Avizul Comitetului (art. 70.1.s)

Avizul 5/2023 referitor la Proiectul de decizie de punere în aplicare a Comisiei Europene privind protecția adecvată a datelor cu caracter personal în temeiul Cadrului UE-SUA privind confidențialitatea datelor

Adoptat la 28 februarie 2023

Rezumat

La 13 decembrie 2022, Comisia Europeană a publicat un proiect de decizie privind caracterul adecvat al nivelului de protecție („proiectul de decizie"), ale cărui anexe includ un nou cadru pentru schimburile transatlantice de date cu caracter personal, Cadrul UE-SUA privind confidențialitatea datelor („CCD"), menit să înlocuiască Scutul de confidențialitate UE-SUA anterior, declarat nevalid de Curtea de Justiție a Uniunii Europene („CJUE") la 16 iulie 2020 în cauza Schrems II. Componenta-cheie a CCD o reprezintă principiile Cadrului UE-SUA privind confidențialitatea datelor, inclusiv principiile suplimentare (denumite în mod colectiv „principiile CCD").

În conformitate cu articolul 70 alineatul (1) litera (s) din Regulamentul (UE) 2016/679[1] al Parlamentului European și al Consiliului („RGPD"), Comisia a solicitat avizul Comitetului European pentru Protecția Datelor („CEPD") cu privire la proiectul de decizie.

CEPD a evaluat caracterul adecvat al nivelului de protecție oferit în SUA pe baza examinării proiectului de decizie. CEPD a evaluat atât aspectele comerciale, cât și accesul la datele cu caracter personal transferate din UE și utilizarea acestora de către autoritățile publice din SUA.

CEPD a ținut seama de cadrul juridic aplicabil al UE privind protecția datelor, astfel cum este prevăzut în RGPD, precum și drepturile fundamentale la respectarea vieții private și la protecția datelor, astfel cum sunt consacrate la articolele 7 și 8 din Carta Drepturilor Fundamentale a Uniunii Europene și la articolul 8 din Convenția Europeană a Drepturilor Omului. De asemenea, acesta a luat în considerare dreptul la o cale de atac eficientă și la un proces echitabil prevăzut la articolul 47 din Cartă, precum și jurisprudența referitoare la diferitele drepturi fundamentale.

În plus, CEPD a luat în considerare cerințele criteriilor de referință privind caracterul adecvat al nivelului de protecție adoptate de CEPD[2].

Principalul obiectiv al CEPD este de a prezenta Comisiei un aviz cu privire la caracterul adecvat al nivelului de protecție acordat persoanelor ale căror date cu caracter personal sunt transferate către SUA. Este important să se recunoască faptul că CEPD nu se așteptă să aibă loc o reproducere a legislației europene privind protecția datelor în cadrul de protecție a datelor aplicat în SUA.

Cu toate acestea, CEPD reamintește că, pentru a se considera că se oferă un nivel de protecție adecvat, articolul 45 din RGPD și jurisprudența CJUE impun ca legislația țării terțe să ofere persoanelor vizate un nivel de protecție în esență echivalent cu cel garantat în UE.

1.1. Aspecte generale privind protecția datelor

CCD prevede că respectarea principiilor CCD de către organizațiile CCD poate fi limitată în unele cazuri (de exemplu, în măsura necesară pentru a respecta o hotărâre judecătorească sau pentru a răspunde interesului public). Pentru a identifica mai bine impactul acestor derogări asupra nivelului de protecție a persoanelor vizate, CEPD recomandă Comisiei să includă în proiectul de decizie clarificări cu privire

[1] Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

[2] Grupul de lucru „Articolul 29", Criterii de referință privind caracterul adecvat al nivelului de protecție, WP 254 rev.01, 28 noiembrie 2017, astfel cum au fost revizuite ultima dată și adoptate la 6 februarie 2018, aprobate de CEPD la 25 mai 2018 („Criteriile de referință privind caracterul adecvat al nivelului de protecție").

la domeniul de aplicare al derogărilor, inclusiv cu privire la garanțiile aplicabile în temeiul legislației SUA.

CEPD constată că structura și numerotarea anexelor îngreunează identificarea informațiilor și trimiterea la acestea. Acest lucru contribuie la o prezentare globală complexă a noului cadru, care compilează în anexele sale documente cu valoare juridică diferită și nu poate înlesni o bună înțelegere a principiilor CCD de către persoanele vizate, organizațiile CCD și autoritățile UE pentru protecția datelor. De asemenea, CEPD subliniază că terminologia ar trebui utilizată în mod consecvent în cadrul CCD. În mod similar, unii termeni esențiali nu sunt definiți[3].

CEPD salută actualizările aduse principiilor CCD[4], care vor constitui cadrul juridic obligatoriu pentru organizațiile CCD, însă constată că, în pofida unei serii de modificări și explicații suplimentare incluse în considerentele proiectului de decizie, principiile CCD la care organizațiile CCD trebuie să adere rămân, în esență, neschimbate din perspectiva celor aplicabile în temeiul Scutului de confidențialitate [care au stat la baza revizuirilor comune anuale realizate de Grupul de lucru „Articolul 29" („GL29") și CEPD]. De asemenea, principiile CCD sunt, în mare măsură, aceleași precum cele din proiectul de decizie privind Scutul de confidențialitate, care au stat la baza avizului GL29 din 2016[5]. Pentru acele principii CCD care sunt, în esență, neschimbate, CEPD consideră că nu este necesar să repete toate observațiile formulate anterior de GL29. CEPD a decis să se concentreze asupra unor aspecte specifice pe care le consideră și mai relevante în prezent, având în vedere evoluția mediului juridic și tehnologic.

De exemplu, CEPD constată că unele aspecte problematice semnalate anterior de Grupul de lucru „Articolul 29" și de CEPD în legătură cu principiile Scutului de confidențialitate rămân valabile. În special, acestea se referă la drepturile persoanelor vizate (de exemplu, unele excepții cu privire la dreptul de acces, momentul exercitării dreptului la opoziție și modalitățile de exercitare a acestuia), la absența unor definiții-cheie, la lipsa de claritate în ceea ce privește aplicarea principiilor CCD în cazul persoanelor împuternicite de către operator și la derogarea amplă pentru informațiile aflate la dispoziția publicului[6].

De asemenea, CEPD ar dori să reitereze că nivelul de protecție a persoanelor ale căror date sunt transferate nu trebuie să fie subminat de transferul ulterior de la destinatarul inițial al datelor transferate[7]. CEPD invită încă o dată Comisia să clarifice faptul că garanțiile impuse de destinatarul inițial importatorului din țara terță trebuie să fie eficace în lumina legislației țării terțe, înainte de realizarea unui transfer ulterior în contextul CCD.

Evoluțiile rapide în domeniul procesului decizional automatizat și al creării de profiluri – din ce în ce mai mult prin intermediul tehnologiilor IA – necesită o atenție deosebită. CEPD salută trimiterile Comisiei la garanții specifice prevăzute de legislația relevantă a SUA în diferite domenii[8]. Cu toate acestea, nivelul de protecție a persoanelor pare să difere în funcție de normele sectoriale – dacă există – care se aplică situației în cauză. CEPD susține că sunt necesare norme specifice privind procesul decizional automatizat pentru a oferi garanții suficiente, inclusiv dreptul persoanei de a cunoaște logica

[3] Acesta este cazul termenilor „agent" și „persoană împuternicită de operator". În plus, conceptul de „date privind resursele umane" nu a fost încă discutat cu autoritățile SUA.
[4] De exemplu, clarificarea faptului că datele codificate sunt date cu caracter personal.
[5] Grupul de lucru „Articolul 29", Avizul 01/2016 cu privire la proiectul de decizie privind caracterul adecvat al Scutului de confidențialitate UE-SUA, adoptat la 13 aprilie 2016 („Avizul 01/2016 al GL29").
[6] Scutul de confidențialitate UE-SUA – A treia revizuire comună anuală, raportul CEPD adoptat la 12 noiembrie 2019, punctul 11.
[7] Secțiunea 3.A.9 din Criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD.
[8] Considerentul 35 din proiectul de decizie.

implicată, de a contesta decizia și de a obține o intervenție umană atunci când decizia o afectează în mod semnificativ.

CEPD reamintește importanța supravegherii eficace și a asigurării respectării efective a CCD și consideră că verificările conformității în ceea ce privește cerințele de fond sunt esențiale. Aceste aspecte vor fi monitorizate îndeaproape de CEPD, inclusiv în contextul revizuirilor periodice. CEPD ia act de angajamentele reînnoite exprimate în scrisorile Comisiei Federale pentru Comerț (*Federal Trade Commission*) („FTC")[9] și ale Departamentului Transporturilor (*Department of Transportation*) („DoT")[10] în ceea ce privește asigurarea respectării CCD, de exemplu, investigarea cu prioritate a presupuselor încălcări ale CCD.

CEPD constată că persoanelor vizate din UE li se oferă șapte modalități de recurs în cazul în care datele lor cu caracter personal sunt prelucrate cu încălcarea CCD. Aceste mecanisme de recurs sunt aceleași precum cele incluse în Scutul de confidențialitate anterior, care au făcut obiectul unor observații din partea GL29[11]. Eficacitatea acestor mecanisme de recurs va fi monitorizată îndeaproape de CEPD, inclusiv în contextul revizuirilor periodice.

1.2. Accesarea și utilizarea de către autoritățile publice din SUA a datelor cu caracter personal transferate din Uniunea Europeană

În proiectul de decizie, Comisia Europeană concluzionează că „orice ingerință a autorităților publice din SUA în interes public, în special în scopul asigurării respectării legii penale și în scopuri legate de securitatea națională, în drepturile fundamentale ale persoanelor ale căror date cu caracter personal sunt transferate din Uniune către Statele Unite ale Americii în temeiul Cadrului UE-SUA privind confidențialitatea datelor se va limita la ceea ce este strict necesar pentru atingerea obiectivului legitim în cauză și că există o protecție juridică efectivă împotriva unei astfel de ingerințe"[12].

Comisia Europeană ajunge la această concluzie în urma unei evaluări aprofundate a Ordinului executiv nr. 14086 de consolidare a garanțiilor pentru activitățile SUA de colectare de informații pe baza semnalelor electromagnetice (OE nr. 14086). OE nr. 14086 a fost emis de președintele SUA la 7 octombrie 2022, în urma negocierilor purtate între Comisia Europeană și Guvernul SUA în contextul invalidării deciziei anterioare privind caracterul adecvat al nivelului de protecție, denumită Scutul de confidențialitate, de către Curtea de Justiție a Uniunii Europene (CJUE).

CEPD ar saluta condiționarea nu numai a intrării în vigoare, ci și a adoptării deciziei, printre altele, de adoptarea unor politici și proceduri actualizate pentru punerea în aplicare a OE nr. 14086 de către toate serviciile de informații ale SUA. CEPD recomandă Comisiei să evalueze aceste politici și proceduri actualizate și să comunice această evaluare CEPD.

În ceea ce privește accesul autorităților la datele cu caracter personal transferate către SUA, CEPD și-a concentrat analiza pe evaluarea noului OE nr. 14086, deoarece acesta urmărește în mod efectiv să abordeze și să remedieze deficiențele identificate de CJUE în hotărârea sa Schrems II atunci când a declarat nevalidă decizia anterioară privind caracterul adecvat al nivelului de protecție.

CEPD recunoaște că, prin adoptarea OE nr. 14086, a fost modificat cadrul juridic al SUA pentru activitățile de colectare de informații pe baza semnalelor electromagnetice și consideră că garanțiile suplimentare incluse în acest ordin reprezintă o îmbunătățire semnificativă. OE nr. 14086 introduce

[9] Anexa IV la proiectul de decizie.
[10] Anexa V la proiectul de decizie.
[11] A se vedea, în special, secțiunea 2.2.6 litera (a) din Avizul 01/2016 al GL29.
[12] Considerentul 195 din proiectul de decizie.

conceptele de necesitate și proporționalitate în cadrul juridic al SUA privind informațiile colectate pe baza semnalelor electromagnetice și prevede un nou mecanism de recurs pentru persoanele din UE în cazul în care UE ar fi desemnată drept organizație de integrare economică regională eligibilă. CEPD consideră că noul mecanism de recurs a fost îmbunătățit în mod semnificativ în comparație cu așa-numitul mecanism anterior al Ombudsmanului în temeiul Scutului de confidențialitate. Spre deosebire de cadrul juridic anterior, care nu a creat drepturi pentru persoanele din UE, astfel cum a remarcat în mod explicit CJUE, noul OE nr. 14086 creează astfel de drepturi și oferă mai multe garanții pentru independența Curții de Reexaminare a Protecției Datelor (*Data Protection Review Court*), precum și competențe mai eficace pentru a remedia încălcările.

Comparând garanțiile suplimentare incluse în OE nr. 14086 cu ceea ce CEPD a stabilit ca reprezentând garanțiile esențiale europene (GEE), precum standardul elaborat pe baza jurisprudenței CJUE și a Curții Europene a Drepturilor Omului (CEDO), în evaluarea sa, CEPD a identificat în continuare o serie de aspecte care necesită clarificări suplimentare, cărora trebuie să li se acorde atenție sau care constituie motive de preocupare. Aceste aspecte reflectă faptul că, deși CEPD și-a bazat avizul pe hotărârea Schrems II, domeniul de aplicare al evaluării CEPD include în mod necesar considerații care depășesc constatările specifice din hotărârea Schrems II.

CEPD consideră că sunt necesare clarificări suplimentare cu privire la aspectele care vizează, în special, „colectarea temporară în masă" și păstrarea și diseminarea ulterioare ale datelor colectate (în masă) în cadrul juridic al SUA.

Întrucât testul echivalenței esențiale nu este un test al identității și întrucât garanțiile incluse în noul cadru juridic privind informațiile colectate pe baza semnalelor electromagnetice au fost consolidate, principalul punct de interes și de preocupare al CEPD îl reprezintă o evaluare a garanțiilor în ansamblul lor, care urmează o abordare holistică a acestora la nivelul întregului ciclu de prelucrare, de la colectarea datelor până la diseminarea lor, și include elementele de supraveghere și de recurs.

În acest sens, CEPD evidențiază în continuare următoarele constatări:

Deși recunoaște că OE nr. 14086 introduce conceptele de necesitate și proporționalitate în cadrul juridic al informațiilor colectate pe baza semnalelor electromagnetice, CEPD subliniază necesitatea de a monitoriza îndeaproape efectele acestor modificări în practică, inclusiv revizuirea politicilor și a procedurilor interne de punere în aplicare a garanțiilor prevăzute de ordinul executiv la nivel de agenție.

CEPD salută, de asemenea, faptul că OE nr. 14086 conține o listă de scopuri specifice în care poate și nu poate avea loc colectarea, observând totodată că obiectivele pot fi actualizate cu obiective suplimentare – nu neapărat de ordin public – în lumina noilor imperative de securitate națională.

Ca deficiență a cadrului actual, CEPD a identificat, în special, că, atunci când permite colectarea de date în masă în temeiul Ordinului executiv nr. 12333, cadrul juridic al SUA nu conține cerința autorizării prealabile de către o autoritate independentă, astfel cum se prevede în cea mai recentă jurisprudență a CEDO, și nici nu prevede o reexaminare independentă sistematică *ex post* de către o instanță sau de către un organism independent echivalent. În ceea ce privește autorizarea independentă prealabilă a supravegherii în temeiul articolului 702 din Legea privind supravegherea activităților străine de spionaj (*Foreign Intelligence Surveillance Act* – FISA), CEPD regretă faptul că, atunci când certifică un program care autorizează vizarea unor persoane care nu sunt cetățeni americani/rezidenți SUA, Curtea de Supraveghere a Activităților Străine de Spionaj (*United States Foreign Intelligence Surveillance Court*) („FISC") nu examinează cererea cu privire la programul respectiv din perspectiva respectării OE nr. 14086, chiar dacă serviciile de informații care desfășoară programul în cauză sunt obligate să

respecte acest ordin. În opinia CEPD, garanțiile suplimentare cuprinse în acest ordin ar trebui totuși să fie luate în considerare, inclusiv de către FISC. CEPD reamintește că rapoartele Comitetului de supraveghere în materie de protecție a vieții private și a libertăților civile (*Privacy and Civil Liberties Oversight Board*) („PCLOB") ar fi deosebit de utile pentru a evalua modul în care vor fi puse în aplicare garanțiile prevăzute de OE nr. 14086, precum și modul în care aceste garanții sunt aplicate atunci când sunt colectate date în temeiul articolului 702 din FISA și al OE nr. 12333.

În ceea ce privește mecanismul de recurs, CEPD recunoaște îmbunătățirile semnificative în ceea ce privește competențele Curții de Reexaminare a Protecției Datelor („DPRC") și independența sporită a acesteia în comparație cu Ombudsmanul. De asemenea, CEPD recunoaște garanțiile suplimentare prevăzute în noul mecanism de recurs, cum ar fi rolul avocaților speciali, care includ promovarea interesului reclamantului, precum și reexaminarea mecanismului de recurs de către PCLOB. Deși ține seama de natura securității naționale și de garanțiile prevăzute în OE nr. 14086, CEPD este totuși preocupat în legătură cu aplicarea generală a răspunsului standard al DPRC prin care informează reclamantul că fie nu au fost identificate încălcări eligibile, fie s-a emis o decizie care impune o remediere adecvată, precum și în legătură cu caracterul inatacabil al acestuia. Având în vedere importanța mecanismului de recurs, CEPD invită Comisia să monitorizeze îndeaproape funcționarea în practică a acestui mecanism.

CEPD se așteaptă ca Comisia să își respecte angajamentul de a suspenda, abroga sau modifica decizia privind caracterul adecvat al nivelului de protecție din motive de urgență, în special în cazul în care executivul SUA ar decide să restricționeze garanțiile incluse în ordinul executiv[13].

În general, CEPD salută îmbunătățirile substanțiale pe care le oferă ordinul executiv în comparație cu cadrul juridic anterior, în special în ceea ce privește introducerea principiilor necesității și proporționalității și a mecanismului de recurs individual pentru persoanele vizate din UE. Având în vedere preocupările exprimate și clarificările necesare, CEPD sugerează că aceste preocupări ar trebui abordate în cadrul viitoarele revizuiri comune, Comisia urmând să furnizeze clarificările solicitate pentru a consolida motivele emiterii proiectului de decizie și pentru a asigura o monitorizare atentă a punerii în aplicare concrete a acestui nou cadru juridic, în special a garanțiilor pe care le oferă.

[13] Considerentul 212 din proiectul de decizie.

Cuprins

1 INTRODUCERE 9
1.1 Cadrul de protecție a datelor din SUA 9
1.2 Domeniul de aplicare al evaluării CEPD 11
1.3 Observații și preocupări de natură generală 13
1.3.1 Analiza dreptului intern 13
1.3.2 Angajamente internaționale la care a aderat SUA 13
1.3.3 Evoluția legislației SUA privind protecția datelor 14
1.3.4 Domeniul de aplicare al proiectului de decizie 15
1.3.5 Limitări ale obligației de a adera la principiile CCD 15
1.3.6 Modificări în ceea ce privește Scutul de confidențialitate 15
1.3.7 Lipsa de claritate a documentelor CCD 16
2 ASPECTE GENERALE PRIVIND PROTECȚIA DATELOR 16
2.1 Principii referitoare la conținut 16
2.1.1 Concepte 16
2.1.2 Principiul limitării scopului 17
2.1.3 Dreptul de acces, dreptul la rectificare, dreptul la ștergere și dreptul la opoziție 17
2.1.4 Restricții privind transferurile ulterioare de date 19
2.1.5 Procesul decizional automatizat și crearea de profiluri 20
2.2 Mecanisme procedurale și de asigurare a respectării legii 21
2.3 Mecanisme de recurs 22
3 ACCESAREA ȘI UTILIZAREA DE CĂTRE AUTORITĂȚILE PUBLICE DIN SUA A DATELOR CU CARACTER PERSONAL TRANSFERATE DIN UNIUNEA EUROPEANĂ 23
3.1 Accesarea și utilizarea datelor în scopul asigurării respectării legii penale 23
3.1.1 Accesul autorităților de aplicare a legii la datele cu caracter personal ar trebui să se bazeze pe norme clare, precise și accesibile. 23
3.1.2 Trebuie să se demonstreze necesitatea și proporționalitatea în raport cu obiectivele legitime urmărite 24
3.1.3 Ar trebui să existe un mecanism de supraveghere independent 26
3.1.4 Persoanele trebuie să dispună de căi de atac eficiente 26
3.1.5 Utilizarea ulterioară a informațiilor colectate 28
3.2 Accesarea și utilizarea datelor în scopuri legate de securitatea națională 28
3.2.1 Garanția A – Prelucrarea ar trebui să fie în conformitate cu dispozițiile legii și să se bazeze pe norme clare, precise și accesibile 30
3.2.2 Garanția B – Trebuie să se demonstreze necesitatea și proporționalitatea în raport cu obiectivele legitime urmărite 33

3.2.3 Garanția C – Supravegherea.....44
3.2.4 Garanția D – Persoanele trebuie să dispună de căi de atac eficiente.....48
4 PUNEREA ÎN APLICARE ȘI MONITORIZAREA PROIECTULUI DE DECIZIE 57

Comitetul European pentru Protecția Datelor

Comitetul European pentru Protecția Datelor adoptă următoarea declarație:

având în vedere articolul 70 alineatul (1) litera (s) din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE („RGPD")[1],

având în vedere Acordul privind SEE, în special anexa XI și Protocolul 37 la acesta, astfel cum a fost modificat prin Decizia nr. 154/2018 a Comitetului mixt al SEE din 6 iulie 2018[2],

având în vedere articolele 12 și 22 din Regulamentul său de procedură,

A ADOPTAT PREZENTUL AVIZ:

1 INTRODUCERE

1.1 Cadrul de protecție a datelor din SUA

1. Statele Unite ale Americii („SUA") și Uniunea Europeană („UE") au abordări diferite în ceea ce privește viața privată și protecția datelor. În timp ce, în UE, respectarea vieții private și protecția datelor sunt drepturi fundamentale garantate la articolele 7 și 8 din Carta Drepturilor Fundamentale a Uniunii Europene, protecția datelor în SUA este, în general, abordată din perspectiva protecției consumatorilor. Prin urmare, abordările în materie de reglementare din SUA și UE diferă[3].

2. Spre deosebire de abordarea cuprinzătoare a UE adoptată prin RGPD, în SUA nu există o legislație generală cuprinzătoare privind protecția datelor la nivel federal. Protecția vieții private în SUA se realizează mai degrabă printr-o abordare sectorială și statală. De exemplu, unele sectoare specifice sunt reglementate de acte specifice, cum ar fi:

   - Legea privind portabilitatea și răspunderea în materie de asigurări de sănătate (*Health Insurance Portability and Accountability Act*) (HIPAA)[4];

---

[1] Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (Text cu relevanță pentru SEE) (JO L 119, 4.5.2016, p. 1).

[2] Trimiterile la „statele membre" din prezentul aviz trebuie înțelese ca trimiteri la „statele membre ale SEE".

[3] A se vedea, de asemenea, anexa I secțiunea I din Proiectul de decizie de punere în aplicare a Comisiei Europene în temeiul Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului privind nivelul adecvat de protecție a datelor cu caracter personal în temeiul Cadrului UE-SUA privind confidențialitatea datelor, publicat la 13 decembrie 2022 („proiectul de decizie").

[4] Legea privind portabilitatea și răspunderea în materie de asigurări de sănătate (HIPAA) din 1996 este o lege federală a SUA. Aceasta stabilește standarde naționale de protecție a informațiilor sensibile ale pacienților în materie de sănătate. Obiectivul HIPAA este de a proteja în mod adecvat informațiile persoanelor în materie de sănătate, permițând în același timp circulația acestora pentru furnizarea și promovarea unei asistențe medicale

- Legea privind respectarea vieții private a copiilor în mediul online (*Children's Online Privacy Protection Act*) (COPPA)[5];
- Legea Gramm-Leach-Billey (*Gramm-Leach-Billey Act*) (GLBA)[6].

