE nr. 14086 în aprilie 2023 și a fost consultat cu privire la numirea judecătorilor și a avocaților speciali ai Curții de Reexaminare a Protecției Datelor (DPRC). De asemenea, comitetul a lansat un proiect de supraveghere pentru (1) a evalua punerea în aplicare a politicilor și procedurilor actualizate adoptate de serviciile de informații pentru a se asigura că acestea sunt în concordanță cu OE și (2) pentru a efectua o evaluare anuală a funcționării noului mecanism de recurs (a se vedea mai jos)[74]. Membrii PCLOB au confirmat că respectivul comitet intenționează să efectueze ambele evaluări în viitorul apropiat. În ceea ce privește căile de atac, aceștia au explicat că, în absența plângerilor, evaluarea PCLOB se va axa pe politicile și procedurile puse în aplicare pentru instituirea mecanismului.

În ceea ce privește alte activități de supraveghere, PCLOB a publicat un raport privind articolul 702 din FISA la 28 septembrie 2023[75]. Prezentul raport reprezintă o continuare a unui raport anterior din 2014 și conține informații factuale și juridice actualizate privind funcționarea programelor de supraveghere din articolul 702 din FISA. Raportul conține, de asemenea, recomandări privind respectarea de către serviciile de informații a cerințelor aplicabile și sugestii adresate Congresului pentru a consolida în continuare mai multe aspecte ale articolului 702 din FISA în contextul reautorizării sale (inclusiv prin codificarea

[71] https://oig.nsa.gov/reports/Article/3609957/semiannual-report-to-congress-1-april-2023-to-30-september-2023/.

[72] PCLOB este o agenție independentă care 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. Acesta poate avea acces la toate informațiile relevante (inclusiv informații clasificate), poate desfășura interviuri și audia martori. Comitetul poate emite recomandări pentru autoritățile de aplicare a legii și de informații și prezintă rapoarte periodice către Congres și către Președinte. Rapoartele sale sunt puse la dispoziția publicului în cea mai mare măsură posibilă.

[73] https://documents.pclob.gov/prod/Documents/EventsAndPress/834a1977-f420-4b2a-ae93-8a522b2c7c74/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL)%20-%20Completed%20508%20-%2010202022.pdf.

[74] https://www.pclob.gov/OversightProjects/Details/1115.

[75] https://documents.pclob.gov/prod/Documents/OversightReport/8ca320e5-01d3-4d6a-8106-3384aad6ff31/2023%20PCLOB%20702%20Report%20-%20Nov%2017%202023%20-%201446.pdf.

obiectivelor legitime pentru activitățile de supraveghere enumerate în OE nr. 14086)[76]. În cursul reuniunii de evaluare, PCLOB a informat că se așteaptă să primească în curând răspunsuri din partea serviciilor de informații cu privire la punerea în aplicare a recomandărilor sale, care vor contribui la un viitor raport de monitorizare. Alte proiecte de supraveghere în curs includ unul privind combaterea terorismului intern și impactul acestuia asupra vieții private și a libertăților civile și colectarea de date din surse deschise sau disponibile pe piață de către FBI[77].

În cele din urmă, ONG-urile consultate în contextul evaluării și-au exprimat îngrijorarea cu privire la faptul că mandatul mai multor membri ai PCLOB urmează să expire în viitorul apropiat, ceea ce ar putea lăsa PCLOB fără cvorum. Mai exact, mandatul președintelui a expirat, iar perioada în care acesta poate continua să își exercite această funcție se încheie în ianuarie 2025, în timp ce mandatul unui membru a expirat deja, iar un al treilea mandat va expira în luna ianuarie a anului viitor. În cursul reuniunii de evaluare, membrii au explicat că nu se așteaptă ca PCLOB să ajungă în situația de a nu avea cvorum, deoarece a fost deja emisă o nominalizare pentru locul care este în prezent vacant (și se așteaptă confirmarea din partea Senatului)[78]. Aceștia au subliniat, de asemenea, că, și în ipoteza în care comitetul și-ar pierde cvorumul, acest lucru nu ar afecta capacitatea sa de a continua să desfășoare proiecte de supraveghere. Cu toate acestea, având în vedere rolul important al PCLOB de a evalua punerea în aplicare a OE nr. 14086, Comisia va monitoriza îndeaproape situația viitoarelor posturi vacante și a numirilor.