3. În ceea ce privește accesul autorităților la datele cu caracter personal transferate din UE către SUA, se aplică o serie de temeiuri juridice, limitări și garanții diferite. Procesele juridice pentru accesul la informații în scopul asigurării respectării legii decurg în mod direct din Constituția SUA (al Patrulea Amendament), din dreptul material și procedural sau din orientările și politicile Departamentului de Justiție (*Department of Justice*) la nivel federal sau la nivel de stat. Accesul la informații în scopuri legate de securitatea națională este reglementat de mai multe instrumente juridice și, în special, de Legea privind supravegherea activităților străine de spionaj (FISA), de Ordinul executiv nr. 12333, de Ordinul executiv nr. 14086 recent adoptat, precum și de Regulamentul procurorului general („Regulamentul PG")[7] de instituire a unei Instanțe de Reexaminare a Protecției Datelor („DPRC").

4. La 13 decembrie 2022, Comisia a emis proiectul său de Decizie de Punere în Aplicare în temeiul Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului privind nivelul adecvat de protecție a datelor cu caracter personal în temeiul Cadrului UE-SUA privind confidențialitatea datelor („proiectul de decizie"), a cărui anexă conține Cadrul UE-SUA privind confidențialitatea datelor („CCD"). Din motivele explicate mai sus, proiectul de decizie are la bază CCD și nu un cadru juridic federal specific și cuprinzător.

5. CCD funcționează astfel: *„ Departamentul Comerțului (Department of Commerce) («Departamentul») publică principiile cadrului UE-SUA privind confidențialitatea datelor, inclusiv principiile suplimentare (denumite în mod colectiv «principiile») și anexa I la principii («anexa I»), în calitate de autoritate competentă cu scopul de a stimula, a promova și a dezvolta comerțul internațional [titlul 15 articolul 1512 din U.S.C. – Codul legislației SUA (US Code)]"* [8].

---

de înaltă calitate. HIPAA reglementează utilizarea și divulgarea informațiilor în materie de sănătate de către entitățile care fac obiectul Regulamentului privind respectarea vieții private (*Privacy Rule*). De asemenea, aceasta include standarde cu privire la drepturile persoanelor de a înțelege și de a controla modul în care le sunt utilizate informațiile în materie de sănătate.
https://www.hhs.gov/hipaa/for-professionals/privacy/index.html; https://www.justice.gov/opcl/privacy-act-1974.

[5] Obiectivul principal al COPPA este de a le permite părinților să controleze ce informații cu caracter personal sunt colectate de la copiii lor cu vârsta sub 13 ani de la operatorii site-urilor web și ai serviciilor online destinate copiilor (inclusiv prin intermediul aplicațiilor mobile și al dispozitivelor IoT precum jucăriile inteligente) sau ai site-urilor destinate publicului larg. COPPA prevede obligația acestor operatori de a furniza o notificare în acest sens părinților și de a obține consimțământul verificabil al acestora. Acest lucru este valabil și pentru datele provenite de la copii străini, în cazul în care site-urile web sau serviciile sunt operate în SUA și fac obiectul COPPA. În același timp, reglementările se aplică, de asemenea, site-urilor web și serviciilor operatorilor cu sediul în străinătate, în cazul în care acestea se adresează copiilor din SUA. A se vedea: https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#A.%20General%20Questions și anexa IV la proiectul de decizie, p 3.

[6] Unul dintre obiectivele Legii Gramm-Leach-Bliley este de a proteja viața privată a consumatorilor în sectorul financiar. Legea GLB impune instituțiilor financiare să explice clienților practicile de schimb de informații și să instituie garanții pentru a proteja informațiile despre clienți, de exemplu, pentru societățile reglementate de FTC în temeiul Regulamentului FTC privind garanțiile (*FTC Safeguards Rule*) (https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act).

[7] Ordinul nr. 5517-2022 al procurorului general, care modifică regulamentele Departamentului de Justiție al SUA, în conformitate cu cele autorizate și prevăzute în OE nr. 14086.

[8] Secțiunea I din anexa I la proiectul de decizie.

6. Dezvoltarea principiilor („principiile CCD”) a avut loc prin consultări cu Comisia Europeană („Comisia”), cu industria și cu alte părți interesate, în vederea atingerii obiectivului de facilitare a comerțului UE-SUA[9], asigurându-se în același timp că persoanelor vizate li se oferă un nivel de protecție în esență echivalent cu cel garantat în UE.

7. Principiile CCD sunt descrise drept o „componentă-cheie” a CCD. Pe de o parte, acestea oferă un „mecanism gata de utilizare” pentru transferurile de date din UE către SUA. Pe de altă parte, datele cu caracter personal transferate din UE către SUA sunt garantate și protejate în conformitate cu legislația UE.

8. CCD se aplică numai organizațiilor din SUA care s-au autocertificat în conformitate cu cerințele cadrului („organizațiile CCD”). Pentru moment, acest lucru este posibil numai dacă ele intră sub jurisdicția Comisiei Federale pentru Comerț („FTC”) sau a Departamentului Transporturilor („DoT”). În viitor, alte organisme statutare – care dețin competența de a supraveghea punerea în aplicare a principiilor CCD – ar putea fi adăugate într-o viitoare anexă.

9. Principiile CCD explică faptul că respectivele condiții ale cadrului sunt aplicabile de către (i) FTC în temeiul secțiunii 5 din Legea Comisiei Federale pentru Comerț (*Federal Trade Commission Act*) (legea FTC), care interzice actele neloiale sau frauduloase în domeniul comerțului sau care afectează comerțul[10] și (ii) DoT în temeiul titlului 49 articolul 41712 din U.S.C., care interzice unui transportator sau unui agent de bilete să desfășoare orice practică neloială sau frauduloasă în cadrul activității de transport aerian sau pentru vânzarea de servicii de transport aerian.

10. Principiile CCD subliniază că acestea nu afectează aplicarea RGPD și nici nu limitează obligațiile existente în materie de confidențialitate care se aplică în alt mod în temeiul legislației SUA.

1.2 Domeniul de aplicare al evaluării CEPD

11. Proiectul de decizie reflectă evaluarea de către Comisie a CCD în urma discuțiilor cu guvernul SUA. În conformitate cu articolul 70 alineatul (1) litera (s) din RGPD, CEPD are obligația de a prezenta un aviz asupra constatărilor Comisiei în ceea ce privește caracterul adecvat al nivelului de protecție într-o țară terță și, dacă este necesar, depune eforturi pentru a face propuneri în vederea soluționării oricărei probleme.

12. CEPD salută actualizările aduse principiilor CCD[11], care vor constitui cadrul juridic obligatoriu pentru organizațiile CCD. Cu toate acestea, CEPD constată că principiile CCD rămân, în esență, aceleași precum cele din Scutul de confidențialitate[12] [care au stat la baza revizuirilor comune anuale ale Grupului de lucru „Articolul 29” („GL29”) și CEPD]. De asemenea, principiile CCD sunt, în mare măsură, aceleași precum cele din proiectul de decizie privind Scutul de confidențialitate, care au stat la baza avizului GL29 din 2016 („Avizul 01/2016”)[13]. Pentru acele principii CCD care sunt, în esență, neschimbate, CEPD consideră că nu este necesar să repete toate observațiile formulate anterior de GL29. CEPD a decis să

[9] *Ibidem*.
[10] Titlul 15 articolul 45 litera (a) din U.S.C.
[11] De exemplu, clarificarea faptului că datele codificate sunt date cu caracter personal.
[12] Decizia de punere în aplicare (UE) 2016/1250 a Comisiei din 12 iulie 2016 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind caracterul adecvat al protecției oferite de Scutul de confidențialitate UE-SUA (JO L 207, 1.8.2016, p. 1).
[13] Grupul de lucru „Articolul 29”, Avizul 01/2016 cu privire la proiectul de decizie privind caracterul adecvat al Scutului de confidențialitate UE-SUA, adoptat la 13 aprilie 2016 („Avizul 01/2016 al GL29”).

se concentreze asupra unor aspecte specifice pe care le consideră și mai relevante în prezent, având în vedere evoluția mediului juridic și tehnologic.

13. În plus, în conformitate cu jurisprudența CJUE[14], o parte foarte importantă a analizei se referă la regimul juridic al accesului autorităților la datele cu caracter personal transferate către SUA.

14. În evaluarea sa, CEPD a ținut seama de cadrul european aplicabil în materie de protecție a datelor, inclusiv de articolele 7, 8 și 47 din Carta Drepturilor Fundamentale a Uniunii Europene („Carta"), care protejează dreptul la respectarea vieții private și de familie, dreptul la protecția datelor cu caracter personal și dreptul la o cale de atac eficientă și la un proces echitabil, precum și de articolul 8 din Convenția Europeană a Drepturilor Omului („CEDO"), care protejează dreptul la respectarea vieții private și de familie. În plus față de cele de mai sus, CEPD a luat în considerare cerințele RGPD, jurisprudența relevantă și criteriile de referință privind caracterul adecvat al nivelului de protecție adoptate de CEPD („Criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD")[15].

15. Obiectivul acestui exercițiu este de a oferi Comisiei un aviz privind evaluarea caracterului adecvat al nivelului de protecție oferit de CCD. Conceptul de „nivel de protecție adecvat", care era deja prevăzut în temeiul Directivei 95/46/CE, a fost dezvoltat în continuare de CJUE. Prin urmare, este important să se reamintească standardul stabilit de CJUE în hotărârile Schrems I[16] (prin care se declară nevaliditatea „Safe Harbour") și Schrems II[17] (prin care se declară nevaliditatea Scutului de confidențialitate).

16. În hotărârea Schrems I, CJUE a stabilit că, deși „nivelul de protecție" din țara terță trebuie să fie „în esență echivalent" cu cel garantat în UE, „mijloacele la care această țară terță a recurs, în această privință, pentru a asigura un astfel de nivel de protecție pot fi diferite de cele puse în aplicare în cadrul Uniunii"[18]. Prin urmare, obiectivul nu este de a reflecta punctual legislația europeană, ci de a stabili cerințele esențiale și de bază ale legislației examinate. Caracterul adecvat al nivelului de protecție poate fi obținut prin intermediul unei combinații de drepturi pentru persoanele vizate și obligații pentru cei care prelucrează date cu caracter personal sau care exercită control asupra prelucrării, precum și prin supravegherea de către organisme independente. Cu toate acestea, normele de protecție a datelor sunt eficace numai dacă sunt executorii și sunt respectate în practică. Prin urmare, este necesar să se ia în considerare nu doar conținutul normelor aplicabile transferului de date cu caracter personal către o țară terță sau o organizație internațională, ci și sistemul existent pentru asigurarea eficacității acestor norme. Mecanismele eficiente de punere în aplicare sunt de o importanță fundamentală pentru eficacitatea normelor de protecție a datelor[19].

---

[14] În special: Hotărârea Curții de Justiție din 6 octombrie 2015, Maximilian Schrems/Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650 și Hotărârea Curții de Justiție din 16 iulie 2020, Data Protection Commissioner/Facebook Ireland Limited și Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559.

[15] Grupul de lucru „Articolul 29", Criterii de referință privind caracterul adecvat al nivelului de protecție, WP 254 rev.01, 28 noiembrie 2017, astfel cum au fost revizuite ultima dată și adoptate la 6 februarie 2018, aprobate de CEPD la 25 mai 2018 („Criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD").

[16] Hotărârea Schrems I a Curții de Justiției a Uniunii Europene din 6 octombrie 2015, Maximilian Schrems/Data Protection Commissioner, C-392/14, ECLI:EU:C:2015:650 („hotărârea Schrems I a CJUE").

[17] Hotărârea Curții de Justiție din 16 iulie 2020, Data Protection Commissioner/Facebook Ireland Limited și Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559 („hotărârea Schrems II a CJUE").

[18] Hotărârea Schrems I a CJUE, punctele 73-74.

[19] Criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD, p. 2.

17. În hotărârea sa Schrems II, CJUE a stabilit că legile în baza cărora serviciile de informații din SUA pot accesa date cu caracter personal transferate către SUA (articolul 702 din FISA/OE nr. 12333) restrâng în mod disproporționat drepturile consacrate la articolele 7 și 8 din Carta Drepturilor Fundamentale a Uniunii Europene și, ca atare, nu sunt circumscrise astfel încât să îndeplinească cerințe în esență echivalente cu cele prevăzute, în dreptul Uniunii, la articolul 52 alineatul (1) a doua teză din Cartă[20].

18. În plus, CJUE a afirmat că anteriorul cadru juridic nu prevedea garanții în esență echivalente cu cele prevăzute la articolul 47 din Cartă, întrucât mecanismul Ombudsmanului nu putea compensa faptul că nici Directiva nr. 28 privind politica prezidențială (*Presidential Policy Directive 28 – PPD-28*), nici OE nr. 12333 nu acordau persoanelor care nu sunt cetățeni americani/rezidenți SUA o cale de atac eficientă[21]. Ombudsmanul nu își desfășura activitatea în condiții de independență în raport cu puterea executivă și nu deținea competența de a adopta decizii cu caracter obligatoriu pentru serviciile de informații din SUA[22].

19. OE nr. 14086, care înlocuiește în cea mai mare parte PPD-28, a introdus, în temeiul legislației SUA, două noi cerințe care reflectă cele stabilite în hotărârea Schrems II a CJUE: pe de o parte, cerința ca activitățile de colectare de informații pe baza semnalelor electromagnetice să se desfășoare numai în măsura în care acest lucru este necesar pentru a promova colectarea de informații în baza unei priorități validate și numai în măsura și într-un mod proporționale cu respectiva prioritate validată în materie de informații și, pe de altă parte, cerința de instituire a unui mecanism de recurs.

20. În prezentul aviz, CEPD evaluează în special în ce măsură CCD, precum și OE nr. 14086, adoptat recent, abordează efectiv cele constatate de CJUE în hotărârea sa.

1.3 Observații și preocupări de natură generală

1.3.1 Analiza dreptului intern

21. CEPD înțelege că evaluarea cuprinsă în proiectul de decizie se referă la principiile CCD. Cu toate acestea, CEPD ar aprecia furnizarea unor informații cu privire la contextul juridic din SUA în care își desfășoară activitatea organizațiile CCD. Acest lucru i-ar permite o mai bună înțelegere a interacțiunii dintre CCD și legislația SUA. De exemplu, la punctul 1 din anexa I[23], se stabilește că principiile CCD nu „[...] limitează obligațiile de confidențialitate care se aplică în alt mod în temeiul legislației SUA”, fără a se descrie aceste obligații.

1.3.2 Angajamente internaționale la care a aderat SUA

22. În conformitate cu articolul 45 alineatul (2) litera (c) din RGPD și cu Criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD, atunci când evaluează caracterul adecvat al nivelului de protecție asigurat de o țară terță, Comisia ține seama, printre altele, de angajamentele internaționale la care a aderat țara terță în cauză sau de alte obligații care decurg din participarea țării terțe respective la sisteme multilaterale sau regionale, mai ales în domeniul protecției datelor cu caracter personal, precum și de punerea în aplicare a unor astfel de obligații.

23. SUA este parte la mai multe acorduri internaționale care garantează dreptul la viață privată, cum ar fi Pactul internațional cu privire la drepturile civile și politice (articolul 17), Convenția privind drepturile persoanelor cu handicap (articolul 22) și Convenția cu privire la drepturile copilului (articolul 16). În

[20] Hotărârea Schrems II a CJUE, punctele 184-185.
[21] Hotărârea Schrems II a CJUE, punctul 192.
[22] Hotărârea Schrems II a CJUE, punctul 195.
[23] Secțiunea I ultima teză din anexa I la proiectul de decizie.

plus, în calitate de țară membră OCDE, SUA aderă la Cadrul OCDE privind protecția vieții private, în special la Orientările privind protecția vieții private și a fluxurilor transfrontaliere de date cu caracter personal. La 14 decembrie 2022, miniștrii și reprezentanții la nivel înalt ai membrilor OCDE și ai Uniunii Europene au adoptat Declarația OCDE privind accesul autorităților la datele cu caracter personal deținute de entitățile din sectorul privat. SUA este, de asemenea, parte la Convenția de la Budapesta privind criminalitatea informatică.

24. În plus, SUA este membră a Sistemului de norme transfrontaliere de protecție a vieții private (CBPR) elaborate de Cooperarea Economică Asia-Pacific (APEC), care oferă o certificare sprijinită la nivel guvernamental cu privire la confidențialitatea datelor și la care întreprinderile pot adera pentru a demonstra respectarea normelor de protecție a vieții private recunoscute la nivel internațional. Aceste norme de protecție a vieții private au fost validate de liderii APEC.

25. CEPD ia act, de asemenea, de participarea SUA în calitate de stat observator la lucrările Comitetului consultativ al Convenției 108 a Consiliului Europei.

26. În plus, CEPD ia act de și salută implicarea continuă a organismelor SUA în formatul nou stabilit în 2021 al „Mesei rotunde a autorităților pentru protecția datelor și a vieții private din țările G7" (masa rotundă a APD G7), care reunește autorități independente de supraveghere a protecției datelor și a vieții private din țările G7. În acest context, acestea au sprijinit, de exemplu, ultimul comunicat al mesei rotunde a APD G7[24], adoptat la 8 septembrie 2022 la Bonn, Germania, care s-a axat pe conceptul de „liberă circulație a datelor cu încredere" (*Data Free Flow with Trust*).

1.3.3 Evoluția legislației SUA privind protecția datelor

27. CEPD ia act în special de evoluțiile legislației SUA în materie de confidențialitate a datelor la nivel de stat. CEPD salută adoptarea de legi privind protecția datelor în cinci state (California, Colorado, Connecticut, Virginia și Utah), care au intrat sau vor intra în vigoare până în 2023[25]..

28. CEPD constată, de asemenea, că în multe alte state ale SUA au fost deja lansate inițiative similare de promovare a unor alte astfel de legi la nivel de stat.

29. În plus, CEPD salută în mod explicit eforturile depuse în ceea ce privește inițiativa bipartizană de promovare a unei legi federale privind protecția datelor, respectiv Legea americană privind confidențialitatea și protecția datelor (*American Data Privacy and Protection Act*) (ADPPA).

---

[24] Masa rotundă a autorităților pentru protecția datelor și a vieții private din țările G7, „Promoting Data Free Flow with Trust and knowledge sharing about the prospects for International Data Spaces" („Promovarea liberei circulații a datelor cu încredere și schimb de cunoștințe cu privire la perspectivele instituirii spațiilor internaționale de date", 8 septembrie 2022, https://www.bfdi.bund.de/SharedDocs/Downloads/EN/G7/Communique-2022.pdf?__blob=publicationFile&v=1.

[25] Legea privind protecția vieții private a consumatorilor din California (*California Consumer Privacy Act*) (2018; cu intrare în vigoare la 1 ianuarie 2020); Legea privind drepturile în materie de protecție a vieții private din California (*California Privacy Rights Act*) (2020; pe deplin în vigoare la 1 ianuarie 2023); Legea privind protecția vieții private din Colorado (*Colorado Privacy Act*) (2021; cu intrare în vigoare la 1 iulie 2023); Legea privind confidențialitatea datelor din Connecticut (*Connecticut Data Privacy Act*) (2022; cu intrare în vigoare la 1 iulie 2023); Legea privind protecția datelor consumatorilor din Virginia (*Virginia Consumer Data Protection Act*) (2021; cu intrare în vigoare la 1 ianuarie 2023); Legea privind protecția vieții private a consumatorilor (*Utah Consumer Privacy Act*) (2022; cu intrare în vigoare la 31 decembrie 2023).

1.3.4 Domeniul de aplicare al proiectului de decizie

30. Conform articolului 1 din proiectul de decizie, Comisia concluzionează că SUA asigură un nivel adecvat de protecție a datelor cu caracter personal transferate din UE către organizații din Statele Unite ale Americii care sunt incluse în „Lista cadrului privind confidențialitatea datelor", gestionată și pusă la dispoziția publicului de către Departamentul Comerțului („DoC") în conformitate secțiunea I.3. din anexa I[26].

31. CCD este disponibil pentru societățile aflate sub jurisdicția FTC sau DoT. Trebuie menționat că, în viitor, ar putea fi adăugate și alte organisme statutare din SUA cu competențe similare[27].

1.3.5 Limitări ale obligației de a adera la principiile CCD

32. Punctul I.5. din anexa I prevede că aderarea la principiile CCD de către organizațiile CCD poate fi limitată, printre altele, (i) în măsura necesară pentru a respecta o hotărâre judecătorească sau pentru a îndeplini cerințe de interes public, de asigurare a respectării legii[28] sau de securitate națională[29] (inclusiv în cazul în care legile sau regulamentele administrative stabilesc obligații contradictorii) și (ii) în temeiul unei legi, al unei hotărâri judecătorești sau al unui regulament administrativ care prevede autorizații exprese, cu condiția ca organizația CCD care a recurs la o asemenea autorizație să poată demonstra că nerespectarea principiilor CCD se limitează la măsura necesară pentru garantarea intereselor legitime superioare pe care această autorizație urmărește să le servească.

33. Fără o cunoaștere deplină a legislației SUA, atât la nivel federal, cât și la nivel de stat, este dificil pentru CEPD să evalueze în detaliu domeniul de aplicare al derogărilor enumerate la acest punct. Prin urmare, CEPD recomandă Comisiei să includă în proiectul de decizie clarificări cu privire la domeniul de aplicare al derogărilor, inclusiv cu privire la garanțiile aplicabile în temeiul legislației SUA, pentru a identifica mai bine impactul acestor derogări asupra nivelului de protecție a persoanelor vizate. De asemenea, CEPD subliniază că Comisia ar trebui să fie informată cu privire la aplicarea și adoptarea oricărei legi sau a oricărui regulament administrativ care ar afecta aderarea la principiile CCD, precum și că aceasta ar trebui să monitorizeze astfel de acțiuni.

1.3.6 Modificări în ceea ce privește Scutul de confidențialitate

34. CEPD salută eforturile depuse pentru a răspunde cerințelor conținute de hotărârea Schrems II. Cu toate acestea, CEPD consideră că ar fi fost oportună abordarea mai multor probleme identificate (i) în Avizul 01/2016 al GL29 și (ii) în revizuirile comune anterioare[30] cu ocazia negocierilor CCD.

---

[26] Articolul 1 secțiunea Considerații finale din proiectul de decizie, p. 57. CEPD înțelege că proiectul de decizie nu va viza transferurile de la entități situate în afara UE, dar care fac obiectul RGPD în temeiul articolului 3 alineatul (2) din RGPD către entități certificate din SUA.

[27] Secțiunea I punctul 2 din anexa I la proiectul de decizie.

[28] A se vedea secțiunea 3.1 din prezentul aviz pentru mai multe observații privind utilizarea datelor cu caracter personal care fac obiectul CCD UE-SUA în scopul asigurării respectării legii.

[29] A se vedea secțiunea 3.2 din prezentul aviz pentru mai multe observații privind utilizarea datelor cu caracter personal care fac obiectul CCD UE-SUA în scopuri legate de securitatea națională.

[30] Revizuiri anuale: Scutul de confidențialitate UE-SUA – Prima revizuire comună anuală, WP 255, raportul GL29 adoptat la 28 noiembrie 2017 („raportul aferent primei revizuiri comune anuale"); Scutul de confidențialitate UE-SUA – A doua revizuire comună anuală, raportul CEPD adoptat la 22 ianuarie 2019 („raportul aferent celei de a doua revizuiri comune anuale"); Scutul de confidențialitate UE-SUA – A treia revizuire comună anuală, raportul CEPD adoptat la 12 noiembrie 2019 („raportul aferent celei de a treia revizuiri comune anuale").

35. De asemenea, CEPD constată că, în pofida unei serii de modificări și explicații suplimentare incluse în considerentele proiectului de decizie, principiile CCD la care organizațiile CCD trebuie să adere rămân, în esență, neschimbate din perspectiva celor aplicabile în temeiul Scutului de confidențialitate.

1.3.7 Lipsa de claritate a documentelor CCD

36. CEPD constată că structura și numerotarea anexelor îngreunează identificarea informațiilor și trimiterea la acestea. Acest lucru contribuie la o prezentare globală complexă a noului cadru, care compilează în anexele sale documente cu valoare juridică diferită și nu poate înlesni o bună înțelegere a principiilor CCD de către persoanele vizate, organizațiile CCD și autoritățile UE pentru protecția datelor („APD din UE").

37. De asemenea, CEPD subliniază că terminologia ar trebui utilizată în mod consecvent în cadrul CCD. Acest lucru nu se întâmplă în prezent, de exemplu, în cazul noțiunii de „prelucrare". Astfel, unele părți ale CCD enumeră anumite tipuri de operațiuni de prelucrare a datelor în loc să utilizeze termenul „prelucrare". Acest lucru poate duce la insecuritate juridică și la posibile lacune în ceea ce privește protecția[31].

38. CEPD salută faptul că definițiile unora dintre termenii utilizați sunt incluse în CCD[32]. Totuși, acest lucru nu se întâmplă în cazul altor termeni esențiali, precum „agent" sau „persoană împuternicită de operator", care, în opinia CEPD, necesită o definiție clară și specifică în secțiunea I punctul 8 din anexa I la CCD, convenită de SUA și UE, pentru a evita confuzia într-o etapă ulterioară pentru organizațiile CCD care se prevalează de CCD, pentru autoritățile de supraveghere și pentru publicul larg.

39. În ceea ce privește problema interpretărilor divergente în UE și SUA ale conceptului de date privind resursele umane, CEPD este de acord cu cele prevăzute în raportul Comisiei emis în urma celei de a treia revizuiri în legătură cu obiectivul de a continua discuțiile cu autoritățile SUA[33].

2 ASPECTE GENERALE PRIVIND PROTECȚIA DATELOR

2.1 Principii referitoare la conținut

2.1.1 Concepte

40. Pe baza Criteriilor de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD, cadrul juridic al țării terțe ar trebui să includă concepte și/sau principii de bază privind protecția datelor. Deși acestea nu trebuie să corespundă terminologiei RGPD, ele ar trebui să reflecte conceptele consacrate în legislația europeană privind protecția datelor și să fie în concordanță cu acestea. De exemplu, RGPD include următoarele concepte importante: „date cu caracter personal", „prelucrarea datelor cu caracter personal", „operator de date", „persoană împuternicită de operator", „destinatar"

[31] De exemplu, (i) potrivit formulării din secțiunea III punctul 6 litera (f) din anexa I la proiectul de decizie, principiile CCD ar fi aplicabile numai în cazul în care organizația „stochează, utilizează sau divulgă" datele primite [și anume, nu pentru alte operațiuni acoperite de termenul „prelucrare", cum ar fi colectarea, înregistrarea, modificarea, extragerea, consultarea, ștergerea) și (ii) potrivit secțiunii II punctul 4 litera (a) din proiectul de decizie, securitatea datelor ar fi impusă numai pentru „crearea, gestionarea, utilizarea sau diseminarea" de informații cu caracter personal.

[32] Secțiunea I punctul 8 din anexa I la proiectul de decizie.

[33] Raportul aferent celei de a treia revizuiri comune, paginile 5, 15, 16 și 30; A se vedea, de asemenea, Documentul de lucru al serviciilor Comisiei care însoțește Raportul Comisiei către Parlamentul European și Consiliu privind cea de a treia evaluare anuală a Scutului de confidențialitate UE-SUA, p. 17-18.

și „date sensibile”. CEPD salută faptul că definițiile termenilor „date cu caracter personal”, „prelucrare” și „operator” sunt incluse în CCD, astfel cum au fost incluse și în Scutul de confidențialitate.

41. CEPD constată că măsura în care principiile CCD sunt aplicabile organizațiilor CCD care primesc date cu caracter personal din UE în scopuri de „simplă prelucrare” (denumite „agenți” sau „persoane împuternicite de către operator”) rămâne neclară. CCD nu face distincție între principiile CCD aplicabile agenților și principiile CCD aplicabile operatorilor, iar mai multe dintre obligațiile incluse în principiile CCD nu sunt adecvate pentru agenți/persoane împuternicite de operatori. De exemplu, un agent/o persoană împuternicită de operator nu ar trebui să fie în măsură să furnizeze persoanelor toate elementele notificării complete, astfel cum se prevede în principiul notificării (de exemplu, scopurile pentru care colectează și utilizează informații cu caracter personal cu privire la acestea)[34], întrucât un agent/o persoană împuternicită de operator nu poate stabili singur(ă) mijloacele și scopurile prelucrării[35].

2.1.2 Principiul limitării scopului

42. Criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD prevăd, în conformitate cu RGPD, că date cu caracter personal ar trebui să fie prelucrate într-un scop anume și să fie utilizate ulterior numai în măsura în care acest lucru nu este incompatibil cu scopul prelucrării.

43. Principiul integrității datelor și al limitării scopului prevede că o organizație nu poate prelucra informații cu caracter personal într-un mod incompatibil cu scopurile pentru care acestea au fost colectate sau cu scopurile aprobate ulterior de persoana în cauză[36]. CEPD constată că se utilizează o terminologie diferită în secțiunile care tratează principiului notificării, al opțiunii și al integrității datelor și al limitării scopului. Astfel cum a remarcat GL29 și în pofida clarificărilor utile din considerentele proiectului de decizie, termeni precum „scopuri diferite”, „scopuri care diferă în mod semnificativ” sau „o utilizare care nu este în concordanță cu” sunt utilizați în CCD în absența unei definiri clare a conceptelor respective, ceea ce ar putea conduce la insecuritate juridică.

2.1.3 Dreptul de acces, dreptul la rectificare, dreptul la ștergere și dreptul la opoziție

44. În CCD, dreptul de acces, dreptul la rectificare și dreptul la ștergere ale persoanelor vizate sunt reglementate în temeiul principiului accesului[37].

45. Principiul accesului rămâne neschimbat față de Scutul de confidențialitate. În consecință, unele preocupări exprimate în Avizul 01/2016 al GL29 sunt încă valabile, astfel cum se detaliază mai jos.

46. În ceea ce privește dreptul de acces al persoanelor, CEPD consideră că este necesar să reitereze că detaliile privind obligația de a răspunde cererilor din partea persoanelor ar trebui introduse în textul principal al principiului (acestea sunt încă descrise doar într-o notă de subsol[38]).). De asemenea, ar trebui să fie clar faptul că accesul ar trebui acordat în măsura în care o organizație CCD prelucrează

[34] Secțiunea II punctul 1 litera (a) din anexa I la proiectul de decizie.
[35] A se vedea, de asemenea, Avizul 01/2016 al GL29, p. 16.
[36] Secțiunea II punctul 5 din anexa I la proiectul de decizie.
[37] Secțiunea II punctul 6 și secțiunea III punctul 8 litera (a) punctul (i) din anexa I la proiectul de decizie.
[38] Secțiunea III punctul 8 litera (a) punctul (i) subpunctul 1 din anexa I la proiectul de decizie – nota de subsol 14.

informații cu caracter personal, nu numai atunci când le „stochează”[39]. În opinia CEPD, formularea actuală ar putea conduce la o interpretare restrictivă a dreptului de acces.

47. În legătură cu lista excepțiilor cu privire la dreptul de acces[40], unele dintre ele au în continuare tendința de a înclina balanța în favoarea intereselor organizațiilor CCD. CEPD este în continuare preocupat de faptul că, în aceste cazuri, nu pare să existe nicio cerință de a ține seama de drepturile și interesele persoanei în cauză[41].

48. O altă excepție, care a făcut anterior obiectul preocupărilor GL29[42] și pe care CEPD o consideră prea amplă este excepția cu privire la dreptul de acces la informațiile aflate la dispoziția publicului și la informațiile extrase din registrele publice[43]. CEPD a afirmat în repetate rânduri că, în conformitate cu dreptul UE, persoanele vizate au întotdeauna dreptul de acces la datele lor, indiferent dacă datele cu caracter personal au fost sau nu publicate. În cazul în care cererile de acces ar fi respinse pe motiv că datele au fost obținute din surse aflate la dispoziția publicului sau din registre publice, persoanele în cauză și-ar pierde capacitatea de a controla acuratețea datelor și de a verifica dacă acestea au fost făcute publice în mod legal.

49. CEPD reamintește că dreptul de acces este consacrat la articolul 8 alineatul (2) din Cartă. Deși nu este un drept absolut, acesta este fundamental pentru dreptul la protecția datelor cu caracter personal deoarece facilitează exercitarea celorlalte drepturi ale persoanei vizate, cum ar fi dreptul la rectificare și dreptul la ștergerea datelor, precum și dreptul la opoziție[44].

50. Pe lângă dreptul de acces și dreptul la ștergere, persoanele vizate ar trebui să aibă dreptul de a se opune în orice moment, din motive întemeiate și legitime legate de situația lor particulară, prelucrării datelor care le privesc, conform condițiilor specifice stabilite în cadrul juridic al țării terțe[45].

51. În cadrul principiului opțiunii, CCD prevede dreptul la opoziție (dreptul de refuz) în ceea ce privește divulgarea de informații cu caracter personal către o parte terță sau utilizarea informațiilor cu caracter personal într-un scop semnificativ diferit[46]. În plus, persoanele beneficiază în orice moment de dreptul de a renunța la utilizarea informațiilor lor cu caracter personal în scopuri de marketing direct[47]. Cu excepția contextului utilizării în scopuri de marketing direct, nu sunt detaliate modalitățile de exercitare a dreptului la opoziție, în special momentul exercitării acestuia. Prin urmare, CEPD invită Comisia să clarifice modul în care persoanele își pot exercita dreptul la opoziție.

52. Astfel cum se menționează în Avizul 01/2016 al GL29, CEPD consideră că simpla trimitere la existența acestui drept în politica de confidențialitate nu poate fi suficientă, ci ar trebui să se ofere o posibilitate individualizată de a exercita acest drept nu numai în cazul divulgării sau al reutilizării informațiilor cu caracter personal. CEPD subliniază că, în CCD, ar trebui să se ofere un drept general la opoziție din motive întemeiate și legitime legate de situația particulară a persoanei vizate. CEPD recomandă ca

[39] Secțiunea III punctul 8 litera (d) punctul (ii) din anexa I la proiectul de decizie.
[40] Secțiunea III punctul 8 litera (e) din anexa I la proiectul de decizie.
[41] Avizul 01/2016 al GL29, punctul 2.2.5.
[42] Avizul 01/2016 al GL29, punctul 2.2.9.
[43] Secțiunea III punctul 15 literele (d)-(e) din anexa I la proiectul de decizie.
[44] Avizul 01/2016 al GL29, punctul 2.2.5.
[45] Secțiunea 3.A.8. din Criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD.
[46] Secțiunea II punctul 2 litera (a) din anexa I la proiectul de decizie.
[47] Secțiunea III punctul 12 litera (a) din anexa I la proiectul de decizie.

acest drept la opoziție să fie garantat în orice moment și să nu se limiteze la utilizarea datelor în scopuri de marketing direct[48].

53. În legătură cu datele privind resursele umane, CEPD apreciază clarificările Comisiei în ceea ce privește aplicarea principiilor notificării și opțiunii în situația în care o organizație certificată din SUA intenționează să utilizeze date privind resursele umane într-un scop diferit, care nu are legătură cu raportul de muncă, precum comunicările cu caracter publicitar[49]. Cu toate acestea, CEPD susține că prelucrarea ulterioară a datelor privind resursele umane în scopuri care nu au legătură cu raportul de muncă va fi considerată, în majoritatea cazurilor, incompatibilă cu scopul inițial și că, atunci când consimțământul se acordă în contextul unui raport de muncă, acesta va fi rareori complet liber.

54. CEPD reiterează, de asemenea, preocupările GL29 în ceea ce privește derogarea de la aplicarea principiilor notificării și opțiunii în cazul datelor privind resursele umane „în măsura și pe durata necesară, fără a aduce atingere capacității organizației de a lua decizii de promovare, numire sau alte decizii similare privind ocuparea forței de muncă”[50], aceasta fiind, potrivit CEPD, amplă și vagă[51].

2.1.4 Restricții privind transferurile ulterioare de date

55. Transferurile ulterioare de date cu caracter personal efectuate de destinatarul inițial al transferului de date ar trebui să fie autorizate numai în cazul în care noul destinatar (și anume destinatarul transferului ulterior) face, de asemenea, obiectul unor norme (inclusiv norme contractuale) care asigură un nivel de protecție adecvat și urmează instrucțiunile relevante atunci când prelucrează date în numele operatorului de date. Nivelul de protecție a persoanelor fizice ale căror date sunt transferate nu trebuie să fie subminat de transferul ulterior. Destinatarul inițial al datelor transferate din UE este responsabil să asigure faptul că sunt prevăzute garanții adecvate pentru transferurile ulterioare de date în absența unei decizii privind caracterul adecvat al nivelului de protecție. Astfel de transferuri ulterioare de date ar trebui să se realizeze numai pentru scopuri specificate și limitate și în măsura în care există un temei juridic pentru prelucrarea respectivă[52].

56. În conformitate cu principiului responsabilității pentru transferurile ulterioare al CCD, transferurile ulterioare pot avea loc numai în scopuri limitate și specificate, pe baza unui contract încheiat între organizația CCD și partea terță (sau a unui acord asemănător în cadrul unui grup de întreprinderi) și numai în cazul în care contractul respectiv îi impune părții terțe în cauză să asigure același nivel de protecție precum cel garantat de principiile CCD[53].

57. CEPD ar dori să reitereze preocupările exprimate în Avizul 01/2016 al GL29 cu privire la derogarea de la necesitatea de a încheia un contract pentru transferurile între operatori realizate în cadrul grupului[54]. În legătură cu datele privind resursele umane, CEPD continuă să nu înțeleagă justificarea

[48] Avizul 01/2016 al GL29, punctul 2.2.2.
[49] Secțiunea III punctul 9 litera (b) punctul (i) din anexa I la proiectul de decizie, precum și considerentul 15 și nota de subsol 27 din acesta.
[50] Secțiunea III punctul 9 litera (b) punctul (iv) din anexa I la proiectul de decizie.
[51] Avizul 01/2016 al GL29, punctul 2.2.7.
[52] Secțiunea 3.A.9 din Criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD.
[53] Secțiunea II punctul 3 din anexa I la proiectul de decizie.
[54] Secțiunea III punctul 10 litera (b) punctul (i) din anexa I la proiectul de decizie, cu includerea formulării „sau [pe baza] altor instrumente din cadrul grupului (de exemplu, programe de conformitate și control”), care, aparent, nu trebuie să fie obligatorii.

derogării de la obligația de a încheia un contract cu un operator terț în cazul transferurilor ulterioare pentru „necesități operaționale ocazionale în contextul unui raport de muncă”[55].

58. În plus, CEPD ar dori să repete solicitarea GL29[56] ca organizațiile care intră sub incidența cadrului să evalueze, înainte de efectuarea unui transfer ulterior, dacă respectivele cerințe obligatorii ale legislației naționale a țării terțe aplicabile destinatarului nu ar submina continuitatea protecției persoanelor vizate ale căror date sunt transferate[57].

59. CEPD susține că transferurile ulterioare de date cu caracter personal către țări terțe ar putea duce la ingerințe în drepturile fundamentale ale persoanelor și invită Comisia să clarifice faptul că garanțiile impuse de destinatarul inițial importatorului din țara terță trebuie să fie eficace în lumina legislației țării terțe, înainte de realizarea unui transfer ulterior în contextul CCD[58].

2.1.5 Procesul decizional automatizat și crearea de profiluri

60. Deciziile bazate exclusiv pe prelucrarea automată (procesul decizional individual automatizat), inclusiv crearea de profiluri, care produc efecte juridice sau care afectează în mod semnificativ persoana vizată pot avea loc numai în anumite condiții stabilite în cadrul juridic al țării terțe. În cadrul european, aceste condiții includ, de exemplu, necesitatea de a obține consimțământul explicit al persoanei vizate sau necesitatea unei astfel de decizii pentru încheierea unui contract. În cazul în care decizia nu respectă astfel de condiții stabilite în cadrul juridic al țării terțe, persoana vizată ar trebui să aibă dreptul de a nu face obiectul deciziei respective. Legislația țării terțe ar trebui, în orice caz, să prevadă garanțiile necesare, inclusiv dreptul de a fi informat cu privire la motivele specifice care stau la baza deciziei și logica implicată, de a corecta informațiile inexacte sau incomplete, precum și de a contesta decizia în cazul în care aceasta s-a întemeiat pe o bază factuală incorectă[59].

61. CCD nu prevede nicio garanție juridică specifică în cazul în care persoanele fac obiectul unor decizii care produc efecte juridice în ceea ce le privește sau care le afectează în mod semnificativ și care se bazează exclusiv pe prelucrarea automată a datelor menită să evalueze anumite aspecte personale referitoare la acestea, cum ar fi randamentul lor profesional, solvabilitatea, încrederea pe care o prezintă sau conduita.

62. Astfel cum s-a luat deja în considerare în Avizul 01/2016 al GL29 și de către CEPD în avizele anterioare asupra deciziilor privind caracterul adecvat al nivelului de protecție referitoare la Japonia și Coreea de

---

[55] Secțiunea III punctul 9 litera (e) punctul (i) din anexa I la proiectul de decizie, care include exemple precum asigurările.

[56] Avizul 01/2016 al GL29, punctul 2.2.3, p. 21.

[57] Având în vedere hotărârea *Schrems II*, CEPD a oferit clarificări suplimentare privind obligațiile exportatorilor și importatorilor de date în ceea ce privește transferurile ulterioare într-o serie de orientări și recomandări: a se vedea Recomandările 01/2020 ale CEPD privind măsurile care completează instrumentele de transfer pentru a asigura conformitatea cu nivelul UE de protecție a datelor cu caracter personal (versiunea 2.0; adoptate la 18 iunie 2021); Recomandările 02/2020 privind garanțiile esențiale europene pentru măsurile de supraveghere (adoptate la 10 noiembrie 2020); Orientările nr. 04/2021 privind codurile de conduită ca instrumente pentru transferuri (versiunea 2.0; adoptate la 22 februarie 2022); Recomandările 1/2022 privind cererea de aprobare și privind elementele și principiile care se regăsesc în regulile corporatiste obligatorii pentru operatori (adoptate la 14 noiembrie 2022); Orientările nr. 07/2022 privind certificarea ca instrument pentru transferuri (adoptate la 14 februarie 2023, în urma consultării publice).

[58] Avizul 01/2016 al GL29, punctul 2.2.3, p. 21.

[59] Secțiunea 3.B.3. din Criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD.

Sud[60], CEPD constată că evoluțiile rapide în domeniul procesului decizional automatizat și al creării de profiluri – din ce în ce mai mult prin intermediul tehnologiilor IA – necesită o atenție deosebită în acest sens[61].

63. CEPD ia act de argumentele Comisiei, potrivit cărora este puțin probabil ca inexistența în CCD a unor norme specifice privind procesul decizional automatizat să afecteze nivelul de protecție în ceea ce privește datele cu caracter personal care au fost colectate în Uniune (întrucât orice decizie bazată pe prelucrarea automată ar fi, de regulă, luată de operatorul din Uniune care are o relație directă cu persoana vizată în cauză)[62]. Cu toate acestea, în opinia CEPD, nu poate fi exclus faptul că procesul decizional automatizat ar putea fi utilizat de un operator cu sediul în SUA cu privire la datele transferate în temeiul proiectului de decizie (de exemplu, în contextul unui raport de muncă, pentru evaluarea randamentului la locul de muncă, în legătură cu asigurările sau locuințele).

64. CEPD salută trimiterile Comisiei la garanții specifice prevăzute de legislația relevantă a SUA în diferite domenii[63]. Cu toate acestea, în opinia CEPD, nivelul de protecție a persoanelor pare să difere în funcție de normele sectoriale – dacă există – care se aplică situației în cauză. Există riscul ca unele situații să nu fie acoperite deoarece nu intră în domeniul de aplicare al actelor legislative menționate. În plus, conținutul drepturilor individuale în ceea ce privește procesul decizional automatizat este descris în mod diferit în diversele acte legislative.

65. În acest context, CEPD consideră că este necesară introducerea în CCD a unor norme specifice privind procesul decizional automatizat pentru a oferi garanții suficiente, inclusiv dreptul persoanei de a cunoaște logica implicată, de a contesta decizia și de a obține intervenție umană atunci când decizia o afectează în mod semnificativ[64].

2.2 Mecanisme procedurale și de asigurare a respectării legii

66. CEPD constată că, în continuare, CCD se bazează pe un sistem de autocertificare, chiar dacă acesta este considerat de către Comisie drept un sistem de „certificare".

67. CEPD reamintește îmbunătățirile aduse în urma revizuirilor comune anterioare, de exemplu, în ceea ce privește rolul DoC, în ceea ce privește procesul de (re)autocertificare [...], monitorizarea respectării de către societăți a principiilor CCD (de pildă, prin controale la fața locului sau utilizarea chestionarelor de conformitate) și identificarea și abordarea declarațiilor false de participare (de exemplu, prin căutări pe internet).

68. În același timp, GL29 și CEPD și-au exprimat îngrijorarea cu privire la o anumită lipsă de supraveghere a respectării cerințelor Scutului de confidențialitate[65]. În special, CEPD este de acord cu constatările Comisiei în urma celei de a treia revizuiri anuale a Scutului de confidențialitate, și anume că, în temeiul

---

[60] Avizul 28/2018 al CEPD referitor la Proiectul de decizie de punere în aplicare al Comisiei Europene privind nivelul de protecție adecvat a datelor cu caracter personal în Japonia, adoptat la 5 decembrie 2018; Avizul 32/2021 al CEPD referitor la Proiectul de decizie de punere în aplicare a Comisiei Europene în temeiul Regulamentului (UE) 2016/679 privind protecția adecvată a datelor cu caracter personal în Republica Coreea, adoptat la 24 septembrie 2021.

[61] A se vedea, *printre altele*, cauza C-634/21, *OQ/Land Hesse (SCHUFA Holding și alții)* – Cerere de decizie preliminară (în curs de soluționare).

[62] Considerentele 33 și 34 din proiectul de decizie.

[63] Considerentul 35 din proiectul de decizie.

[64] A se vedea, de asemenea, raportul aferent celei de a treia revizuiri comune, punctul 76.

[65] Raportul aferent celei de a treia revizuiri comune, punctul 7.

Scutului de confidențialitate aceste controale la fața locului ale DoC au tins să se limiteze la cerințele formale(cum ar fi lipsa răspunsului din partea punctelor de contact desemnate sau inaccesibilitatea online a politicii de confidențialitate a unei societăți)[66]. CEPD consideră că verificările conformității în ceea ce privește cerințele de fond sunt esențiale.

69. De asemenea, CEPD reamintește importanța supravegherii eficace (inclusiv a respectării cerințelor de fond) și a asigurării respectării efective a CCD. Acest aspect va fi monitorizat îndeaproape de CEPD, inclusiv în contextul revizuirilor periodice.

70. În ceea ce privește asigurarea respectării CCD, CEPD ia act de angajamentele reînnoite exprimate în scrisorile FTC[67] și DoT[68] de investigare cu prioritate a presupuselor încălcări ale CCD, de luare a măsurilor corespunzătoare de asigurare a respectării CCD împotriva entităților care fac declarații false sau frauduloase de participare, de monitorizare a ordinelor de executare privind încălcările CCD și de cooperare cu APD din UE. În acest sens, CEPD recunoaște, de asemenea, că FTC a indicat că se așteaptă să își concentreze în continuare eforturile de asigurare a respectării CCD asupra încălcărilor de fond ale acestuia și că intenționează să investigheze încălcările (și) din proprie inițiativă. Aceste aspecte vor fi monitorizate îndeaproape de CEPD, inclusiv în contextul revizuirilor periodice.

2.3 Mecanisme de recurs

71. CEPD salută prezentarea clară în proiectul de decizie a celor șapte modalități de recurs acordate persoanelor vizate din UE în cazul în care datele lor cu caracter personal sunt prelucrate cu încălcarea CCD[69].

72. Aceste mecanisme diferite de recurs sunt stabilite în conformitate cu cerințele principiului recursului, al punerii în aplicare și al responsabilității și ale principiului suplimentar 11 privind „soluționarea litigiilor și punerea în aplicare a deciziilor" emis de DoC și menționat în anexa I la proiectul de decizie[70].

73. Astfel cum a subliniat Comisia în proiectul de decizie, „persoanei vizate ar trebui să i se pună la dispoziție căi de atac administrative și judiciare efective"[71]. Această formulare reflectă cerința prevăzută la articolul 45 alineatul (2) litera (a) din RGPD, care impune Comisiei, în cadrul evaluării sale privind caracterul adecvat al nivelului de protecție asigurat de o țară terță, să țină seama în special de „reparații[le] efective pe cale administrativă și judiciară pentru persoanele vizate ale căror date cu caracter personal sunt transferate"[72]. Această cerință este reamintită, de asemenea, în Criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD[73].