2.2.3. Căi de atac

OE nr. 14086, completat de un regulament al procurorului general, a instituit un nou mecanism de recurs pentru a gestiona și soluționa plângerile eligibile înaintate de persoane referitoare la activitățile SUA de colectare de informații de tip SIGINT[79]. Orice persoană din UE are dreptul de a înainta 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, articolul 702 din FISA, OE nr. 12333) în ceea ce privește datele cu caracter personal transferate către SUA care îi afectează în mod negativ interesele din perspectiva vieții private și a libertăților civile. Persoanele fizice pot depune o plângere la o APD dintr-un stat membru al UE, care direcționează plângerea, prin intermediul secretariatului CEPD, către mecanismul de recurs. Mecanismul constă în două niveluri, cu investigarea inițială a plângerilor efectuată de CLPO ODNI și posibilitatea ca persoanele fizice să conteste decizia CLPO în fața unei DPRC independente. Odată finalizată activitatea de examinare a plângerii de către CLPO ODNI sau DPRC, persoanele fizice sunt informate, prin intermediul autorității naționale, că „examinarea fie nu a identificat încălcări eligibile, fie CLPO ODNI/DPRC a emis o decizie care impune o remediere adecvată”. Deciziile CLPO ODNI și DPRC sunt obligatorii pentru serviciile de informații.

De la adoptarea Deciziei privind caracterul adecvat al nivelului de protecție, au fost luate măsuri suplimentare pentru ca mecanismul de recurs să devină pe deplin operațional.

---

[76] Comisia observă că unele dintre aceste recomandări au fost incluse ca parte a RISAA, inclusiv recomandarea privind colectarea „informațiilor despre” sau recomandarea privind consolidarea rolului experților FISC (amici).
[77] https://www.pclob.gov/OversightProjects.
[78] https://documents.pclob.gov/prod/Documents/EventsAndPress/deb9cd13-12af-4250-998e-a520a2419a6b/PCLOB%20nominee%20press%20release%206-13-24.pdf.
[79] Considerentele 176-194 din Decizia privind caracterul adecvat al nivelului de protecție.

În ceea ce privește instituirea DPRC, la 14 noiembrie 2023 au fost numiți în instanță opt judecători [și anume cu doi judecători mai mulți decât numărul minim prevăzut în temeiul OE nr. 14086, astfel cum a fost completat de reglementările procurorului general de la titlul 28 articolul 201.3 litera (a) din Codul regulamentelor federale][80]. Aceștia au fost numiți pe baza criteriilor stabilite în OE nr. 14086 și în conformitate cu procesul stabilit în acesta, inclusiv după consultarea, printre altele, a PCLOB[81]. Printre aceștia se numără foști judecători ai Tribunalului Federal Districtual și ai Curții de Apel, un fost procuror general al SUA și un fost membru al PCLOB. Astfel cum prevede OE, cel puțin jumătate dintre judecători au experiență judiciară anterioară. În plus, în aprilie 2024 au fost numiți doi avocați speciali – practicieni în domeniul dreptului cu expertiză atât în viața privată, cât și în securitatea națională, pentru a reprezenta interesele persoanelor fizice în fața DPRC. În cadrul reuniunii de evaluare s-a confirmat că toți judecătorii și avocații speciali au primit cea mai înaltă autorizație de securitate și, prin urmare, pot avea acces la materiale clasificate atunci când își îndeplinesc sarcinile pentru DPRC. DPRC a publicat, de asemenea, o serie de întrebări frecvente, oferind mai multe informații cu privire la rolul, independența și funcționarea sa[82].

În ceea ce privește tratarea plângerilor, ODNI a adoptat, la 6 decembrie 2022, Directiva nr. 126 privind comunitatea serviciilor de informații, care reglementează în detaliu (prin stabilirea de termene, instituirea unui registru electronic securizat și a unor canale de comunicare securizate, solicitând CLPO și elementelor comunității serviciilor de informații să coopereze cu PCLOB în contextul evaluării anuale a mecanismului de recurs etc.) diferite aspecte ale procesului de investigare și soluționare a plângerilor[83]. Prezenta directivă este aplicabilă în întreaga comunitate a serviciilor de informații din SUA și a fost completată de proceduri interne suplimentare adoptate de serviciile individuale de informații cu privire la cooperarea acestora cu CLPO ODNI în contextul tratării unei plângeri (de exemplu, dezvoltarea unui registru securizat pentru partajarea plângerilor și a documentelor de răspuns și comunicații securizate între agențiile relevante). DPRC va emite, de asemenea, în lunile următoare, norme mai detaliate privind tratarea plângerilor și alte aspecte procedurale.

O serie de măsuri suplimentare au fost luate în Uniunea Europeană și în Statele Unite pentru a informa publicul larg, precum și pentru a facilita depunerea și tratarea plângerilor. Aceasta include adoptarea de către CEPD a unei note de informare privind noul mecanism de recurs[84], a unui model de formular de plângere (care urmează să fie tradus și publicat de toate APD în limbile lor naționale)[85] și a unui regulament de procedură care reglementează cooperarea dintre autoritățile naționale de supraveghere și secretariatul CEPD[86]. În mod similar, ODNI a publicat

[80] https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-judges-data-protection-review-court.
[81] Articolul 3 litera (d) partea A din OE nr. 14086.
[82] https://www.justice.gov/opcl/dprc-resources.
[83] https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf.
[84] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/information-note-data-protection-framework-redress_en.
[85] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/template-complaint-form-us-office-director-national_en.
[86] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/rules-procedure-data-protection-framework-redress_en.