74. CEPD constată că aceste mecanisme de recurs sunt aceleași precum cele incluse în Scutul de confidențialitate anterior, care au făcut obiectul unor observații din partea GL29[74].

---

[66] Raportul Comisiei către Parlamentul European și Consiliu privind cea de a treia evaluare anuală a Scutului de confidențialitate UE-SUA [23.10.2019, COM(2019) 495 final], p. 4.
[67] Anexa IV la proiectul de decizie.
[68] Anexa V la proiectul de decizie.
[69] Considerentul 67 din proiectul de decizie.
[70] Secțiunea II punctul 7 și secțiunea III punctul 11 din anexa I la proiectul de decizie și anexa I la anexa I.
[71] Considerentul 64 din proiectul de decizie.
[72] A se vedea, de asemenea, considerentul 141 din RGPD care face trimitere la articolul 47 din Carta Drepturilor Fundamentale pentru dreptul la o cale de atac eficientă în UE.
[73] Criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD, p. 8.
[74] A se vedea, în special, secțiunea 2.2.6 litera (a) din Avizul 01/2016 al GL29.

75. În ceea ce privește mecanismul de arbitraj, CEPD constată că această opțiune nu este disponibilă în ceea ce privește derogările de la principiile CCD[75] și, prin urmare, face trimitere la observația sa formulată la punctul 33.

76. În ceea ce privește alte căi de atac judiciare disponibile în temeiul legislației SUA, CEPD ar aprecia, de asemenea, detalii suplimentare cu privire la legislația menționată[76] și face trimitere la observația sa formulată la punctul 21.

77. În plus, CEPD salută scrisoarea FTC în care aceasta își exprimă intenția de a colabora îndeaproape cu APD din UE[77]. CEPD salută, de asemenea, angajamentul FTC de a acorda prioritate soluționării plângerilor, deși este posibil ca acest lucru să nu ofere certitudine persoanelor vizate cum că plângerile înaintate de acestea vor fi examinate în toate cazurile.

78. În ceea ce privește posibilitatea, în anumite cazuri, ca persoanele să își prezinte plângerile unei APD din UE, CEPD ar aprecia furnizarea de informații suplimentare (i) cu privire la măsura în care posibilitatea APD din UE de a oferi consiliere cu privire la măsuri reparatorii sau compensatorii ar putea include recomandarea impunerii unor amenzi sau utilizarea competențelor de investigare și (ii) măsura în care acțiunea APD din UE ar fi luată în considerare ca dovadă pentru acțiunile de asigurare a respectării CCD întreprinse de FTC sau DoT[78].

79. Eficacitatea mecanismelor de recurs va fi monitorizată îndeaproape de CEPD, inclusiv în contextul revizuirilor periodice.

3 ACCESAREA ȘI UTILIZAREA DE CĂTRE AUTORITĂȚILE PUBLICE DIN SUA A DATELOR CU CARACTER PERSONAL TRANSFERATE DIN UNIUNEA EUROPEANĂ

3.1 Accesarea și utilizarea datelor în scopul asigurării respectării legii penale

3.1.1 Accesul autorităților de aplicare a legii la datele cu caracter personal ar trebui să se bazeze pe norme clare, precise și accesibile.

80. CEPD apreciază informațiile și explicațiile mai detaliate în comparație cu decizia anterioară privind caracterul adecvat al nivelului de protecție, prevăzute în proiectul de decizie în ceea ce privește accesarea și utilizarea datelor cu caracter personal de către autoritățile publice din SUA în scopul asigurării respectării legii penale. Anexa VI din proiectul de decizie include, de asemenea, o scrisoare din partea Departamentului de Justiție al SUA – Divizia Penală „care conține o scurtă prezentare generală a principalelor instrumente de investigare utilizate pentru obținerea de date comerciale și a altor informații din registre de la societățile din Statele Unite ale Americii în scopul asigurării respectării legii penale sau în interes public (civil și de reglementare), inclusiv a limitărilor cu privire la acces prevăzute de mecanismele respective”. Potrivit scrisorii, toate procesele juridice descrise în scrisoare se utilizează pentru obținerea de informații de la societățile din SUA, fără a ține cont de cetățenia sau locul de reședință al persoanei vizate, și decurg în mod direct din Constituția SUA (al patrulea

[75] Anexa I partea A din anexa I la proiectul de decizie.
[76] Considerentul 85 din proiectul de decizie.
[77] Anexa IV la proiectul de decizie.
[78] Secțiunea III punctul 5 litera (b) punctul (iii) din anexa I la proiectul de decizie.

amendament), din dreptul material și procedural sau din orientările și politicile Departamentului de Justiție. Această prezentare generală nu vizează instrumentele de investigare în materie de securitate națională utilizate de autoritățile de aplicare a legii în investigații cu privire la terorism și alte investigații privind securitatea națională[79].

81. CEPD constată că proiectul de decizie și anexa VI la acesta tratează în principal aspecte legate de autoritățile federale de aplicare a legii și de reglementare[80] și nu se referă în mod specific la legislația la nivel de stat care prevede astfel de proceduri de obținere a informațiilor. Anexa VI menționează, de asemenea, că „există alte temeiuri juridice în baza cărora societățile pot contesta solicitările de date primite din partea agențiilor administrative în funcție de industriile specifice ale acestora și de tipurile de date pe care le dețin", oferind, în plus, mai multe exemple neexhaustive, cum ar fi Legea privind secretul bancar (*Bank Secrecy Act*) și regulamentele sale de punere în aplicare[81], Legea privind raportarea echitabilă a creditelor (*Fair Credit Reporting Act*)[82] și Legea privind dreptul la confidențialitatea informațiilor financiare (*Right to Financial Privacy Act*)[83]. CEPD constată că temeiul juridic aplicabil unei anumite solicitări de acces depinde de natura datelor solicitate, de natura societății, de natura procedurilor juridice (penale, administrative, legate de alte interese publice) și de natura entității care solicită accesul. Întrucât toate normele aplicabile pentru a limita accesul autorităților de aplicare a legii la datele transferate către SUA se bazează pe Constituție, pe dreptul material și pe politicile transparente ale Departamentului de Justiție, CEPD recunoaște accesibilitatea acestor norme și invită Comisia să reflecte acest element în proiectul de decizie. Din anexa VI rezultă că aceste legi se aplică indiferent de cetățenie sau de locul de reședință al persoanei vizate și includ, în general, cerințele celui de al Patrulea Amendament (deși, adesea, acestea depășesc aceste cerințe și includ măsuri de protecție suplimentare).

82. În concluzie, CEPD ia act de evaluarea mai detaliată cuprinsă în proiectul de decizie în comparație cu decizia anterioară privind caracterul adecvat al nivelului de protecție în ceea ce privește accesul autorităților federale de aplicare a legii. În ceea ce privește accesul autorităților de aplicare a legii la nivel de stat, CEPD constată, de asemenea, că, în conformitate cu anexa VI, măsurile de protecție în temeiul legislației la nivel de stat trebuie să fie cel puțin egale cu cele prevăzute de Constituția SUA, inclusiv, dar fără a se limita la cel de al Patrulea Amendament. CEPD invită Comisia să evalueze suplimentar elementul de protecție conferit în temeiul legislației la nivel de stat în cadrul viitoarelor revizuiri.

3.1.2 Trebuie să se demonstreze necesitatea și proporționalitatea în raport cu obiectivele legitime urmărite

83. CEPD constată în mod corespunzător că solicitarea accesului la date în scopul asigurării respectării legii poate fi considerată, în general, ca urmărind un obiectiv legitim. Cu toate acestea, în același timp, astfel de ingerințe sunt acceptabile numai atunci când sunt necesare și proporționale[84].

---

[79] Nota de subsol 1 din anexa VI la proiectul de decizie.
[80] A se vedea considerentele 90-93 din proiectul de decizie.
[81] Titlul 31 articolul 5318 din U.S.C.; titlul 31 capitolul X din C.F.R. – Codul regulamentelor federale (*Code of Federal Regulations*).
[82] Titlul 15 articolul 1681b din U.S.C.
[83] Titlul 12 articolele 3401-3423 din U.S.C.
[84] A se vedea Hotărârea Curții de Justiție din 6 octombrie 2020 în cauzele conexate C-511/18, C-512/18 și C-520/18, La Quadrature du Net și alții, ECLI:EU:C:2020:791 („hotărârea La Quadrature du Net a CJUE"), punctul 140. A se vedea, de asemenea, AEPD, *Assessing the necessity of measures that limit the fundamental*

84. Potrivit jurisprudenței constante a CJUE, principiul proporționalității impune ca măsurile legislative care introduc ingerințe în dreptul la viață privată și la protecția datelor cu caracter personal „să fie de natură să atingă obiectivele legitime urmărite de reglementarea în cauză și să nu depășească limitele a ceea ce este adecvat și necesar pentru realizarea acestor obiective”[85]. Prin urmare, evaluarea necesității și a proporționalității se face întotdeauna, în principiu, în legătură cu o măsură specifică prevăzută de legislație.

85. Autoritățile SUA precizează în anexa VI că procurorii federali și agenții federali de investigații sunt în măsură să obțină accesul la documente și la alte informații din registre din partea organizațiilor prin intermediul „mai multor tipuri de procese juridice obligatorii, inclusiv prin citații emise de marele juriu, citații administrative și mandate de percheziție” și pot obține alte comunicări „în baza mecanismelor federale de interceptare a comunicațiilor în temeiul legislației penale”[86]. În plus, agențiile cu responsabilități civile și de reglementare pot emite citații organizațiilor în legătură cu „documente comerciale, informații stocate electronic sau alte elemente tangibile”[87]. Procesele în sine sunt explicate, de asemenea, în considerentele 90-93 din proiectul de decizie. CEPD remarcă, în acest sens, evoluția pozitivă a jurisprudenței SUA în ceea ce privește informațiile stocate electronic, menționată în proiectul de decizie[88].

86. Anexa VI precizează, de asemenea, că aceste proceduri judiciare sunt nediscriminatorii și sunt utilizate, în general, pentru a obține informații de la „societățile” din SUA, indiferent dacă acestea sunt certificate sau nu în temeiul Cadrului UE-SUA privind confidențialitatea datelor și „fără a ține cont de cetățenia sau locul de reședință al persoanei vizate”.

87. În plus, anexa VI conține aspecte cu privire la garanțiile prevăzute în temeiul celui de al Patrulea Amendament al Constituției SUA, potrivit cărora percheziții și punerea sub sechestru efectuate de autoritățile de aplicare a legii necesită în principal un mandat emis de instanță pe baza unui motiv întemeiat și cu respectarea cerințelor privind caracterul particular al mandatului și menționează că, în cazuri excepționale în care cerința prezentării mandatului nu se aplică, măsura de asigurare a respectării legii face obiectul unui test privind caracterul rezonabil în temeiul celui de al Patrulea Amendament[89]. O persoană care face obiectul unei percheziții sau ale cărei bunuri fac obiectul unei

---

right to the protection of personal data: A Toolkit (Evaluarea necesității unor măsuri care limitează dreptul fundamental la protecția datelor cu caracter personal: un set de instrumente), 11 aprilie 2017 și AEPD, *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data* (Orientări privind evaluarea proporționalității măsurilor care limitează drepturile fundamentale la viață privată și la protecția datelor cu caracter personal), 19 decembrie 2019.

[85] A se vedea Hotărârea Curții de Justiție din 8 aprilie 2014 în cauzele conexate C-293/12 și C-594/12, Digital Rights Ireland, ECLI:EU:C:2014:238 („hotărârea Digital Rights Ireland a CJUE”), punctul 46 și jurisprudența citată în aceasta.

[86] Anexa VI la proiectul de decizie, p. 2.

[87] Anexa VI la proiectul de decizie, p. 4.

[88] A se vedea nota de subsol 146 din proiectul de decizie. Într-o hotărâre din 2018, Curtea Supremă a SUA a confirmat că autoritățile de aplicare a legii necesită un mandat de percheziție sau o renunțare la prezentarea unui mandat pentru a avea acces la istoricul de localizare al celulelor, care oferă o imagine de ansamblu cuprinzătoare asupra deplasărilor unui utilizator și că utilizatorul se poate aștepta în mod rezonabil la respectarea vieții private în ceea ce privește aceste informații [Timothy Ivory Carpenter/Statele Unite ale Americii, nr. 16-402, 585 U.S. (2018)].

[89] A se vedea anexa VI la proiectul de decizie, p. 2.

percheziții poate solicita invalidarea probelor obținute sau rezultate în urma unei percheziții ilegale în cazul în care se aduc astfel de probe împotriva persoanei respective în cursul unui proces penal[90].

88. În concluzie, CEPD constată că sistemul de instrumente de investigare utilizate pentru obținerea de date comerciale și alte informații din registre de la societățile din Statele Unite în scopul asigurării respectării legii penale sau în interes public – inclusiv limitările cu privire la acces și garanțiile prevăzute – oferă un sistem de măsuri cuprinzător, însă complex, care reflectă, printre altele, caracterul federal al guvernului SUA.

89. Astfel, s-ar putea considera că sistemul de măsuri de investigare din SUA în materie de asigurare a respectării legii îndeplinește, în general, cerințele de necesitate și proporționalitate în ceea ce privește drepturile fundamentale la viață privată și la protecția datelor.

3.1.3 Ar trebui să existe un mecanism de supraveghere independent

90. CEPD constată în mod corespunzător că majoritatea procedurilor descrise în proiectul de decizie și în anexa VI presupun implicarea unei hotărâri a unei instanțe înainte ca autoritățile să obțină accesul la date [de exemplu, hotărâri judecătorești de interceptare, capturare și trasabilitate[91], ordine judecătorești de supraveghere în temeiul Legii federale privind interceptarea comunicațiilor (*Federal Wiretap Law*)[92], mandate de percheziție – Codul federal de procedură penală (*Federal Rules of Criminal Procedure*), norma 41[93]]. Cu toate acestea, se pare că nu toate procedurile impun implicarea *a priori* a unei instanțe. De exemplu, autoritățile civile și de reglementare „pot emite citații”[94]. În aceste cazuri, există însă posibilitatea unui control judiciar *ex post* al caracterului rezonabil al citației, întrucât „un destinatar al unei citații administrative poate contesta respectiva citație în instanță”[95].

91. În plus, proiectul de decizie descrie activitatea de supraveghere a agențiilor federale de aplicare a legislației penale de către diferite organisme, de la controlul intern asigurat de responsabilii pentru protecția vieții private și a libertăților civile până la controlul extern exercitat de inspectorul general și de anumite comitete din cadrul Congresului SUA[96]. Comisia Europeană oferă informații nuanțate și detaliate și, în general, ajunge la concluzii ușor de înțeles. Prin urmare, CEPD se abține de la reproducerea constatărilor și evaluărilor factuale în prezentul aviz.

92. Pe baza informațiilor disponibile, CEPD constată că, în ceea ce privește accesul autorităților de aplicare a legii la datele deținute de societăți din SUA, există un mecanism de supraveghere independent destul de robust.

3.1.4 Persoanele trebuie să dispună de căi de atac eficiente

93. Potrivit jurisprudenței CJUE, persoanele trebuie să dispună de o cale de atac eficientă pentru a-și exercita drepturile atunci când consideră că acestea nu sunt sau nu au fost respectate. CJUE a explicat în hotărârea Schrems I că „o reglementare care nu prevede nicio posibilitate a justițiabilului de a exercita căi legale pentru a avea acces la date cu caracter personal care îl privesc sau pentru a obține rectificarea sau ștergerea unor astfel de date nu respectă nici substanța dreptului fundamental la o

[90] A se vedea considerentul 90 din proiectul de decizie.
[91] A se vedea considerentul 92 din proiectul de decizie.
[92] A se vedea anexa VI la proiectul de decizie, p. 3.
[93] A se vedea considerentul 90 din proiectul de decizie și anexa VI la acesta, p. 3.
[94] A se vedea anexa VI la proiectul de decizie, p. 4, precum și considerentul 91 din acesta.
[95] A se vedea anexa VI la proiectul de decizie, p. 4, precum și considerentul 91 din acesta.
[96] A se vedea considerentele 103-106 din proiectul de decizie.

protecție jurisdicțională efectivă, astfel cum este consacrat la articolul 47 din Cartă. Astfel, articolul 47 primul paragraf din Cartă impune ca orice persoană ale cărei drepturi și libertăți garantate de dreptul Uniunii sunt încălcate să aibă dreptul la o cale de atac efectivă în fața unei instanțe judecătorești, în conformitate cu condițiile stabilite de acel articol"[97].

94. Proiectul de decizie[98] și anexa VI la acesta conțin informații suplimentare cu privire la posibilele căi de atac care decurg din dreptul material, aflate la dispoziția persoanelor atunci când autoritățile publice obțin accesul la datele lor în mod ilegal.

95. În această privință, potrivit Comisiei[99], titlul 5 articolul 702 din U.S.C. [Legea privind procedura administrativă (*Administrative Procedure Act* – APA)] prevede că o persoană care este victima unui abuz juridic în urma acțiunilor agenției sau este afectată ori lezată într-un alt mod în urma acțiunilor agenției în sensul unei legi relevante are dreptul la un control jurisdicțional al acestora.

96. În plus, Legea privind comunicațiile stocate (*Stored Communications Act* – SCA) [adoptată ca titlul II din Legea privind confidențialitatea comunicațiilor electronice (*Electronic Communications Privacy Act*)] prevede că orice persoană lezată de orice încălcare a capitolului respectiv în care comportamentul care constituie încălcarea este realizat în cunoștință de cauză sau cu intenție poate obține impunerea unor măsuri reparatorii corespunzătoare, în cadrul unei acțiuni civile, asupra persoanei sau a entității respective, alta decât Statele Unite ale Americii, care a participat la încălcarea respectivă[100]. În plus, orice persoană care este lezată de o încălcare a capitolului respectiv sau a capitolului 119 săvârșită cu intenție poate iniția o acțiune în fața Curții Districtuale a Statelor Unite ale Americii (*United States District Court*) împotriva Statelor Unite ale Americii pentru a obține despăgubiri bănești[101].

97. În plus, proiectul de decizie conține, de asemenea, informații privind dreptul de a obține accesul la evidențele agențiilor federale în temeiul Legii privind libertatea de informare (*Freedom of Information Act* – FOIA)[102] și al altor legi care conferă persoanelor dreptul de a introduce o acțiune împotriva unei autorități publice sau a unui funcționar public din SUA cu privire la prelucrarea datelor lor cu caracter personal, cum ar fi Legea privind interceptarea comunicațiilor (*Wiretap Law*), Legea privind fraudele și abuzurile informatice (*Computer Fraud and Abuse Act*), Legea federală privind acțiunile în răspundere civilă (*Federal Torts Claim Act*), Legea privind dreptul la confidențialitatea informațiilor financiare și Legea privind raportarea echitabilă a creditelor[103].

98. Prin urmare, CEPD salută clarificările furnizate de Comisie cu privire la căile de atac judiciare aflate la dispoziția persoanelor. CEPD invită, de asemenea, Comisia să clarifice și dacă aceste căi de atac îi permit persoanei vizate „[să aibă] acces la date cu caracter personal care [o] privesc sau [să obțină] rectificarea sau ștergerea unor astfel de date", în conformitate cu cerințele CJUE.

---

[97] Hotărârea Schrems I a CJUE, punctul 95.
[98] A se vedea considerentele 107-112 din proiectul de decizie.
[99] A se vedea considerentul 109 din proiectul de decizie.
[100] Titlul 18 articolul 2707 din U.S.C.
[101] Titlul 18 articolul 2712 din U.S.C.
[102] A se vedea considerentul 111 din proiectul de decizie.
[103] A se vedea considerentul 112 din proiectul de decizie.

3.1.5 Utilizarea ulterioară a informațiilor colectate

3.1.5.1 Utilizarea ulterioară a datelor transferate accesate de autoritățile de aplicare a legii din SUA

99. CEPD constată în sens pozitiv că proiectul de decizie evaluează utilizarea ulterioară a datelor accesate de autoritățile de aplicare a legii din SUA. Cu toate acestea, CEPD regretă faptul că se oferă doar un exemplu de temeiuri în baza cărora poate avea loc o diseminare ulterioară a informațiilor[104]. În acest sens, CEPD recomandă Comisiei să includă clarificări suplimentare în proiectul de decizie cu privire la principiile și garanțiile aplicabile utilizării ulterioare a datelor, cum ar fi cele incluse în Legea privind protecția informațiilor cu caracter personal (*Privacy Act*) (titlul 5 articolul 552a din U.S.C.)[105].

3.1.5.2 Transferuri ulterioare în afara SUA

100. De asemenea, CEPD constată că, deși Comisia Europeană a făcut referire la transferurile ulterioare de la autoritățile de aplicare a legii din SUA către autoritățile din țări terțe, aceasta a avut în vedere numai Orientările procurorului general privind operațiunile interne ale FBI (AGG-DOM)[106]. CEPD consideră că astfel de informații și de analize sunt esențiale pentru a permite o evaluare cuprinzătoare a nivelului de protecție oferit de cadrul legislativ și de practicile utilizate în SUA cu privire la divulgarea și la utilizarea ulterioară a datelor la nivel internațional. Având în vedere că, în ceea ce privește transferurile ulterioare în afara SUA în ansamblul lor, Comisia a dat un singur exemplu limitat, CEPD invită Comisia să aducă o serie de clarificări suplimentare cu privire la normele și garanțiile aplicabile transferurilor ulterioare, precum și utilizării și divulgării ulterioare a informațiilor cu caracter personal colectate în scopul asigurării respectării legii în SUA și transferate ulterior către țări terțe, inclusiv în temeiul acordurilor internaționale.

3.2 Accesarea și utilizarea datelor în scopuri legate de securitatea națională

101. Ca observație generală, CEPD recunoaște că statelor li se acordă o marjă largă de apreciere în materie de securitate națională, recunoscută, de asemenea, de CEDO. CEPD reamintește, de asemenea, că, astfel cum a subliniat în recomandările sale actualizate privind garanțiile esențiale europene pentru măsurile de supraveghere[107], articolul 6 alineatul (3) din Tratatul privind Uniunea Europeană prevede că drepturile fundamentale consacrate în Convenția Europeană a Drepturilor Omului constituie principii generale ale dreptului Uniunii. Cu toate acestea, astfel cum reamintește CJUE în jurisprudența sa, aceasta din urmă nu constituie, atât timp cât UE nu a aderat la ea, un instrument juridic integrat formal în ordinea juridică a Uniunii[108]. Astfel, nivelul de protecție a drepturilor fundamentale impus de articolul 45 din RGPD trebuie stabilit pe baza dispozițiilor acestui regulament, interpretate în lumina drepturilor fundamentale consacrate de Carta Drepturilor Fundamentale a Uniunii Europene. Acestea fiind spuse, în conformitate cu articolul 52 alineatul (3) din Cartă, drepturile cuprinse în aceasta care corespund unor drepturi garantate prin Convenția Europeană a Drepturilor Omului au același înțeles și întindere ca și cele prevăzute de Convenția Europeană a Drepturilor Omului. În consecință, astfel cum a reamintit CJUE, trebuie să se țină seama de jurisprudența CEDO privind drepturile care sunt prevăzute, de asemenea, în Carta Drepturilor Fundamentale a Uniunii Europene ca prag minim de

[104] A se vedea considerentul 102 din proiectul de decizie.
[105] A se vedea secțiunea B punctul 1 litera (g) din Orientările procurorului general cu privire la operațiunile interne ale FBI (*Attorney General Guidelines for Domestic FBI Operations*) (AGG-DOM), p. 36.
[106] A se vedea considerentul 102 din proiectul de decizie.
[107] A se vedea Recomandările 02/2020 ale CEPD privind garanțiile esențiale europene pentru măsurile de supraveghere.
[108] A se vedea hotărârea Schrems II a CJUE, punctul 98.

protecție pentru interpretarea drepturilor corespunzătoare din Cartă[109]. Cu toate acestea, ultima teză din articolul 52 alineatul (3) din Carta Drepturilor Fundamentale a Uniunii Europene prevede că „[a]ceastă dispoziție nu împiedică dreptul Uniunii să confere o protecție mai largă".