întrebări frecvente și o fișă informativă privind noul mecanism de recurs și s-a implicat în activități de sensibilizare a publicului[87].

În plus, în ultimul an, CEPD și autoritățile relevante din SUA au cooperat îndeaproape cu privire la mai multe aspecte operaționale. În special, astfel cum s-a confirmat în cursul reuniunii de evaluare, acestea au instituit un canal de comunicare criptat pentru a transmite plângeri din partea autorităților naționale din UE către secretariatul CEPD, de la secretariatul CEPD către CLPO ODNI, precum și către Biroul pentru protecția vieții private și a libertăților civile din cadrul Departamentului de Justiție (OPCL) și între CLPO ODNI și alte autorități din SUA (de exemplu, DPRC). În plus, CLPO ODNI a explicat că au fost instituite proceduri interne suplimentare pentru cooperarea serviciilor individuale de informații cu CLPO ODNI în ceea ce privește tratarea plângerilor.

În cele din urmă, OPCL, care oferă sprijin administrativ DPRC, a informat, de asemenea, că DPRC funcționează în cadrul propriei linii bugetare specifice și dispune de facilitățile necesare pentru a-și îndeplini sarcinile, inclusiv calculatoare și laptopuri securizate, telefoane etc. În plus, astfel cum se prevede în OE nr. 14086, DoC a luat măsurile necesare, inclusiv prin crearea unui canal de comunicare criptat cu CLPO ODNI, pentru a păstra o evidență a tuturor plângerilor eligibile primite. DoC va contacta periodic CLPO ODNI pentru a stabili dacă informațiile referitoare la o plângere individuală au fost declasificate. În acest caz, DoC va informa persoana în cauză în acest sens, pentru a-i permite să obțină acces la astfel de informații.

La momentul reuniunii de evaluare, autoritățile de supraveghere din UE nu primiseră nicio plângere și, prin urmare, noul mecanism de recurs nu fusese încă declanșat.

3. CONCLUZIE

Pe baza informațiilor colectate în cursul acestei prime evaluări, Comisia concluzionează că autoritățile SUA au instituit structurile și procedurile necesare pentru a asigura funcționarea eficace a Cadrului privind confidențialitatea datelor. În acest context, Comisia apreciază foarte mult cooperarea foarte bună cu autoritățile SUA pentru efectuarea evaluării.

Deși această primă evaluare s-a axat în mod firesc pe verificarea existenței tuturor elementelor constitutive ale cadrului, experiența în ceea ce privește punerea în practică a garanțiilor care se aplică atât prelucrării datelor de către societățile certificate, cât și accesului la date de către autoritățile publice este în mod necesar limitată după doar un an de funcționare. Prin urmare, Comisia va monitoriza îndeaproape evoluțiile relevante din lunile și anii următori, acordând o atenție deosebită (1) viitoarelor rapoarte ale PCLOB privind punerea în aplicare a OE nr. 14086 și funcționarea mecanismului de recurs în materie de colectare a informațiilor de tip SIGINT, în special DPRC; (2) posibilelor modificări suplimentare ale articolului 702 din FISA și (3) numirii membrilor PCLOB pentru ocuparea viitoarelor posturi vacante.

În plus, pentru a asigura o funcționare continuă și eficace, Comisia consideră că este important:

[87] https://www.dni.gov/files/CLPT/documents/Fact_Sheets/The_Role_of_the_ODNI_CLPO_FAQs.pdf și https://www.dni.gov/files/CLPT/documents/Fact_Sheets/Data_Privacy_Framework.pdf.

- astfel cum s-a anunțat în cadrul reuniunii de evaluare, ca DoC să utilizeze într-o mai mare măsură diferitele instrumente prevăzute în CCD pentru monitorizarea respectării principiilor de către întreprinderi și pentru detectarea declarațiilor false de participare;
- ca FTC să își dezvolte în continuare abordarea proactivă în ceea ce privește investigarea și asigurarea respectării de către societățile certificate a principiilor CCD UE-SUA și
- ca DoC, FTC și autoritățile UE pentru protecția datelor să elaboreze instrumente de orientare comune cu privire la cerințele-cheie în temeiul principiilor CCD UE-SUA, de exemplu cu privire la datele privind resursele umane și transferurile ulterioare.

Având în vedere acest rezultat al evaluării și astfel cum se prevede în considerentul 211 din Decizia privind caracterul adecvat al nivelului de protecție, Comisia consideră că este oportun să efectueze următoarea evaluare periodică după trei ani. Astfel se va acumula mai multă experiență în aplicarea practică a CCD și se va putea ține seama de evoluțiile viitoare menționate mai sus. Prin urmare, în conformitate cu articolul 3 alineatul (4) din Decizia privind caracterul adecvat al nivelului de protecție, Comisia va consulta CEPD și comitetul instituit în temeiul articolului 93 alineatul (1) din Regulamentul general privind protecția datelor cu privire la frecvența evaluărilor viitoare.