102. Prin urmare, în evaluarea următoare, CEPD a ținut seama de jurisprudența CEDO, în măsura în care Carta Drepturilor Fundamentale a Uniunii Europene, astfel cum a fost interpretată de CJUE, nu conferă un nivel mai ridicat de protecție care să prevadă alte cerințe decât jurisprudența CEDO.

103. Cadrul juridic al SUA include mai multe instrumente juridice care prevăd posibilitatea colectării și a accesării și prelucrării ulterioare de date de către serviciile de informații din SUA.

104. Astfel cum reamintește Comisia Europeană în proiectul de decizie, „serviciile de informații din SUA pot solicita accesul la datele cu caracter personal care au fost transferate către organizații din Statele Unite ale Americii numai în scopuri legate de securitatea națională, astfel cum este autorizat prin lege, în special în temeiul Legii privind supravegherea activităților străine de spionaj (FISA) sau al dispozițiilor legale care autorizează accesul prin intermediul scrisorilor privind securitatea națională (NSL)"[110]. „Serviciile de informații din SUA au, de asemenea, posibilitatea de a colecta date cu caracter personal în afara Statelor Unite ale Americii, astfel de date putând include date cu caracter personal aflate în tranzit între Uniune și Statele Unite ale Americii" în temeiul Ordinului executiv nr. 12333 (OE nr. 12333)[111].

105. În ceea ce privește regimurile specifice de colectare a datelor, în special articolul 702 din FISA și OE nr. 12333, OE nr. 14086 prevede în prezent noi norme de consolidare a garanțiilor pentru activitățile SUA de colectare de informații pe baza semnalelor electromagnetice. Aceste norme generale se aplică orizontal și „trebuie puse în aplicare în continuare prin politici și proceduri ale serviciilor, care le transpun în direcții concrete pentru operațiunile de zi cu zi"[112]. OE.nr. 14086 a înlocuit în cea mai mare parte Directiva nr. 28 privind politica prezidențială anterioară („PPD-28")[113].

106. Prin urmare, pentru a evalua cadrul juridic aplicabil colectării, accesului și prelucrării ulterioare a datelor în scopuri legate de securitatea națională, este important să se examineze cadrul juridic specific care reglementează colectarea datelor în interiorul și în afara SUA, și anume articolul 702 din FISA și OE nr. 12333, care, ca atare, nu s-au schimbat de la revizuirea anterioară a Scutului de confidențialitate, ținând seama de faptul că noul Ordin executiv nr. 14086 prevede garanții care trebuie puse în aplicare și în contextul colectării de date pe baza unor texte specifice, cum ar fi articolul 702 din FISA și OE nr. 12333.

[109] A se vedea hotărârea CJUE La Quadrature du Net, punctul 124.
[110] A se vedea considerentul 115 din proiectul de decizie.
[111] A se vedea considerentul 117 din proiectul de decizie.
[112] A se vedea considerentul 120 din proiectul de decizie.
[113] Acest ordin executiv revocă PPD-28, cu excepția secțiunilor 3 și 6 din directiva menționată și a anexei clasificate la aceasta, care rămân în vigoare. A se vedea memorandumul prezidențial privind securitatea națională din 7 octombrie 2022.

3.2.1 Garanția A – Prelucrarea ar trebui să fie în conformitate cu dispozițiile legii și să se bazeze pe norme clare, precise și accesibile

107. Pentru evaluarea configurației generale de colectare a datelor în scopuri legate de securitatea națională, CEPD dorește să reamintească prima dintre cele patru așa-numite „garanții esențiale europene", conform căreia „prelucrarea ar trebui să se bazeze pe norme clare, precise și accesibile"[114].

108. În conformitate cu jurisprudența constantă a CJUE, orice restrângere a dreptului la protecția datelor cu caracter personal trebuie să fie prevăzută de lege și temeiul juridic care permite ingerința în acest drept trebuie să definească el însuși întinderea restrângerii exercitării dreptului vizat[115]. Curtea a reamintit, de asemenea, că „reglementarea trebuie să fie obligatorie din punct de vedere juridic în dreptul intern"[116]. În această privință, jurisprudența Curții Europene a Drepturilor Omului clarifică faptul că termenul „lege" ar trebui înțeles în sensul său material și nu în sensul său formal. Aceasta poate include acte normative de rang inferior și măsuri de reglementare luate de organismele profesionale de reglementare în temeiul unor competențe independente de reglementare care le-au fost delegate de Parlament și chiar o lege nescrisă. Pentru a fi „lege", o normă trebuie să fie cel puțin accesibilă în mod adecvat și formulată cu suficientă precizie[117].

109. Gradul de precizie necesar trebuie măsurat în funcție de întinderea restrângerii dreptului[118]. În plus, în ceea ce privește „previzibilitatea" legii, CEDO a reamintit în cauza *Zakharov* că, în contextul măsurilor de supraveghere secretă, cum ar fi interceptarea comunicațiilor, „previzibilitatea nu poate însemna că o persoană trebuie să fie pusă în posibilitatea de a prevedea când autoritățile pot intercepta comunicațiile sale astfel încât să-și poată adapta comportamentul în consecință". Cu toate acestea, existența unor norme clare și detaliate privind măsurile de supraveghere secretă este esențială pentru a preveni riscul arbitrarului în cazul în care o competență a executivului este exercitată în secret. „Legea trebuie să fie elaborată cu suficientă claritate pentru a indica tuturor în mod corespunzător în ce împrejurări și în ce condiții abilitează autoritățile publice să adopte astfel de măsuri secrete."[119]

110. În plus, CJUE a clarificat faptul că evaluarea legislației aplicabile a țării terțe ar trebui să se axeze pe măsura în care aceasta poate fi invocată în fața unei instanțe. Drepturile acordate persoanelor vizate ar trebui să fie în special opozabile, iar persoanelor ar trebui să li se acorde drepturi opozabile autorităților publice[120], ceea ce directiva anterioară, respectiv PPD-28, nu prevedea. OE nr. 14086, care, în opinia CEPD, are același efect juridic în ordinea juridică a SUA precum PPD-28 (și anume obligatoriu pentru executiv), prevede acum drepturi opozabile autorităților publice. O evaluare detaliată a noilor drepturi opozabile ale persoanelor vizate este furnizată în secțiunea privind căile de atac.

---

[114] Recomandările 02/2020 privind garanțiile esențiale europene pentru măsurile de supraveghere (adoptate la 10 noiembrie 2020). A se vedea hotărârea Schrems II, punctele 175 și 180 și Avizul 1/15 (Acordul PNR UE-Canada) din 26 iulie 2017, punctul 139, precum și jurisprudența citată.

[115] A se vedea hotărârea Schrems II a CJUE, punctele 174-175 și jurisprudența citată. A se vedea, de asemenea, în ceea ce privește accesul autorităților publice ale statelor membre, cauza C-623/17, Privacy International, ECLI:EU:C:2020:790 („hotărârea Privacy International a CJUE"), punctul 65 și hotărârea La Quadrature du Net a CJUE, punctul 175.

[116] Hotărârea Privacy International a CJUE, punctul 68.

[117] CEDO, Sunday Times împotriva Regatului Unit (Hotărârea nr. 1), 26 aprilie 1979, CE:ECHR:1979:0426JUD000653874 („Hotărârea CEDO nr. 1 Sunday Times împotriva Regatului Unit"), punctul 49.

[118] CEDO, Hotărârea nr. 1 Sunday Times împotriva Regatului Unit, punctul 49.

[119] CEDO, Zakharov împotriva Rusiei, 4 decembrie 2015 („hotărârea Zakharov a CEDO"), punctul 229.

[120] A se vedea hotărârea Schrems II a CJUE, punctul 181.

111. Considerentele 114-152 din proiectul de decizie și anexa VII oferă un rezumat al anumitor aspecte cu privire la cadrul juridic aplicabil, limitările de colectare, limitările referitoare la păstrare și diseminare, conformitate și supraveghere, transparență și recurs. Sistemul juridic al SUA pentru activitățile de colectare de informații constă într-o serie de documente diferite, inclusiv rapoarte, politici și proceduri individuale ale serviciilor. În această privință, evaluarea CEPD se axează pe un număr limitat de aspecte pe care le consideră esențiale.

112. În conformitate cu considerentele 115-119 din proiectul de decizie, accesul autorităților de securitate națională din SUA la datele cu caracter personal transferate poate avea loc numai în temeiul FISA, în temeiul altor dispoziții legale (titlul 12 articolul 3414 din U.S.C., titlul 15 articolele 1681u-1681v din U.S.C. și titlul 18 articolul 2709 din U.S.C.) sau, în legătură cu datele cu caracter personal aflate în tranzit, în temeiul OE nr. 12333. Din considerentele 116 și 118 din proiectul de decizie reiese că evaluarea Comisiei în legătură cu accesul autorităților de securitate națională din SUA la datele cu caracter personal se concentrează pe articolele 105, 302, 402, 501 și 702 din FISA (activități de colectare de informații externe care vizează persoane care nu sunt cetățeni americani/rezidenți SUA aflate în afara SUA) și pe OE nr. 12333 (activități de colectare de informații externe care vizează datele cu caracter personal aflate în tranzit), acestea fiind considerate cele mai relevante. Prin urmare, avizul CEPD se limitează la evaluarea acestor dispoziții realizată de Comisie, ținând seama de limitările și garanțiile prevăzute în OE nr. 14086[121].

113. În acest sens, trebuie remarcat faptul că toate instrumentele juridice menționate în proiectul de decizie sunt accesibile publicului larg (din interiorul și din afara SUA) și sunt disponibile online. În plus, cerințele prevăzute în OE sunt obligatorii pentru întreaga comunitate a serviciilor de informații[122] și se aplică în mod transversal tuturor activităților care au ca scop colectarea de informații externe.

114. Conceptul de „informații colectate pe baza semnalelor electromagnetice" nu este definit în OE nr. 14086. Ordinul face trimitere la definițiile prevăzute în OE nr. 12333 pentru stabilirea domeniului de aplicare al informațiilor externe și al contrainformațiilor, care sunt definite în sens larg. În această privință, chiar dacă s-a susținut că, de la introducerea FISA, OE nr. 12333 poate fi utilizat numai pentru colectarea de date în afara teritoriului SUA, CEPD reamintește că OE nr. 12333, care rămâne neschimbat, nu conține suficiente detalii cu privire la domeniul său geografic de aplicare, la măsura în care datele pot fi colectate, păstrate sau diseminate ulterior sau la natura infracțiunilor care pot conduce la supraveghere sau cu privire la tipul de informații care pot fi colectate sau utilizate. În principiu, orice colectare de informații externe care intră sub incidența OE nr. 12333 poate avea loc la discreția președintelui SUA[123]. Cu toate acestea, în opinia CEPD, scopul principal al OE nr. 14086 este de a stabili limitele pentru colectarea și prelucrarea datelor cu caracter personal în contextul colectării de informații externe, indiferent de programul de supraveghere utilizat și de unde se obțin date. Prin urmare, CEPD înțelege că garanțiile suplimentare prevăzute în OE nr. 14086 se aplică, de asemenea, în contextul programelor de supraveghere aplicabile datelor cu caracter personal aflate în tranzit care au loc în temeiul OE nr. 12333[124].

---

121 Acest ordin executiv revocă PPD-28, cu excepția secțiunilor 3 și 6 din directiva menționată și a anexei clasificate la aceasta, care rămân în vigoare. A se vedea memorandumul prezidențial privind securitatea națională din 7 octombrie 2022.

122 A se vedea considerentul 120 din proiectul de decizie.

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

[124] A se vedea considerentul 134 din proiectul de decizie.

115. În acest sens, OE nr. 14086 enumeră 12 obiective legitime care ar trebui urmărite atunci când se efectuează colectarea de informații pe baza semnalelor electromagnetice și cinci obiective pentru care colectarea de informații pe baza semnalelor electromagnetice nu trebuie efectuată[125], precum și șase obiective legitime pentru utilizarea datelor colectate în masă[126]. În timp ce unele dintre acestea sunt destul de detaliate (de exemplu, „salvarea ostaticilor"), altele sunt mai generale (de exemplu, „securitatea globală"). OE nr. 14086 stabilește, de asemenea, o listă de obiective interzise, care include, în special, eliminarea sau restricționarea „intereselor legitime în materie de confidențialitate"[127]. OE nr. 14086 prevede, de asemenea, posibilitatea adăugării pe listă de către președintele Statelor Unite ale Americii a altor obiective pentru care este permisă colectarea, care, în baza deciziei președintelui, ar putea să nu fie făcute publice în cazul în care președintele consideră că acest lucru ar reprezenta un risc pentru securitatea națională a Statelor Unite ale Americii[128]. Astfel de actualizări pot fi autorizate numai „în lumina noilor imperative de securitate națională".

116. Doar obiectivele în sine nu pot fi invocate de serviciile de informații pentru a justifica o colectare de informații pe baza semnalelor electromagnetice; acestea trebuie să fie justificate în continuare, în scopuri operaționale, în priorități mai concrete pentru care pot fi colectate informații pe baza semnalelor electromagnetice. OE nr. 14086 detaliază procedura de validare a priorităților pentru care pot fi colectate informații pe baza semnalelor electromagnetice[129]. CEPD înțelege că procesul de definire a priorităților validate în materie de informații este gestionat, în principiu, de directorul Comunității Serviciilor de Informații și recunoaște că acesta ar trebui, în general, să implice evaluarea Responsabilului pentru protecția libertăților civile din cadrul Biroului Directorului Serviciului Național de Informații (*Office of the Director of National Intelligence*), cu care directorul poate să nu fie de acord, caz în care acesta „include evaluarea responsabilului pentru protecția libertăților civile și opiniile directorului atunci când prezintă președintelui Cadrul național de priorități ale serviciilor de informații (*National Intelligence Priorities Framework*) (NIPF)"[130].

117. Cu toate acestea, CEPD constată, de asemenea, că, în conformitate cu definiția „priorității validate în materie de informații", astfel de priorități înseamnă, pentru „majoritatea activităților de colectare de informații pe baza semnalelor electromagnetice din Statele Unite ale Americii"[131], o prioritate validată în temeiul secțiunii 2 litera (b) punctul (iii) din ordinul executiv (descrisă la punctul anterior). Procesul de validare poate, în unele cazuri, să difere de acest proces în „circumstanțe restrânse", caz în care președintele sau șeful unui element al Comunității Serviciilor de Informații poate stabili o prioritate, „în măsura posibilului", în conformitate cu criteriile stabilite în aceeași secțiune 2 litera (b) punctul (iii) partea A subpunctele 1-3, care include cerința de a lua în considerare în mod corespunzător viața privată și libertățile civile ale tuturor persoanelor, însă fără implicarea responsabilului pentru protecția libertăților civile.

118. În plus, OE nr. 14086 subliniază că „activitățile de colectare de informații pe baza semnalelor electromagnetice trebuie să fie cât mai adaptate posibil" pentru a promova o prioritate validată în materie de informații și că elementele „Comunității Serviciilor de Informații trebuie să ia în considerare

[125] A se vedea secțiunea 2 litera (b) punctul (ii) partea A subpunctele 1-5 din Ordinul executiv nr. 14086 („OE nr. 14086").
[126] A se vedea considerentul 134 din proiectul de decizie și secțiunea 2 litera (c) punctul (ii) din OE nr. 14086.
[127] A se vedea secțiunea 2 litera (b) punctul (ii) partea A subpunctul 2 din OE nr. 14086.
[128] A se vedea secțiunea 2 litera (b) punctul (i) partea B din OE nr. 14086.
[129] A se vedea considerentul 129 din proiectul de decizie.
[130] A se vedea secțiunea 2 litera (b) punctul (iii) partea B din OE nr. 14086.
[131] A se vedea secțiunea 4 litera (n) din OE nr. 14086.

disponibilitatea, fezabilitatea și caracterul adecvat al altor surse mai puțin intruzive", prevăzând totodată cerințe generale privind necesitatea și proporționalitatea[132].

119. În plus, în conformitate cu secțiunea 5 litera (h), OE nr. 14086 creează dreptul de a depune plângeri eligibile la Responsabilul pentru protecția libertăților civile și de a obține reexaminarea deciziilor adoptate de acesta de către Curtea de Reexaminare a Protecției Datelor, în conformitate cu mecanismul de recurs instituit în secțiunea 3 din ordinul respectiv.

120. Textul FISA pare să fie mai clar și mai precis decât OE nr. 12333 cu privire la tipul de operațiuni de colectare de informații care pot fi autorizate. În prezent, FISA și OE nr. 12333 trebuie aplicate în lumina OE nr. 14086 și, în special, ținând seama, printre altele, de principiile necesității și proporționalității.

121. Cerințele prevăzute în OE nr. 14086 trebuie puse în aplicare în continuare prin politici și proceduri ale serviciilor, care le transpun în direcții concrete pentru operațiunile de zi cu zi. În acest sens, OE nr. 14086 oferă serviciilor de informații din SUA un termen maxim de un an pentru a-și actualiza politicile și procedurile existente (și anume până la 7 octombrie 2023) în vederea alinierii acestora la cerințele ordinului executiv. Aceste politici și proceduri actualizate trebuie să fie elaborate în consultare cu Procurorul General, cu Responsabilul pentru protecția libertăților civile și cu Comitetul de supraveghere în materie de protecție a vieții private și a libertăților civile (PCLOB) și trebuie să fie puse la dispoziția publicului în cea mai mare măsură posibilă[133].

122. CEPD ar saluta condiționarea nu numai a intrării în vigoare, ci și a adoptării deciziei, printre altele, de adoptarea unor politici și proceduri actualizate pentru punerea în aplicare a OE nr. 14086 de către toate serviciile de informații ale SUA. CEPD recomandă Comisiei să evalueze aceste politici și proceduri actualizate și să comunice această evaluare CEPD.

123. În cele din urmă, în ceea ce privește păstrarea datelor transferate odată ce au fost colectate în scopuri legate de securitatea națională, CEPD constată că OE nr. 14086 prevede că normele aplicabile datelor cu caracter personal ale persoanelor care sunt cetățeni americani/rezidenți SUA se aplică și datelor cu caracter personal ale persoanelor care nu sunt cetățeni americani/rezidenți SUA[134]. Din proiectul de decizie reiese că aceste norme sunt prevăzute la articolul 309 din Legea privind autorizarea serviciilor de informații pentru anul fiscal 2015 (*Intelligence Authorization Act for Fiscal Year 2015*)[135], care stabilește, în principiu, o perioadă maximă de păstrare de cinci ani pentru orice comunicație telefonică sau electronică care nu are caracter public dobândită fără consimțământul persoanei vizate. În această privință, CEPD recomandă Comisiei să ofere mai multă claritate în cadrul deciziei în ceea ce privește evaluarea normelor de păstrare aplicabile datelor cu caracter personal ale persoanelor care sunt cetățeni americani/rezidenți SUA.

3.2.2 Garanția B – Trebuie să se demonstreze necesitatea și proporționalitatea în raport cu obiectivele legitime urmărite

3.2.2.1 Garanții orizontale prevăzute de noul Ordin executiv nr. 14086 – necesitate și proporționalitate

124. Noul OE nr. 14086, care înlocuiește, în mare măsură, PPD-28, își propune să prevadă norme de consolidare a garanțiilor pentru activitățile de colectare de informații pe baza semnalelor

[132] A se vedea secțiunea 2 litera (c) punctul (i) părțile A și B din OE nr. 14086.
[133] A se vedea secțiunea 2 litera (c) punctul (iv) părțile B și C din OE nr. 14086.
[134] Considerentul 150 din proiectul de decizie.
[135] Nota de subsol 272 din proiectul de decizie.

electromagnetice desfășurate de Statele Unite ale Americii, care să fie puse în aplicare în continuare de către elementele comunității serviciilor de informații în politicile și procedurile lor interne.

125. OE nr. 14086 introduce două noi cerințe în temeiul legislației SUA, care reflectă cerințele reamintite de CJUE în hotărârea sa în cauza Schrems II, și anume ca activitățile de colectare de informații pe baza semnalelor electromagnetice să se desfășoare numai în măsura în care acest lucru este necesar pentru a promova colectarea de informații în baza unei priorități validate și numai în măsura și într-un mod proporționale cu respectiva prioritate validată în materie de informații[136].

126. CEPD înțelege că aceste elemente au fost incluse pentru a reflecta principiile necesității și proporționalității prevăzute în dreptul UE și în jurisprudența CJUE și a CEDO, care urmăresc să se asigure că prelucrarea și colectarea datelor se limitează la ceea ce este necesar și proporțional.

127. În acest sens, CEPD reamintește procesul prevăzut pentru validarea priorităților în materie de informații, precum și posibila derogare (a se vedea punctele 116 și 117).

128. În plus, CEPD observă că aceste principii ale necesității și proporționalității prevăzute în OE vor trebui să fie operaționalizate și puse în aplicare, în termen de un an, în politicile și procedurile fiecărui element al Comunității Serviciilor de Informații[137].

3.2.2.2 Garanții specifice pentru colectarea de informații pe baza semnalelor electromagnetice

129. CEPD observă, de asemenea, că OE nr. 14086 prevede limitări în ceea ce privește obiectivele pentru care pot și nu pot fi colectate date cu caracter personal, în contextul colectării de informații pe baza semnalelor electromagnetice[138].

130. CEPD salută dispozițiile incluse în ordinul executiv potrivit cărora se va acorda prioritate colectării direcționate față de colectarea în masă[139]. În contextul colectării de informații pe baza semnalelor electromagnetice, ordinul executiv prevede o listă de 12 obiective pentru care pot fi colectate date, care trebuie să fie justificate suplimentar în funcție de prioritățile în materie de informații (a se vedea punctul 117), precum și o listă de cinci obiective pentru care nu se vor desfășura activități de colectare de informații pe baza semnalelor electromagnetice[140]. În principiu, aceste dispoziții constituie o garanție pentru asigurarea necesității colectării de date.

131. Cu toate acestea, CEPD reamintește că OE nr. 14086 prevede, de asemenea, posibilitatea adăugării pe listă de către președintele Statelor Unite ale Americii a altor obiective (a se vedea punctele 114 și 115)[141].

3.2.2.3 Garanții specifice pentru colectarea în masă

132. În hotărârea Schrems I CJUE a subliniat că *„protecția dreptului fundamental la respectarea vieții private la nivelul Uniunii impune ca derogările de la protecția datelor cu caracter personal și limitările acesteia să fie efectuate în limitele strictului necesar”*[142] și a stabilit că *„trebuie să se considere că o reglementare care permite autorităților publice să aibă acces în mod generalizat la conținutul comunicărilor*

[136] A se vedea secțiunea 2 litera (a) punctul (ii) părțile A și B din OE nr. 14086.
[137] A se vedea secțiunea 2 litera (c) punctul (iv) partea B din OE nr. 14086.
[138] A se vedea secțiunea 2 litera (b) punctul (i) partea A subpunctele 1-12 din OE nr. 14086.
[139] A se vedea secțiunea 2 litera (c) punctul (ii) partea A din OE nr. 14086.
[140] A se vedea secțiunea 2 litera (b) punctul (ii) partea A subpunctele 1-5 din OE nr. 14086.
[141] A se vedea secțiunea 2 litera (b) punctul (i) partea B din OE nr. 14086.
[142] Hotărârea Schrems I a CJUE, punctul 92.

electronice aduce atingere substanței dreptului fundamental la respectarea vieții private, astfel cum este garantat la articolul 7 din Cartă".

133. În cauza Schrems II[143], în ceea ce privește analiza colectării în masă în raport cu interpretarea corelată a OE nr. 12333 și a PPD-28, în special a punctelor 183-185, Curtea a subliniat, astfel cum s-a amintit mai sus, că posibilitatea colectării în masă, „care permite, în cadrul programelor de supraveghere întemeiate pe O.E. 12333, accesul la date aflate în tranzit către Statele Unite fără ca accesul menționat să facă obiectul vreunui control jurisdicțional, nu delimitează, indiferent de situație, în mod suficient de clar și de precis conținutul unei astfel de colectări în masă a datelor cu caracter personal ".

134. Prin urmare, CEPD constată că, în hotărârea Schrems II, CJUE nu a exclus, în principiu, colectarea în masă, ci a considerat că, pentru ca o astfel de colectare în masă să aibă loc în mod legal, trebuie să existe limite suficient de clare și de precise pentru a delimita domeniul de aplicare al unei astfel de colectări în masă.

135. CEPD recunoaște, de asemenea, că, deși înlocuiește PPD-28, OE nr. 14086 prevede noi garanții și limite pentru colectarea și utilizarea datelor colectate în afara SUA, deoarece limitările FISA sau ale altor legi mai specifice ale SUA nu se aplică.

136. În ceea ce privește colectarea în masă a datelor, CEPD ia act de faptul că OE nr. 14086 prevede că se permite în continuare colectarea în masă. CEPD subliniază că definiția colectării în masă rămâne aceeași precum în directiva anterioară, respectiv în PPD-28, și anume: „*Informațiile pe baza semnalelor electromagnetice colectate în «masă» înseamnă colectarea autorizată a unor cantități mari de date operative pe baza semnalelor electromagnetice care, din motive tehnice sau operaționale, sunt obținute fără a se recurge la factori de diferențiere (de exemplu, fără utilizarea unor identificatori specifici sau a unor termeni de selecție)*"[144].

137. De la pronunțarea hotărârii Schrems II, Curtea nu a mai precizat garanțiile necesare pentru realizarea unei colectări în masă. Cu toate acestea, CEPD reamintește că CEDO a emis hotărâri importante privind colectarea în masă și garanțiile relevante în acest context.

138. CEPD reamintește că, deoarece permite colectarea unor cantități mari de date fără a face distincție între acestea, colectarea în masă prezintă riscuri mai mari pentru persoane[145] decât colectarea direcționată și, prin urmare, impune necesitatea furnizării unor garanții suplimentare.

139. CEPD constată, de asemenea, că CJUE și-a extins jurisprudența referitoare la păstrarea datelor privind traficul și a datelor de localizare, precum și la accesul ulterior la aceste date păstrate de operatorii de telecomunicații, inclusiv în scopuri legate de securitatea națională, care, deși nu pot fi considerate direct aplicabile în acest context, ar putea fi relevante într-o anumită măsură în cadrul prezentei evaluări a colectării în masă în contextul OE nr. 12333.

1) <u>Limitarea scopului</u>

[143] A se vedea hotărârea Schrems II a CJUE.

[144] A se vedea secțiunea 4 litera (b) din OE nr. 14086.

[145] A se vedea, de exemplu, CEDO (Marea Cameră), Big Brother Watch și alții împotriva Regatului Unit, 25 mai 2021 („hotărârea Big Brother Watch a CEDO"'), considerentul 363, în care Curtea menționează că „nu este convinsă că obținerea datelor de comunicații aferente prin interceptarea în masă este în mod necesar mai puțin intruzivă decât achiziția de conținut."

140. Ordinul executiv prevede că o colectare în masă ar trebui să aibă loc numai după ce s-a stabilit că *„informațiile necesare pentru promovarea unei priorități validate în materie de informații nu pot fi obținute în mod rezonabil printr-o colectare direcționată”*[146] *și că „elementul Comunității Serviciilor de Informații în cauză trebuie să aplice metode și măsuri tehnice rezonabile pentru a limita datele colectate numai la ceea ce este necesar pentru promovarea unei priorități validate în materie de informații, reducând în același timp la minimum colectarea de informații nepertinente”*[147]. Pe lângă aceste garanții, CEPD recunoaște, de asemenea, că datele colectate în masă trebuie utilizate în vederea îndeplinirii unuia sau mai multora dintre cele șase obiective enumerate[148]. CEPD subliniază, de asemenea, că, deși aceste obiective sunt mai detaliate decât cele prevăzute în directiva anterioară PPD-28, înlocuită în mare măsură de OE nr. 14086, amploarea unor astfel de posibilități de colectare rămâne potențial amplă, și anume vizează volume mari de date.

141. CEPD reamintește încă o dată că OE nr. 14086 prevede, de asemenea, posibilitatea adăugării pe listă de către președintele Statelor Unite ale Americii a altor obiective (a se vedea punctul 115)[149].

2) <u>Autorizarea independentă prealabilă</u>

142. CEPD subliniază importanța semnificativă acordată de CEDO autorizării independente prealabile în contextul colectării în masă a datelor în scopuri legate de securitatea națională. Curtea a stabilit în special că *„pentru a reduce la minimum riscul abuzului de putere de interceptare în masă, Curtea consideră că procesul trebuie să facă obiectul unor «garanții de la un capăt la altul», ceea ce înseamnă că, la nivel intern, trebuie efectuată o evaluare în fiecare etapă a procesului a necesității și proporționalității măsurilor luate, iar interceptarea în masă ar trebui să facă obiectul unei autorizări independente la început, atunci când sunt definite obiectul și amploarea operațiunii, și că operațiunea trebuie să facă obiectul supravegherii și al unui control a posteriori. În opinia Curții, acestea sunt garanții fundamentale care vor constitui piatra de temelie a oricărui regim de interceptare în masă conform cu articolul 8”*[150].

143. CEPD remarcă, de asemenea, următorul punct din această hotărâre pronunțată în Marea Cameră, în care Curtea de la Strasbourg subliniază, de asemenea, că „este de acord cu opinia Camerei potrivit căreia, deși autorizația judiciară reprezintă o «garanție importantă împotriva arbitrariului», nu constituie o «cerință necesară» (punctele 318-320 din hotărârea Camerei). *Cu toate acestea, interceptarea în masă trebuie autorizată de un organ independent,* adică de un organ independent de executiv”[151].

144. În acest context, CEPD constată că ordinul executiv nu prevede o astfel de autorizare prealabilă independentă pentru colectarea în masă și că acest lucru nu este prevăzut nici în OE nr. 12333 (a se vedea secțiunea de mai jos privind OE nr. 12333).

3) <u>Norme privind păstrarea</u>

145. CEPD reamintește că un alt set important de garanții îl reprezintă normele privind durata colectării și păstrării datelor. În acest sens, CEDO a subliniat că *„dreptul intern trebuie să stabilească o limită privind*

[146] A se vedea secțiunea 2 litera (c) punctul (ii) partea A din OE nr. 14086.
[147] A se vedea secțiunea 2 litera (c) punctul (ii) partea A din OE nr. 14086.
[148] A se vedea secțiunea 2 litera (c) punctul (ii) partea B din OE nr. 14086.
[149] A se vedea secțiunea 2 litera (c) punctul (ii) partea C din OE nr. 14086.
[150] A se vedea hotărârea Big Brother Watch a CEDO, punctul 350.
[151] A se vedea hotărârea Big Brother Watch a CEDO, punctul 351.

durata interceptării, procedura care trebuie urmată pentru examinarea, utilizarea și stocarea datelor obținute, precauțiile care trebuie luate la comunicarea datelor către alte părți și circumstanțele în care datele interceptate pot sau trebuie să fie șterse sau distruse"[152], întrucât aceste garanții „*sunt la fel de relevante pentru interceptarea în masă*"[153].

146. În acest sens, CEPD înțelege că ordinul executiv prevede norme privind păstrarea datelor cu caracter personal colectate pe baza semnalelor electromagnetice, inclusiv în masă[154]. CEPD constată că, în conformitate cu secțiunea 2 litera (c) punctul (iii) partea A din OE nr. 14086, fiecare element al Comunității Serviciilor de Informații care gestionează informații cu caracter personal colectate pe baza semnalelor electromagnetice stabilește și aplică politici și proceduri menite să reducă la minimum diseminarea și păstrarea informațiilor cu caracter personal colectate pe baza semnalelor electromagnetice. Totuși, aceste norme nu prevăd o perioadă de păstrare specifică, ci se referă, mai degrabă, în general, la aceleași norme aplicabile pentru păstrarea datelor privind persoanele care sunt cetățeni americani/rezidenți SUA și la situațiile în care nu există nicio decizie finală privind păstrarea datelor. Prin urmare, CEPD este preocupat de faptul că aceste perioade de păstrare, în ceea ce privește colectarea direcționată (a se vedea punctul 122), nu sunt clar definite în acest ordin executiv în privința datelor colectate în masă. CEPD invită Comisia să își împărtășească evaluarea cu privire la necesitatea și proporționalitatea perioadelor de păstrare aplicabile persoanelor care sunt cetățeni americani/rezidenți SUA și informațiile disponibile privind perioadele de păstrare aplicate în practică în cazul în care nu s-a emis nicio decizie finală privind stocarea datelor în temeiul legislației SUA, având în vedere că, în stadiul său actual, proiectul de decizie doar reamintește această regulă generală într-un singur paragraf scurt[155] și într-o notă de subsol[156] care nu permite să se stabilească dacă aceste perioade de stocare sunt necesare și proporționale. Întrucât, astfel cum a subliniat CEDO, aceasta este o garanție esențială pentru exercitarea de către persoanele vizate a drepturilor de care dispun într-un context în care se ia, în primul rând, o măsură deosebit de intruzivă de colectare a datelor lor, CEPD invită Comisia Europeană să ofere clarificări suplimentare cu privire la perioadele de păstrare diferite aplicate în practică.

4) <u>Garanții privind „diseminarea"</u>

147. CEPD reamintește, de asemenea, că, pentru a asigura eficacitatea principiului necesității și proporționalității, precum și a principiului limitării scopului, CEDO a recunoscut, de asemenea, importanța normelor prevăzute de lege privind diseminarea ulterioară a datelor colectate, inclusiv în contextul colectării în masă[157].

148. Secțiunea 2 litera (c) punctul (iii) partea A subpunctul 1 litera (c) din OE nr. 14086 prevede că informațiile care se referă la persoane care nu sunt cetățeni americani/rezidenți SUA și care sunt colectate prin activități de colectare de informații pe baza semnalelor electromagnetice pot fi diseminate numai dacă o persoană autorizată și instruită în mod corespunzător are convingerea rezonabilă că informațiile cu caracter personal vor fi protejate în mod corespunzător și că este necesar ca destinatarul să cunoască aceste informații.

---

[152] A se vedea hotărârea Big Brother Watch a CEDO, punctul 348.
[153] A se vedea hotărârea Big Brother Watch a CEDO, punctul 348.
[154] A se vedea secțiunea 2 litera (c) punctul (iii) partea A subpunctul 2 literele (a)-(c) din OE nr. 14086.
[155] A se vedea proiectul de decizie, punctul 150.
[156] A se vedea nota de subsol 271 din proiectul de decizie.
[157] A se vedea hotărârea Big Brother Watch a CEDO, punctul 348.

149. Ținând seama de acest lucru, CEPD înțelege că dispozițiile privind diseminarea în temeiul OE nr. 14086 nu prevăd nicio interdicție expresă a diseminării în alte scopuri decât cele legate de securitatea națională atunci când este vorba de diseminarea informațiilor către autoritățile competente din SUA[158]. CEPD invită Comisia să ofere clarificări suplimentare privind normele și garanțiile aplicabile în acest caz.

150. Prin urmare, CEPD este preocupat de faptul că datele obținute de autoritățile competente din cadrul Comunității Serviciilor de Informații ar putea fi ulterior transmise autorităților competente din SUA în scopul combaterii criminalității, inclusiv a infracțiunilor grave, în contextul anchetelor penale, oferind astfel autorităților de aplicare a legii, fără alte restricții specifice, posibilitatea de a obține date pe care le-ar fi fost interzis să le colecteze direct și invită Comisia să evalueze suplimentar acest aspect.

151. În contextul specific al transferurilor ulterioare (diseminarea către destinatari din afara guvernului Statelor Unite ale Americii, inclusiv către un guvern străin sau o organizație internațională[159]), CEPD reamintește punctul său de vedere, potrivit căruia protecția acordată datelor ar trebui să fie menținută și în contextul transferurilor ulterioare, inclusiv în domeniul securității naționale[160].

152. În această privință, ordinul executiv prevede anumite garanții, și anume obligația de a ține seama în mod corespunzător de scopul diseminării – deși nu impune în mod expres ca scopul diseminării să fie, de asemenea, acela de a proteja securitatea națională – natura și amploarea informațiilor cu caracter personal care sunt diseminate și potențialul impact negativ asupra persoanei sau a persoanelor în cauză înainte de diseminarea datelor.

153. Deși recunoaște că unele dintre aceste garanții, în special *„potențialul impact negativ"*[161] asupra persoanei (persoanelor) vizată (vizate), reflectă unele cerințe ale CEDO, CEPD subliniază, de asemenea, că aceasta solicită în plus impunerea obligației juridice *„de a analiza și de a stabili dacă destinatarul străin al informațiilor oferă un nivel minim acceptabil de garanții"*[162], obligație pe care CEPD nu o identifică în mod expres în dispozițiile ordinului executiv referitoare la diseminarea către destinatari străini. Prin urmare, CEPD invită Comisia să evalueze în continuare acest element.

154. CEPD constată, de asemenea, că, în cadrul evaluării caracterului adecvat al nivelului de protecție, Comisia Europeană nu a luat în considerare existența acordurilor internaționale încheiate cu țări terțe sau organizații internaționale, care pot prevedea dispoziții specifice pentru transferul internațional de date cu caracter personal de către serviciile de informații către țări terțe. CEPD consideră că încheierea de acorduri bilaterale sau multilaterale cu țări terțe în scopul cooperării în materie de informații este susceptibilă să afecteze cadrul juridic privind protecția datelor, astfel cum a fost evaluat.

155. Prin urmare, CEPD invită Comisia Europeană să clarifice dacă există astfel de acorduri, precum și în ce condiții pot fi încheiate acestea și să evalueze dacă dispozițiile acordurilor internaționale pot afecta nivelul de protecție acordat datelor cu caracter personal transferate din SEE de cadrul legislativ și practicile utilizate cu privire la transferurile ulterioare în scopuri legate de securitatea națională.

---

[158] A se vedea secțiunea 2 litera (c) punctul (iii) partea A subpunctul 1 din OE nr. 14086.
[159] A se vedea în special secțiunea 2 litera (c) punctul (iii) partea A subpunctul 1 litera (d) din OE nr. 14086.
[160] A se vedea, de pildă, Avizul 14/2021 al CEPD referitor la proiectul de decizie de punere în aplicare a Comisiei Europene în temeiul Regulamentului (UE) 2016/679 privind protecția adecvată a datelor cu caracter personal în Regatul Unit al Marii Britanii și Irlandei de Nord, adoptat la 13 aprilie 2021 (secțiunile 4.3.2.1 și 4.3.2.2).
[161] A se vedea secțiunea 2 litera (c) punctul (iii) partea A subpunctul 1 litera (d) din OE nr. 14086.
[162] A se vedea CEDO (Marea Cameră), Centrum För Rättvisa împotriva Suediei, 25 mai 2021, punctul 326.

5) Colectarea temporară în masă pentru a sprijini faza tehnică inițială a colectării direcționate

156. CEPD reamintește că, în contextul ultimei revizuiri comune a Scutului de confidențialitate, discuțiile s-au axat în principal pe interpretarea și aplicarea motivului (a situației/a scenariului) suplimentar pentru colectarea în masă prevăzut în prima teză a notei de subsol 5 de la articolul 2 din PPD-28, care prevedea că *„limitările cuprinse în această secțiune nu se aplică datelor operative pe baza semnalelor electromagnetice obținute temporar pentru a facilita colectarea direcționată*." Autoritățile SUA au explicat la momentul respectiv sensul expresiei *„date operative pe baza semnalelor electromagnetice obținute temporar pentru a facilita colectarea direcționată*". CEPD a înțeles din aceste discuții că, având în vedere respectiva notă de subsol, datele pot fi colectate în masă – și indiferent de cele șase scopuri prevăzute – dacă sunt colectate temporar în vederea stabilirii unui identificator pentru un obiectiv definit. Prin urmare, situația respectivă ar reprezenta un motiv suplimentar de colectare a datelor în masă și, în acest caz, numai principiile generale din articolului 1 din PPD-28 s-ar fi aplicat în continuare. Astfel cum s-a reamintit mai sus, în hotărârea Schrems II, CJUE a considerat că, în ceea ce privește colectarea în masă, OE nr. 12333 coroborat cu PPD-28 nu *„delimitează [...] în mod suficient de clar și de precis conținutul unei astfel de colectări în masă a datelor cu caracter personal*"[163].

157. CEPD constată că o derogare care permite un astfel de tip de colectare în masă este încă prevăzută în OE nr. 14086[164]; cu toate acestea, CEPD salută faptul că această derogare a fost restrânsă în comparație cu PPD-28 și că OE nr. 14086 prevede garanții suplimentare.

158. CEPD înțelege că noul OE nr. 14086 prevede garanții care rămân aplicabile în contextul acestui tip de colectare tehnică în masă cu caracter temporar, în special principiile generale ale necesității și proporționalității în ceea ce privește prioritatea validată în materie de informații atunci când datele sunt obținute fără a se recurge la factori de diferențiere înainte de colectarea direcționată [secțiunea 2 literele (a)-(b) și secțiunea 2 litera (c) punctul (i) din OE nr. 14086]. De asemenea, CEPD înțelege că o astfel de colectare în masă care sprijină o colectare direcționată ulterioară de informații pe baza semnalelor electromagnetice face, de asemenea, obiectul garanțiilor suplimentare prevăzute începând cu subsecțiunea 2 litera (c) punctul (iii)[165].

159. Cu toate acestea, CEPD reamintește, de asemenea, – a se vedea punctul 117 de mai sus – că definiția *„priorității validate în materie de informații*" prevede o procedură derogatorie care nu ar implica Responsabilul pentru protecția libertăților civile din cadrul Biroului Directorului Serviciului Național de Informații.

160. Cu toate acestea, CEPD constată în continuare că garanțiile prevăzute în subsecțiunea privind colectarea în masă nu se aplică colectării temporare în masă utilizate pentru a sprijini faza tehnică inițială a activității de colectare direcționată de informații pe baza semnalelor electromagnetice, astfel cum se subliniază în secțiunea 2 litera (c) punctul (ii) partea D din OE nr. 14086, ceea ce înseamnă în special că, în acest context, datele colectate în masă pot fi utilizate în alte scopuri decât cele enumerate la subsecțiunea 2 litera (c) punctul (ii). CEPD ar aprecia includerea unor clarificări în proiectul de decizie cu privire la scopurile în care pot fi utilizate datele colectate în masă în acest context, precum și cu privire la aplicarea limitărilor prevăzute în subsecțiunea 2 litera (c) punctul (i) pentru colectarea de informații pe baza semnalelor electromagnetice în general (și anume numai pentru obiectivele legitime

[163] Hotărârea Schrems II a CJUE, punctul 183.

[164] A se vedea secțiunea 2 litera (c) punctul (ii) partea D din OE nr. 14086 și nota de subsol 226 din proiectul de decizie.

[165] A se vedea secțiunile anterioare pentru aspecte suplimentare cu privire la aceste dispoziții.

enumerate în subsecțiunea respectivă) în contextul colectării temporare în masă în cadrul proiectului de decizie.

161. În concluzie, CEPD subliniază, de asemenea, că derogarea care urmează să se aplice pentru colectarea temporară în masă în vederea colectării direcționate și pentru celelalte garanții rămâne neclară, în special în ceea ce privește care dintre garanțiile prevăzute în OE nr. 14086 s-ar aplica și în ce etapă (colectare în masă, colectare direcționată ulterioară) și invită Comisia să evalueze în continuare aceste elemente, precum și să analizeze aceste aspecte în practică în viitoarele revizuiri comune.

162. În plus, un alt aspect pe care CEPD îl regretă este că, în ciuda faptului că noțiunea de „temporar" a fost ușor mai detaliată în ordinul executiv decât în PPD-28, în opinia CEPD, aceasta pare totuși să însemne că, atât timp cât obiectivul nu a fost identificat, colectarea în masă ar putea continua. În acest sens, CEPD reamintește necesitatea de a avea norme clare și precise și subliniază încă o dată caracterul esențial al garanției pe care o reprezintă aceste norme pentru persoanele vizate.

163. În concluzie, în ceea ce privește garanțiile aplicabile colectării în masă, CEPD își exprimă în continuare preocuparea că, în pofida garanțiilor suplimentare prevăzute în OE nr. 14086, posibilitatea de a colecta date în masă, și anume fără a se recurge la factori de diferențiere, este încă oferită, în absența unor garanții esențiale, cum ar fi autorizarea prealabilă a colectării acestor date – inclusiv în situația derogatorie a colectării tehnice în masă cu caracter temporar –, ținând seama, de asemenea, de necesitatea unor clarificări suplimentare și de preocupările exprimate cu privire la limitarea strictă a scopului privind accesul ulterior la datele respective, normele clare și stricte de păstrare a datelor și garanțiile mai stricte privind diseminarea datelor colectate în masă, inclusiv în contextul transferurilor ulterioare.

164. În general, CEPD subliniază că hotărârea CEDO menționată mai sus demonstrează încă o dată importanța unei supravegheri cuprinzătoare de către autoritățile de supraveghere independente. CEPD subliniază că supravegherea independentă în toate etapele procesului de acces al autorităților în scopuri legate de securitatea națională este o garanție importantă împotriva măsurilor de supraveghere arbitrare și, prin urmare, pentru evaluarea unui nivel adecvat de protecție a datelor. Garanția de independență a autorităților de supraveghere în înțelesul articolului 8 alineatul (3) din Carta drepturilor fundamentale a Uniunii Europene urmărește să asigure monitorizarea eficace și fiabilă a respectării dispozițiilor în domeniul protecției persoanelor în ceea ce privește prelucrarea datelor cu caracter personal. Acest lucru este valabil mai ales în circumstanțele în care, având în vedere natura supravegherii secrete, persoana nu poate să formuleze o cale de atac sau să participe în mod direct la nicio procedură de recurs anterioară sau concomitentă cu executarea măsurii de supraveghere.

165. CEPD reamintește că, în opinia sa, evaluarea caracterului adecvat depinde de toate circumstanțele, în special de eficacitatea supravegherii *ex post* și a căilor de atac judiciare, astfel cum se prevede în cadrul juridic.

3.2.2.4 Cadrul juridic care organizează colectarea specifică de informații în scopuri legate de securitatea națională de către elementele Comunității Serviciilor de Informații pe teritoriul SUA și în afara acestuia

166. În hotărârea Schrems II, CJUE a subliniat că articolul 702 din FISA *„nu evidențiază în niciun mod existența unor limitări ale abilității pe care o conferă pentru punerea în aplicare a programelor de supraveghere în scopul informării externe și nici existența unor garanții pentru persoane care nu sunt*

cetățeni americani potențial vizate de programele menționate"[166]. Acest lucru a determinat Curtea să considere că *„în aceste condiții [...], articolul respectiv nu este susceptibil de a asigura un nivel de protecție în esență echivalent cu cel garantat de Cartă [...], potrivit căreia un temei juridic care permite ingerințe în drepturile fundamentale trebuie, pentru a respecta principiul proporționalității, să definească el însuși întinderea restrângerii exercitării dreptului vizat și să prevadă norme clare și precise care să reglementeze conținutul și aplicarea măsurii respective și să impună cerințe minime*"[167].

167. În legătură cu OE nr. 12333, Curtea observă că *„nici acest decret nu conferă drepturi opozabile autorităților americane în fața instanțelor judecătorești*"[168] și concluzionează, de asemenea că *„în cadrul programelor de supraveghere întemeiate pe O. E. 12333, accesul la date aflate în tranzit către Statele Unite fără ca accesul menționat să facă obiectul vreunui control jurisdicțional, nu delimitează, indiferent de situație, în mod suficient de clar și de precis conținutul unei astfel de colectări în masă a datelor cu caracter personal*"[169], în urma analizei condițiilor în care ar putea avea loc colectarea în masă în temeiul acestui ordin, coroborat cu PPD-28.

168. În ceea ce privește aceste regimuri specifice de colectare a datelor, OE nr. 14086 prevede în prezent noi norme.

3.2.2.4.1 Colectarea de date în scopuri legate de securitatea națională în temeiul Secțiunii 702

169. CEPD reamintește că acele constatări privind articolul 702 din FISA[170], potrivit cărora, *„în practică, «persoanele care nu sunt cetățeni americani/rezidenți SUA» beneficiază, de asemenea, de restricțiile de acces și de păstrare impuse de procedurile de reducere la minimum și/sau de direcționare a intervențiilor ale diferitelor agenții ca urmare a costurilor și a dificultății de a identifica și de a elimina informațiile referitoare la persoanele care sunt cetățeni americani/rezidenți SUA pentru un volum mare de date, ceea ce înseamnă că, de regulă, întregul set de date este gestionat în conformitate cu standardele mai ridicate în materie de date ale SUA*", au fost apreciate în ultimul raport PCLOB.

170. Potrivit acelor constatări, „programul nu funcționează prin colectarea în masă a comunicațiilor". Rapoartele statistice privind transparența din 2014 și 2021 emise de Biroul Directorului Serviciului Național de Informații au confirmat această constatare. În plus, potrivit raportului PCLOB, pentru a direcționa supravegherea, sunt utilizați „termeni de selecție cu sarcini specifice", cum ar fi o adresă de e-mail sau un număr de telefon.

171. Cu toate acestea, CEPD reamintește, de asemenea, că, în același timp, în contextul secțiunii 702, în cursul ultimei revizuiri a Scutului de confidențialitate s-a clarificat faptul că o „persoană" care urmează să fie identificată drept obiectiv al supravegherii ar putea circumscrie mai multe persoane care utilizează același identificator, cu condiția ca toate aceste persoane să fie persoane care nu sunt cetățeni americani/rezidenți SUA și să îndeplinească criteriile aplicabile pentru a fi vizate. De asemenea, CEPD reamintește că, în cursul celei de a treia revizuiri comune anuale a Scutului de confidențialitate din 2019, s-au solicitat clarificări suplimentare în contextul programului UPSTREAM pentru a exclude faptul că are loc un acces masiv și nediferențiat la datele cu caracter personal ale persoanelor care nu sunt cetățeni americani/rezidenți SUA[171].

---

[166] A se vedea hotărârea Schrems II a CJUE, punctul 180.
[167] A se vedea hotărârea Schrems II a CJUE, punctul 180.
[168] A se vedea hotărârea Schrems II a CJUE, punctul 182.
[169] A se vedea hotărârea Schrems II a CJUE, punctul 183.
[170] A se vedea raportul PCLOB privind programul de supraveghere operat în conformitate cu articolul 702 din FISA, pagina 100.
[171] A se vedea raportul aferent celei de a treia revizuiri comune, pagina 17, punctul 83.

172. În plus, CEPD reamintește că justificarea colectării în temeiul secțiunii 702 din FISA prin „scopul semnificativ de a obține informații externe" lasă în continuare loc unei anumite incertitudini în ceea ce privește limitarea scopului și necesitatea acesteia. Cu toate acestea, CEPD constată faptul că, în conformitate cu secțiunea 2 litera (a) părțile A și B din OE nr. 14086, activitățile de colectare de informații pe baza semnalelor electromagnetice se desfășoară numai după ce s-a stabilit că acestea sunt necesare pentru a promova o prioritate validată și numai în măsura și într-un mod proporțional cu această prioritate, precum și că acestea trebuie să fie cât mai adaptate pentru a promova prioritatea validată, ținând seama în mod corespunzător de factori relevanți, cum ar fi caracterul intruziv al colectării, sensibilitatea datelor sau inexistența unui impact disproporționat asupra vieții private și a libertăților civile. CEPD așteaptă totuși clarificări suplimentare cu privire la modul în care acest lucru va fi pus în aplicare și operaționalizat în mod concret, inclusiv în contextul aplicării secțiunii 702 din FISA.

173. În acest sens, în absența accesului direct la aceste informații, CEPD a solicitat o evaluare independentă a necesității și a proporționalității definiției „obiectivelor" și a conceptului de „informații externe" în temeiul secțiunii 702 din FISA (inclusiv în contextul programului UPSTREAM) în urma reînnoirii sale. CEPD consideră că apelul său anterior la o evaluare independentă suplimentară a procesului de aplicare a termenilor de selecție în cazuri specifice („stabilirea sarcinilor termenilor de selecție"), precum și la clarificări suplimentare în contextul programului UPSTREAM este relevant. Prin urmare, ținând seama de noul OE nr. 14086, CEPD solicită informații suplimentare pentru a evalua și a monitoriza, de asemenea, modul și măsura în care principiile recent introduse ale necesității și proporționalității vor fi aplicate în practică în acest context și se așteaptă ca acest lucru să fie evaluat și în contextul viitoarelor revizuiri comune.

174. CEPD salută faptul că, în calitate de agenție independentă de supraveghere pe deplin funcțională, Comitetul de supraveghere în materie de protecție a vieții private și a libertăților civile (PCLOB) a decis să deruleze „un proiect de supraveghere pentru a examina programul de supraveghere pe care îl desfășoară executivul în temeiul secțiunii 702 din Legea privind supravegherea activităților străine de spionaj (FISA), în așteptarea datei de expirare a secțiunii 702 din decembrie 2023 și a viitoarei examinări publice și de către Congres cu privire la reautorizarea sa"[172]. CEPD salută, de asemenea, faptul că „revizuirea respectivă vizează anumite domenii de interes pentru investigație, inclusiv, dar fără a se limita la interogările cu privire la informațiile persoanelor care sunt cetățeni americani/rezidenți SUA colectate în temeiul articolului 702[173] și colectarea «în contextul programului Upstream» efectuată în temeiul secțiunii 702" și „include, de asemenea, analizarea valorii și a eficacității anterioare și preconizate ale programului, precum și a caracterului adecvat al garanțiilor existente privind viața privată și libertățile civile"[174]. În consecință, CEPD subliniază că ar fi necesar accesul la constatările PCLOB din raportul în cauză cu privire la secțiunea 702 pentru a se evalua în mod adecvat și cuprinzător garanțiile de confidențialitate furnizate și aplicate în contextul acestui program de supraveghere.

175. Ținând seama de noul OE nr. 14086, CEPD solicită, de asemenea, informații suplimentare pentru a evalua și a monitoriza și modul și măsura în care principiile recent introduse ale necesității și

[172] A se vedea *NOTICE OF THE PCLOB OVERSIGHT PROJECT EXAMINING SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)* [COMUNICAREA PCLOB REFERITOARE LA PROIECTUL PCLOB DE SUPRAVEGHERE ÎN VEDEREA EXAMINĂRII ARTICOLULUI 702 DIN LEGEA PRIVIND SUPRAVEGHEREA ACTIVITĂȚILOR STRĂINE DE SPIONAJ (FISA)].

[173] A se vedea mai sus.

[174] A se vedea mai sus.

proporționalității, precum și celelalte garanții prevăzute în prezentul text vor fi aplicate în practică în acest context.

3.2.2.4.2 Colectarea de date în scopuri legate de securitatea națională în temeiul Ordinului Executiv nr. 12333

176. Astfel cum a recunoscut CJUE în hotărârea Schrems II, analiza legislației țării terțe pentru care se ia în considerare caracterul adecvat al nivelului de protecție nu ar trebui să se limiteze la legile și practicile care permit supravegherea în interiorul frontierelor fizice ale țării respective, ci ar trebui să includă și o analiză a temeiurilor juridice din legislația țării terțe respective care îi permit să desfășoare activități de supraveghere în afara teritoriului său în ceea ce privește datele UE. Limitările necesare ale accesului autorităților la date ar trebui extinse la datele cu caracter personal „aflate în tranzit" către țara respectivă, pentru care este recunoscut caracterul adecvat al nivelului de protecție.

177. CEPD salută raportul public general emis de PCLOB cu privire la Ordinul executiv nr. 12333 și publicat în aprilie 2021, dar observă că acest raport are un caracter general, deoarece majoritatea constatărilor sunt clasificate.

178. În acest context, având în vedere incertitudinea și lipsa de claritate cu privire la modul în care a fost aplicat OE nr. 12333, precum și importanța clarificării modului în care acesta va fi aplicat în lumina noului OE nr. 14086, CEPD subliniază încă o dată importanța rapoartelor preconizate ale PCLOB cu privire la acest text[175]. Cu toate acestea, CEPD înțelege că este probabil ca majoritatea conținutului lor să rămână clasificat, astfel că nicio informație suplimentară cu privire la funcționarea concretă a OE nr. 12333 și la necesitatea și proporționalitatea sa nu ar urma să fie disponibilă publicului sau CEPD.

179. Prin urmare, CEPD ar aprecia în special ca raportul PCLOB privind aplicarea OE nr. 14086 să nu fie clasificat, ci accesibil pe deplin după finalizare, inclusiv cu privire la părțile care ar evalua modul în care se vor aplica garanțiile prevăzute de OE nr. 14086 în legătură cu colectarea de date în temeiul OE nr. 12333. CEPD invită, de asemenea, Comisia să acorde o atenție deosebită acestui aspect în contextul viitoarelor revizuiri comune.

180. În general, în legătură cu diferitele instrumente juridice din cadrul juridic al SUA care prevăd posibilitatea colectării și a accesării și prelucrării ulterioare de date de către serviciile de informații din SUA, CEPD ar aprecia clarificări cu privire la interacțiunea acestora cu noul OE nr. 14086 și preconizează furnizarea unor asigurări privind soluționarea preocupărilor anterioare exprimate în avizele anterioare ale CEPD în ceea ce le privește prin adoptarea acestor noi garanții.

181. CEPD invită, de asemenea, Comisia să acorde o atenție deosebită acestor aspecte în contextul viitoarelor revizuiri comune.

3.2.2.4.3 Raportul PCLOB

182. CEPD salută faptul că OE nr. 14086 prevede, de asemenea, cerința ca PCLOB să prezinte un raport privind punerea în aplicare a ordinului executiv. CEPD subliniază că acest raport ar trebui să includă o evaluare a acestei posibilități specifice oferite de ordinul executiv de a colecta date în scopurile enumerate pentru colectarea direcționată, precum și în masă, inclusiv din motive tehnice, pentru a

[175] Raportul general privind OE nr. 12333 a rămas în cea mai mare parte clasificat – doar o scurtă versiune publică a fost pusă la dispoziția publicului, iar raportul și recomandările privind activitățile CIA de combatere a terorismului desfășurate în temeiul OE nr. 12333 au fost și ele doar parțial declasificate.

înțelege mai bine principalii termeni ai OE nr. 14086 și modul în care aceștia sunt înțeleși și aplicați în practică în cadrul diferitelor programe de supraveghere. Acest raport ar fi, de asemenea, necesar pentru a evalua modul în care va fi pus în aplicare ordinul executiv în cadrul procedurilor și politicilor interne ale elementelor Comunității Serviciilor de Informații.

3.2.3 Garanția C – Supravegherea

3.2.3.1 Introducere

183. Activitățile serviciilor de informații din SUA fac obiectul unui proces de supraveghere pe mai multe niveluri. Structura de supraveghere din SUA poate fi împărțită în supraveghere internă și externă. Toate elementele Comunității Serviciilor de Informații au funcționari în materie de supraveghere și conformitate, care efectuează supravegherea periodică a activităților de colectare de informații pe baza semnalelor electromagnetice, inclusiv inspectori generali și Responsabili pentru protecția vieții private și a libertăților civile. În plus, există organisme externe de supraveghere, cum ar fi Comitetul de supraveghere în materie de protecție a vieții private și a libertăților civile (PCLOB) și Comitetul pentru supravegherea serviciilor de informații.

184. CEPD reamintește că are loc o ingerință în momentul colectării datelor, dar și în momentul în care datele sunt accesate de o autoritate publică pentru prelucrare ulterioară. CEDO a precizat în mai multe rânduri că orice ingerință în dreptul la viață privată și la protecția datelor ar trebui să facă obiectul unui sistem de supraveghere eficace, independent și imparțial, care trebuie să fie asigurat fie de un judecător, fie de un alt organism independent[176] (de exemplu, o autoritate administrativă sau un organ parlamentar).

185. Deși CEDO și-a exprimat preferința ca un judecător să fie responsabil cu menținerea supravegherii, aceasta nu a exclus posibilitatea ca un alt organism să fie responsabil, „cu condiția ca acest organ să fie suficient de independent față de puterea executivă”[177] și „față de autoritățile care desfășoară supravegherea și [să fie] învestit cu competențe și atribuții suficiente pentru a exercita un control eficace și permanent”[178].

186. CEDO a adăugat că, atunci când se evaluează independența acestuia, trebuie să se țină seama de „metoda de numire și statutul juridic al membrilor organului de control”[179].

187. De asemenea, CEDO a precizat că trebuie să se verifice dacă activitățile organului de control sunt deschise controlului public. De exemplu, acest lucru ar putea fi realizat în cazul în care rapoartele anuale de control adresate guvernului, respectiv rapoartele publice, sunt prezentate Parlamentului și au fost discutate de Parlament[180].

188. Supravegherea independentă a punerii în aplicare a măsurilor de supraveghere a fost, de asemenea, luată în considerare de CJUE în hotărârea Schrems II, întrucât „[...] controlul exercitat de FISC urmărește astfel să verifice dacă programele de supraveghere menționate corespund obiectivului de

[176] CEDO, Klass și alții împotriva Germaniei, 6 septembrie 1978 („hotărârea Klass a CEDO'), punctele 17 și 51.
[177] Hotărârea Zakharov a CEDO, punctul 258; CEDO, Iordachi și alții împotriva Moldovei, 10 februarie 2009, punctele 40 și 51; CEDO, Dumitru Popescu împotriva României, 26 aprilie 2007, punctele 70-73.
[178] Hotărârea Klass a CEDO, punctul 56.
[179] Hotărârea Zakharov a CEDO, punctul 278.
[180] Hotărârea Zakharov a CEDO, punctul 283. CEDO, L. împotriva Norvegiei, 9 iunie 1990; CEDO, Kennedy împotriva Regatului Unit, 18 mai 2010, punctul 166.

a obține informații operative străine, însă nu se referă la aspectul „dacă persoanele sunt vizate în mod corespunzător pentru a dobândi informații operative străine»”[181].

3.2.3.2 Supravegherea internă

3.2.3.2.1 Inspectorii generali

189. CEPD recunoaște că inspectorilor generali li se încredințează o gamă largă de competențe, necesare pentru monitorizarea activităților serviciilor de informații. În special, inspectorii generali au acces la toate informațiile necesare pentru a evalua conformitatea generală a activității agenților cu legislația, inclusiv, dar fără a se limita la legile privind viața privată și protecția datelor, pot emite citații și pot lua o declarație sub jurământ oricărei persoane în legătură cu o investigație desfășurată de aceștia.

190. Pe baza celor de mai sus, CEPD consideră că inspectorii generali au, în general, competențe de investigare extinse. Cu toate acestea, ei nu dețin competențe de remediere obligatorii și emit doar recomandări fără caracter obligatoriu[182].

191. CEPD recunoaște că, în principiu, inspectorii generali nu sunt împiedicați să inițieze, să efectueze sau să finalizeze un audit sau o investigație sau să emită vreo citație în cursul oricărui audit sau al oricărei investigații și nici nu le este interzis să acționeze astfel[183]. În acest context, CEPD constată, cu toate acestea, că inspectorii generali se află sub autoritatea, conducerea și controlul șefului departamentului respectiv, care le poate interzice să aibă acces la informații, să efectueze o investigație și, printre altele, să emită o citație în cazurile în care șeful departamentului stabilește că o astfel de interdicție este necesară pentru protejarea intereselor naționale. Cu toate acestea, șeful departamentului trebuie să informeze comisiile competente ale Congresului SUA cu privire la exercitarea acestei competențe[184].

192. CEPD observă că inspectorii generali pot fi revocați numai de președintele SUA, care trebuie să informeze Congresul cu privire la motivele unei astfel de revocări.

193. CEPD constată că nu s-au adus modificări semnificative mecanismului de supraveghere internă de la emiterea avizelor GL29 și, ulterior, CEPD. Prin urmare, CEPD înțelege că, în conformitate cu Avizul 01/2016 al GL29[185], în general, există suficiente mecanisme de supraveghere internă.

3.2.3.3 Supravegherea externă

194. CEPD constată că, pe lângă organismele menționate mai jos, diverse alte organisme din cadrul guvernului SUA supraveghează activitățile serviciilor de informații din SUA, cum ar fi Comitetul pentru supravegherea serviciilor de informații (IOB) sau comitetele din cadrul Congresului. Acestea din urmă pot realiza investigații proprii și pot emite rapoarte.

---

[181] Hotărârea Schrems II a CJUE, punctul 179.
[182] Considerentul 105 din proiectul de decizie.
[183] Articolul 3 litera (a) din Legea privind inspectorii generali din 1978 (*Inspector General Act*).
[184] A se vedea, de exemplu, articolul 8 [pentru Departamentul Apărării (*Department of Defence*)], articolul 8E (pentru Departamentul de Justiție), articolul 8G litera (d) punctul 2 părțile A și B (pentru Agenția Națională de Securitate – NSA) din Legea privind inspectorii generali din 1978, titlul 50 din U.S.C. – articolul 403q litera (b) (pentru CIA), articolul 405 litera (f) din Legea privind autorizarea serviciilor de informații pentru anul fiscal 2010 (pentru Comunitatea Serviciilor de Informații).
[185] Avizul 01/2016 al GL29.

3.2.3.3.1 Comitetul de supraveghere în materie de protecție a vieții private și a libertăților civile

195. CEPD recunoaște rolul cuprinzător de supraveghere al PCLOB în ceea ce privește noul mecanism de recurs și punerea în aplicare a OE nr. 14086.

196. În primul rând, noile sale atribuții includ consultarea procurorului general cu privire la numirea judecătorilor din cadrul DPRC și a avocaților speciali. În al doilea rând, PCLOB va revizui anual procesul de recurs, și anume instrumentarea plângerilor eligibile în cadrul mecanismului de recurs. Aceasta va include dacă responsabilul pentru protecția libertăților civile și Curtea de Reexaminare a Protecției Datelor au instrumentat plângerile eligibile în timp util, dacă obțin acces deplin la informațiile necesare și dacă funcționează în conformitate cu OE nr. 14086, precum și dacă deciziile luate de responsabilul pentru protecția libertăților civile și DPRC sunt respectate de Comunitatea Serviciilor de Informații.

197. De asemenea, PCLOB trebuie consultat în procesul de actualizare de către serviciile de informații a politicilor și procedurilor interne pentru punerea în aplicare a OE nr. 14086. În plus, PCLOB va efectua o revizuire a politicilor și procedurilor actualizate și va evalua conformitatea acestora cu OE nr. 14086[186]. Deși constatările PCLOB nu sunt obligatorii *stricto sensu*, șeful fiecărui element al Comunității Serviciilor de Informații este obligat să analizeze cu atenție și să pună în aplicare sau să abordeze în alt mod toate recomandările cuprinse în orice astfel de revizuire, în conformitate cu legislația aplicabilă[187]. CEPD invită Comisia să acorde o atenție deosebită măsurii și modului în care recomandările PCLOB au fost puse în aplicare la nivel de agenție în cadrul revizuirilor viitoare, în cazul în care proiectul de decizie este adoptat.

198. CEPD reamintește că PCLOB, în calitate de comitet independent, este „încurajat", dar nu este obligat să efectueze revizuirea, în cazul în care se ține seama în mod corespunzător de garanțiile prevăzute în OE nr. 14086, iar Comunitatea Serviciilor de Informații a respectat pe deplin cerințele procesului de recurs. Cu toate acestea, CEPD înțelege că PCLOB a afirmat în explicația sa suplimentară adresată CEPD, precum și în public[188] că își va asuma rolul prevăzut în OE nr. 14086.

199. În plus, CEPD salută faptul că rezultatele rapoartelor PCLOB urmează să fie puse la dispoziția publicului. Ținând seama de faptul că diferitele organisme din cadrul mecanismului de recurs și cele ale Comunității Serviciilor de Informații trebuie, în principiu, să pună în aplicare recomandările din rapoartele PCLOB sau să le abordeze în alt mod, CEPD recunoaște că aceste recomandări joacă un rol important în ceea ce privește garanțiile de confidențialitate.

200. CEPD constată că accesul PCLOB la informații este restricționat în cazul în care președintele SUA autorizează desfășurarea de „operațiuni secrete"[189] de către departamentele, agențiile sau entitățile guvernului Statelor Unite ale Americii[190].

201. În urma avizelor sale anterioare, CEPD consideră că PCLOB este un organism independent, ale cărui recomandări au reprezentat o contribuție importantă la reformele din SUA și ale cărui rapoarte au

---

[186] A se vedea secțiunea 2 litera (c) punctul (iv) și secțiunea 2 litera (c) punctul (v) din OE nr. 14086.
[187] A se vedea secțiunea 2 litera (c) punctul (v) partea B din OE nr. 14086.
[188] https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf.
[189] Potrivit titlului 50 articolul 3093 litera (e) punctul 1 din U.S.C., termenul „operațiune secretă" înseamnă o activitate sau o serie de activități desfășurată (desfășurate) de guvernul Statelor Unite ale Americii de influențare a condițiilor politice, economice sau militare din străinătate, în cazul în care se intenționează ca rolul guvernului Statelor Unite ale Americii să nu fie evident sau recunoscut public, dar care nu include (includ) (1) activități al căror scop principal este de a obține informații, activități tradiționale de contrainformații [...].
[190] Titlul 42 articolul 2000ee litera (g) punctul 5 din U.S.C.; titlul 50 articolul 3093 litera (a) din U.S.C.

reprezentat o sursă deosebit de utilă pentru înțelegerea funcționării diferitelor programe de supraveghere, precum și un element esențial al structurii de supraveghere.

202. Cu toate acestea, în cadrul celei de a treia revizuiri comune anuale a Scutului de confidențialitate UE-SUA anterior, CEPD a regretat că PCLOB i-a furnizat aceleași informații precum cele puse la dispoziția publicului larg. În plus, a fost regretabil faptul că PCLOB nu a emis rapoarte suplimentare privind PPD-28 în urma primului său raport pentru a furniza elemente suplimentare cu privire la modul în care sunt aplicate garanțiile PPD-28, precum și un raport general actualizat privind articolul 702 din FISA.

203. Astfel, CEPD salută anunțul PCLOB adresat CEPD, potrivit căruia se preconizează publicarea unui raport de monitorizare privind articolul 702 din FISA în viitorul apropiat. În plus, CEPD își exprimă satisfacția cu privire la comunicarea de către PCLOB a angajamentului de a permite publicarea rapoartelor sale privind OE nr. 14086. Cu toate acestea, CEPD reamintește că publicarea rapoartelor neclasificate este reglementată de legislația SUA și trebuie să fie coordonată cu agențiile din cadrul Comunității Serviciilor de Informații și nu poate fi decisă de PCLOB din proprie inițiativă.

204. Prin urmare, în cazul în care proiectul de decizie este adoptat, CEPD reamintește că, în viitoarele revizuiri ale cadrului UE-SUA privind protecția datelor, experții CEPD care dețin o autorizare de securitate ar trebui să poată examina documente suplimentare și să discute elemente clasificate suplimentare, după cum este necesar pentru a se asigura că informațiile din rapoarte pot fi evaluate în mod adecvat, ținând seama, în același timp, de interesele relevante în materie de securitate națională și de măsurile aplicabile de protecție a vieții private.

205. CEPD salută independența PCLOB, precum și activitatea sa de supraveghere a comunității naționale a serviciilor de informații, care trebuie să respecte recomandările PCLOB sau să le abordeze în alt mod, aceste aspecte urmând a fi indicate în raportul PCLOB către Congresul SUA.

206. Având în vedere cerințele CEDO privind controlul public[191], respectiv ca rapoartele unui organism de supraveghere să fie prezentate Parlamentului și discutate de Parlament, CEPD consideră că este suficient ca PCLOB să își prezinte rapoartele cel puțin de două ori pe an președintelui SUA și, în special, comitetelor din cadrul Congresului (din cadrul Senatului și al Camerei Reprezentanților)[192], care sunt organismele parlamentare ale SUA.

3.2.3.3.2 Curtea de Supraveghere a Activităților Străine de Spionaj (FISC)

207. Curtea de Supraveghere a Activităților Străine de Spionaj este responsabilă cu supravegherea colectării datelor cu caracter personal în temeiul secțiunii 702 din FISA[193], iar deciziile FISC pot fi atacate înaintea Curții de Reexaminare a Supravegherii Activităților Străine de Spionaj (*Foreign Intelligence Surveillance Court of Review* – FISCR).

208. FISC supraveghează procesul de certificare pentru colectarea de informații externe în temeiul secțiunii 702 din FISA și autorizează supravegherea electronică, percheziții și alte măsuri de investigare în scopuri legate de obținerea de informații externe[194]. FISC autorizează, de asemenea, procedurile de direcționare și de reducere la minimum a intervențiilor, precum și de interogare a

[191] CEDO, hotărârea Zakharov, punctul 283 și CEDO, L. împotriva Norvegiei, 9 iunie 1990; CEDO, Kennedy împotriva Regatului Unit, 18 mai 2010, punctul 166.
[192] Titlul 42 articolul 2000ee litera (e) din U.S.C.
[193] Titlul 50 articolul 1881 litera (a) din U.S.C.
[194] www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court.

certificatelor, care sunt obligatorii din punct de vedere juridic pentru serviciile de informații din SUA[195]. În cazul în care FISC constată că nu au fost îndeplinite cerințele, aceasta poate refuza certificarea, integral sau parțial, și poate solicita modificarea procedurilor.

209. În cazul în care se identifică încălcări ale procedurilor de direcționare a intervențiilor, FISC poate solicita serviciului de informații relevant să ia măsuri de remediere[196]. Acestea pot varia de la măsuri individuale la măsuri structurale, de exemplu, de la încetarea acțiunii de obținere a datelor sau ștergerea datelor obținute în mod ilegal până la o modificare a practicii de colectare, inclusiv în ceea ce privește orientările pentru personal și formarea acestuia.

210. CEPD recunoaște că OE nr. 14086 prevede că Responsabilul pentru protecția libertăților civile și DPRC trebuie să raporteze încălcările procurorului general adjunct pentru securitate națională, care raportează aceste încălcări către FISC[197].

211. Astfel cum a constatat CJUE în hotărârea Schrems II, FISC nu autorizează măsuri de supraveghere individuală, ci mai degrabă programe de supraveghere[198]. Prin urmare, CEPD își menține îngrijorarea cu privire la faptul că FISC nu asigură o supraveghere judiciară eficace în ceea ce privește vizarea persoanelor care nu sunt cetățeni americani/rezidenți SUA, un aspect ce pare să nu fie soluționat prin noul OE nr. 14086.

212. În ceea ce privește autorizarea independentă prealabilă[199] a supravegherii în temeiul secțiunii 702 din FISA, CEPD regretă că, astfel cum reiese din proiectul de decizie[200] și din explicațiile furnizate de guvernul SUA, FISC nu pare să fie obligată să respecte garanțiile suplimentare prevăzute de OE nr. 14086 atunci când certifică programele care autorizează vizarea persoanelor care nu sunt cetățeni americani/rezidenți SUA. În opinia CEPD, garanțiile suplimentare cuprinse în acest ordin ar trebui totuși luate în considerare în acest context. CEPD reamintește că rapoartele PCLOB ar fi deosebit de utile pentru a evalua modul în care vor fi puse în aplicare garanțiile prevăzute de OE nr. 14086, precum și modul în care aceste garanții sunt aplicate atunci când sunt colectate date în temeiul articolului 702 din FISA.

3.2.4 Garanția D – Persoanele trebuie să dispună de căi de atac eficiente

213. CEPD reamintește că drepturile efective și opozabile ale persoanelor sunt de o importanță fundamentală pentru constatarea unui nivel adecvat de protecție a datelor într-o țară terță. Persoanele vizate trebuie să dispună de o cale de atac eficientă pentru a-și exercita drepturile atunci când consideră că acestea nu sunt sau nu au fost respectate. CJUE a explicat în hotărârile Schrems I și II că „o legislație care nu prevede nicio posibilitate a justițiabilului de a exercita căi legale pentru a avea acces la date cu caracter personal care îl privesc sau pentru a obține rectificarea sau ștergerea unor

[195] Titlul 50 articolul 1881a litera (i) din U.S.C.
[196] Titlul 50 articolul 1803 litera (h) din U.S.C.
[197] Secțiunea 3 litera (c) punctul (i) partea D din OE nr. 14086; secțiunea 3 litera (d) punctul (i) partea F din OE nr. 14086.
[198] Hotărârea Schrems II a CJUE, punctul 179.
[199] În ceea ce privește colectarea datelor în masă în temeiul OE nr. 12333 în situații care nu sunt de competența FISC, CEPD își exprimă îngrijorarea în legătură cu faptul că nu există un proces de autorizare prealabilă pentru colectarea datelor în masă (a se vedea, de asemenea, garanția B).
[200] Considerentul 165 din proiectul de decizie.

astfel de date nu respectă nici substanța dreptului fundamental la o protecție jurisdicțională efectivă, astfel cum este consacrat la articolul 47 din Cartă”[201].

214. În ceea ce privește căile de atac, sistemul judiciar american conține o limită importantă, care face foarte dificilă inițierea de proceduri judiciare împotriva măsurilor de supraveghere luate de guvernul SUA în fața instanțelor de drept comun. Constituția SUA impune unei persoane să își demonstreze calitatea procesuală, și anume să stabilească o „vătămare concretă, specifică și reală sau iminentă”[202]. În cazurile de supraveghere, o astfel de cerință pare a fi anulată prin lipsa notificării persoanelor care fac obiectul supravegherii, chiar și după încetarea acestor măsuri.

215. În acest context, CEPD salută faptul că OE nr. 14086 instituie un mecanism specific de recurs pentru a gestiona și soluționa plângerile înaintate de persoane care nu sunt cetățeni americani/rezidenți SUA referitoare la activitățile SUA de colectare de informații pe baza semnalelor electromagnetice. În temeiul acestui nou mecanism, cerința privind calitatea procesuală nu se aplică: în conformitate cu secțiunea 4 litera (k) punctul (ii) din OE nr. 14086, reclamantul nu trebuie să demonstreze că datele sale au făcut, de fapt, obiectul activităților SUA de colectare de informații pe baza semnalelor electromagnetice. Astfel, persoanele vizate pot invoca garanțiile prevăzute de OE nr. 14086, inclusiv cele prevăzute de alte legi și dispoziții relevante, astfel cum se menționează în secțiunea 4 litera (d) punctul (iii) din OE nr. 14086[203]. În această privință, noul mecanism adaugă o modalitate de recurs care altfel nu ar exista.

216. Noul mecanism funcționează pe două niveluri: la primul nivel, persoanele pot depune o plângere la Responsabilul pentru protecția libertăților civile din cadrul Biroului Directorului Serviciului Național de Informații. La al doilea nivel, persoanele au posibilitatea de a ataca decizia Responsabilului pentru protecția libertăților civile înaintea unui organism nou creat, așa-numita Curte de Reexaminare a Protecției Datelor (DPRC). Următoarele secțiuni se axează în primul rând pe al doilea nivel al mecanismului de recurs. CEPD consideră că Responsabilul pentru protecția libertăților civile, în calitate de funcționar guvernamental în exercițiul funcțiunii, nu este învestit cu un grad suficient de independență față de puterea executivă și, prin urmare, nu poate, ca atare, să îndeplinească în mod adecvat cerințele care decurg din articolul 47 din Cartă. Această evaluare a fost confirmată de Comisie în mai multe rânduri.

3.2.4.1 Poate fi suficientă instituirea DPRC pe baza unui ordin executiv?

217. DPRC nu este o instanță ordinară instituită de Congres în temeiul articolului III din Constituția SUA, ci pe baza unui ordin executiv emis de președintele SUA. Deși CEPD cunoaște și, în general, salută considerația subiacentă, și anume evitarea cerinței de a demonstra calitatea procesuală (a se vedea, de asemenea, punctul 215), acest lucru ridică o problemă fundamentală: poate îndeplini un astfel de mecanism de recurs cerințele articolului 47 din Cartă (și în ce măsură)? Potrivit acestei dispoziții, orice persoană ale cărei drepturi și libertăți garantate de dreptul Uniunii sunt încălcate are dreptul la o cale de atac eficientă în fața unei instanțe judecătorești constituite în prealabil prin lege.

218. În timp ce formularea în limba engleză a articolului 47 din Cartă se referă la un „tribunal”, alte versiuni lingvistice preferă utilizarea termenului „instanță”[204]. În hotărârea Schrems II, CJUE a reiterat că

[201] Hotărârea Schrems I a CJUE, punctul 95; hotărârea Schrems II a CJUE, punctul 187.
[202] Clapper/Amnesty International USA, 568 U.S. 398 (2013) II. p. 10.
[203] Secțiunea 5 litera (h) din OE nr. 14086 stabilește în mod explicit dreptul persoanelor vizate de a depune plângeri în conformitate cu mecanismul de recurs.
[204] De exemplu, „Gericht” în versiunea în limba germană.

„justițiabilii trebuie să dispună de posibilitatea de a exercita căi legale în fața unei instanțe judecătorești independente și imparțiale pentru a avea acces la date cu caracter personal care îi privesc sau de a obține rectificarea sau ștergerea unor astfel de date”[205]. Cu toate acestea, în același context de evaluare a caracterului adecvat al nivelului de protecție a datelor, CJUE consideră că o protecție jurisdicțională efectivă împotriva unor astfel de ingerințe poate fi asigurată nu numai de o instanță, ci și de un organism care oferă garanții în esență echivalente cu cele prevăzute la articolul 47 din Cartă[206]. În mod similar, Convenția Europeană a Drepturilor Omului prevede că „orice persoană, ale cărei drepturi și libertăți [...] au fost încălcate are dreptul de a se adresa efectiv unei instanțe naționale”[207], care, astfel cum a susținut în mod constant Curtea Europeană a Drepturilor Omului, nu trebuie să fie neapărat o autoritate judiciară[208]. Dimpotrivă, competențele și garanțiile procedurale de care dispune o autoritate, în special dacă aceasta este independentă de puterea executivă și asigură caracterul echitabil al procedurilor, sunt relevante pentru stabilirea eficienței căii de atac în fața autorității respective[209]. Se pare că niciuna din instanțe nu își întemeiază aprecierea pe criterii pur formale, ci consideră că garanțiile materiale sunt decisive.

219. În cauza Schrems II, CJUE a acordat o atenție deosebită posibilităților efective de exercitare a unei căi de atac în domeniul accesului la datele cu caracter personal în scopuri legate de securitatea națională. CEPD ia act de faptul că, procedând astfel, CJUE nu a discutat totuși elementul „constituirii în prealabil prin lege” de la articolul 47 din Cartă, chiar dacă nici mecanismul Ombudsmanului pentru Scutul de confidențialitate nu s-a bazat pe dreptul material al SUA. În loc să abordeze această problemă, CJUE a evaluat diferite aspecte pentru testul său cu privire la caracterul adecvat al nivelului de protecție, cum ar fi lipsa competențelor de remediere. Astfel, hotărârea Schrems II nu oferă nicio orientare cu privire la evaluarea elementului „constituirii în prealabil prin lege” în conformitate cu articolul 47 din Cartă. Cu toate acestea, există și alte hotărâri în care CJUE a formulat observații cu privire la această chestiune. Reiterând jurisprudența constantă a Curții Europene a Drepturilor Omului în această privință, CJUE a reamintit în cauzele C-487/19 și C-132/20 că motivul pentru introducerea termenului „constituită în prealabil prin lege” este acela de a se asigura că organizarea sistemului judiciar într-o societate democratică nu este lăsată la discreția executivului, ci este reglementată prin lege, aceasta emanând de la legiuitor, cu respectarea normelor care reglementează competența sa[210]. Astfel cum reiese din această afirmație, dreptul la o instanță judecătorească constituită în prealabil prin lege este foarte strâns legat de garantarea independenței.

220. În acest context, CEPD concluzionează că, în contextul evaluării caracterului adecvat al nivelului de protecție, mecanismul specific de recurs creat în temeiul OE nr. 14086, spre deosebire de căile de atac prevăzute în fața instanțelor constituite în temeiul articolului III, nu este, în sine, insuficient. Analiza nivelului de protecție în acest sens depinde de măsura în care garanțiile prevăzute în OE nr. 14086 și completate de Regulamentul PG asigură în mod suficient independența DPRC în raport cu celelalte puteri.

221. Comisia ar trebui să monitorizeze în permanență dacă normele prevăzute în OE nr. 14086 și dispozițiile sale suplimentare, în special cele menite să promoveze independența DPRC, sunt pe deplin puse în

[205] A se vedea hotărârea Schrems II a CJUE, punctul 194.
[206] A se vedea hotărârea Schrems II a CJUE, punctul 197.
[207] Articolul 13 din Convenția Europeană a Drepturilor Omului.
[208] Hotărârea Klass a CEDO, punctul 67; hotărârea Big Brother Watch a CEDO, punctul 359.
[209] Hotărârea Klass a CEDO, punctul 67; hotărârea Big Brother Watch a CEDO, punctul 359.
[210] A se vedea CJUE, Hotărârea din 6 octombrie 2021, W.Ż, C-487/19, ECLI:EU:C:2021:798 și Hotărârea din 29 martie 2022, Getin Noble Bank S.A., C-132/20, ECLI:EU:C:2022:235, punctul 129 și punctul 121.

aplicare și funcționează în mod eficace în practică. În plus, orice modificare a cadrului ar trebui să fie analizată cu atenție în ceea ce privește impactul asupra evaluării Comisiei în conformitate cu proiectul de decizie. În acest sens, CEPD observă că modificările aduse OE nr. 14086 și Regulamentul PG pot declanșa adoptarea unor acte de punere în aplicare imediat aplicabile de suspendare, abrogare sau modificare a deciziei privind caracterul adecvat al nivelului de protecție[211].

3.2.4.2 Independență suficientă în raport cu puterea executivă

222. În hotărârea Schrems II, CJUE a subliniat că independența instanței sau a organismului trebuie să fie asigurată, în special în raport cu puterea executivă, cu toate garanțiile necesare, inclusiv în ceea ce privește condițiile de revocare sau de anulare a numirii sale. Mai exact, CJUE a criticat faptul că Ombudsmanul este numit de secretarul de stat și îi raportează direct acestuia. Ombudsmanul a fost considerat ca făcând parte integrantă din Departamentul de Stat al SUA. CJUE a constatat, de asemenea, că nu există garanții speciale pentru revocarea sau anularea numirii Ombudsmanului, subminându-se astfel independența Ombudsmanului în raport cu puterea executivă.

223. CEPD recunoaște că dispozițiile OE nr. 14086 și ale Regulamentului PG de completare nu impun o obligație de raportare pentru DPRC către procurorul general, astfel cum ar fi normal în cazul unei relații de subordonare ierarhică. În plus, DPRC nu face obiectul „supravegherii de zi cu zi" de către procurorul general[212]. Aceste garanții reprezintă o îmbunătățire semnificativă față de Scutul de confidențialitate. Cu toate acestea, DPRC funcționează în cadrul puterii executive, și anume în cadrul Departamentului de Justiție. Din acest motiv, în special, punerea în aplicare și funcționarea eficace a garanțiilor în practică vor fi esențiale pentru a stabili dacă DPRC, deși nu face parte integrantă din Departamentul de Justiție, în calitate de entitate situată totuși în cadrul executivului, poate fi considerată suficient de independentă în practică. CEPD invită Comisia să monitorizeze cu atenție dacă aceste garanții sunt reflectate pe deplin în practică. În plus, CEPD sugerează clarificarea termenului „supraveghere de zi cu zi", astfel încât „judecătorii" DPRC să nu facă obiectul niciunui tip de supraveghere. Comisia a confirmat că „supravegherea de zi cu zi" este menită să fie înțeleasă în acest sens.

224. În plus față de garanțiile de mai sus, CCD UE-SUA prevede anumite garanții în ceea ce privește numirea și revocarea „judecătorilor" DPRC. Deși sunt numiți de procurorul general, numirea lor se bazează pe criteriile utilizate pentru a evalua candidații la funcția de judecători federal și implică o consultare a PCLOB. Revocarea „judecătorilor" înainte de expirarea mandatului lor sau de la o procedură în curs este posibilă numai în circumstanțe strict definite, care, după cum înțelege CEPD, sunt modelate după dispozițiile aplicabile judecătorilor federali[213]. Aplicarea acestor norme reprezintă un pas suplimentar în direcția consolidării poziției independente a DPRC, pentru care, după cum se menționa mai sus, punerea în aplicare în practică va fi esențială. Cu toate acestea, din proiectul de decizie ca atare nu reiese în mod clar dacă și în ce mod se vor respecta aceste cerințe în Statele Unite ale Americii. Pe baza explicațiilor suplimentare furnizate de Comisie și de guvernul SUA, CEPD înțelege că PCLOB poate aborda dispozițiile menționate mai sus în revizuirea sa anuală a procesului de recurs și că responsabilitatea de a monitoriza și de a asigura conformitatea cu toate cerințele legale a inspectorului general din cadrul Departamentului de Justiție include cerințele din OE nr. 14086 și reglementările de instituire a DPRC. CEPD invită Comisia să clarifice acest aspect în proiectul de decizie. Acestea fiind spuse, Comisia ar trebui să țină seama de aceste garanții atunci când monitorizează practica reală de prelucrare a datelor cu caracter personal, astfel cum a fost evaluată în proiectul de decizie.

---

[211] Considerentul 212 din proiectul de decizie.
[212] Articolul 201.7 litera (d) din Regulamentul PG.
[213] Secțiunea 3 litera (d) punctul (iv) din OE nr. 14086; Articolul 201.7 litera (d) din Regulamentul PG.

225. Proiectul de decizie nu specifică dacă și, în caz afirmativ, condițiile în care președintele SUA are autoritatea de a revoca „judecători" din DPRC sau de a anula numirea acestora. CEPD înțelege că o astfel de autoritate nu ar exista, astfel cum a fost explicat de Comisia Europeană și confirmat de reprezentanții guvernului SUA. CEPD sugerează clarificarea acestui aspect în decizia privind caracterul adecvat al nivelului de protecție.

226. „Judecătorii" DPRC sunt numiți pentru mandate reînnoibile de patru ani și, la momentul numirii lor inițiale, trebuie să nu fi fost angajați în cadrul puterii executive în ultimii doi ani[214]. Pe durata mandatului lor de „judecători" în cadrul DPRC, aceștia nu dețin nicio altă funcție oficială în cadrul guvernului SUA[215]. Cu toate acestea, spre deosebire de judecătorii federali americani, aceștia pot participa la activități extrajudiciare, inclusiv activități comerciale, activități financiare, activități de strângere de fonduri fără scop lucrativ, activități fiduciare și pot practica dreptul, în cazul în care aceste activități nu interferează cu îndeplinirea imparțială a sarcinilor lor sau cu eficacitatea sau independența DPRC[216]. Independența sistemului judiciar rezultă nu numai din libertatea de a nu fi obligat prin instrucțiuni, ci și din independența personală. În acest context, sunt relevanți factori precum mandatul, posibilitatea de a fi numit din nou și potențialul de conflicte de interese. Mandatul de patru ani prevăzut în OE nr. 14086, respectiv, în Regulamentul PG este mai scurt decât, de exemplu, mandatele judecătorilor CJUE (șase ani cu posibilitatea numirii din nou) și CEDO (nouă ani fără posibilitatea numirii din nou), însă, prin prisma duratei sale, nu dă naștere unor preocupări serioase. CEPD nu are cunoștință de nicio jurisprudență care să impună un mandat minim în acest caz[217]. CEPD recunoaște, de asemenea, că posibilitatea participării la activități extrajudiciare se acordă cu condiția ca, în termeni simpli, acestea să nu conducă la conflicte de interese care să compromită atribuțiile în cadrul DPRC. CEPD înțelege din explicațiile suplimentare ale guvernului SUA că aceste cerințe fac, de asemenea, obiectul revizuirii și monitorizării de către PCLOB și de către inspectorul general al Departamentului de Justiție (a se vedea punctul 226 de mai sus). Felul în care această cerință va fi aplicată și demonstrată în practică ar trebui, de asemenea, abordat în cadrul revizuirilor comune.

227. În conformitate cu secțiunea 3 litera (d) punctul (i) partea B din OE nr. 14086, toți „judecătorii" DPRC trebuie să dețină autorizări de securitate pentru a putea avea acces la informații clasificate, și anume pentru a-și îndeplini însăși funcția de soluționare a cauzelor în materie de securitate națională[218]. Prin contrast, unele acte cu putere de lege și norme administrative europene privind autorizarea de securitate scutesc judecătorii de cerința unei autorizări de securitate în măsura în care aceștia îndeplinesc sarcini judiciare, considerând că un astfel de control detaliat ar putea intra în conflict cu independența sistemului judiciar[219]. Potrivit explicațiilor guvernului SUA, în timp ce un candidat la o funcție judiciară într-o instanță din SUA face obiectul unei verificări amănunțite, după ce a fost numit în funcția de judecător federal în cadrul unei instanțe din SUA, un judecător federal nu este obligat să obțină o autorizare de securitate pentru a avea acces la documente clasificate relevante pentru cauză.

228. În opinia CEPD, circumstanțele prezentate mai sus evidențiază parțial diferențe între poziția și statutul unui judecător federal din SUA și ale unui „judecător" din cadrul DPRC. Cu toate acestea, garanțiile

[214] Articolul 201.3 litera (a) din Regulamentul PG.
[215] Articolul 201.3 litera (c) din Regulamentul PG.
[216] Articolul 201.7 litera (c) din Regulamentul PG.
[217] A se vedea, de asemenea, *mutatis mutandis*, CEDO (Marea Cameră), Centrum För Rättvisa împotriva Suediei, 25 mai 2021, punctul 346.
[218] A se vedea, de asemenea, articolul 201.11 litera (b) din Regulamentul PG și considerentul 177 din proiectul de decizie.
[219] De exemplu, articolul 2 alineatul (3) din legea germană privind autorizările de securitate.

oferite nu oferă motive de îndoială cu privire la independența DPRC. CEPD îndeamnă Comisia ca, în cazul adoptării proiectului de decizie, să acorde prioritate garanțiilor menționate mai sus în cursul primei revizuiri comune a CCD UE-SUA. În plus, CEPD se așteaptă ca, în cazul adoptării deciziei, Comisia să își respecte angajamentul de a suspenda, abroga sau modifica decizia, dacă executivul SUA alege să restricționeze garanțiile incluse în ordinul executiv[220].

3.2.4.3 Competențele DPRC

3.2.4.3.1 Accesul la informații

229. Protecția juridică efectivă impune ca o instanță să dispună de competențe de investigare suficiente pentru a reexamina măsura contestată. În cauza Kadi II, CJUE a statuat, în ceea ce privește articolul 47 din Cartă, că instanțele Uniunii Europene trebuie să se asigure că o decizie se întemeiază pe o bază factuală suficient de solidă[221]. CJUE precizează că „instanța Uniunii are sarcina să procedeze la această examinare solicitând, dacă este cazul, autorității competente a Uniunii să prezinte informațiile sau elementele de probă, confidențiale sau neconfidențiale, relevante pentru efectuarea unei asemenea examinări”[222], precum și că acesteia „nu i se poate opune secretul sau confidențialitatea [...] [acestor] informații sau elemente de probă”[223].

230. Potrivit considerentului 181 din proiectul de decizie, DPRC reexaminează deciziile Responsabilului pentru protecția libertăților civile cel puțin pe baza dosarului investigației desfășurate de acesta, precum și pe baza oricăror informații și observații furnizate de reclamant, de avocatul special sau de un serviciu de informații. Proiectul de decizie prevede, de asemenea, că DPRC are acces la toate informațiile necesare, pe care le poate obține prin intermediul Responsabilului pentru protecția libertăților civile. Acest lucru se bazează pe dispoziția de la alineatul 201.9 litera (b) din Regulamentul PG, care autorizează DPRC să „solicite Responsabilului pentru protecția libertăților civile din cadrul Biroului Directorului Serviciului Național de Informații să completeze dosarul cu informații explicative sau de clarificare specifice și ca Responsabilul pentru protecția libertăților civile din cadrul Biroului Directorului Serviciului Național de Informații să facă o serie de constatări factuale suplimentare atunci când este necesar pentru a permite DPRC să își desfășoare activitatea de reexaminare”. CEPD înțelege că evaluarea efectuată de DPRC nu se limitează în niciun fel la constatările făcute de Responsabilul pentru protecția libertăților civile la primul nivel al noului mecanism de recurs. Dimpotrivă, DPRC poate solicita atât informații juridice suplimentare, cât și, mai important, circumstanțe factuale suplimentare pentru a analiza dacă a avut loc o încălcare eligibilă. În același timp, CEPD observă, de asemenea, că aceste competențe de investigare în general extinse nu vizează accesul direct la datele deținute cu privire la persoana în cauză. Comisia a explicat că Responsabilul pentru protecția libertăților civile va funcționa întotdeauna ca intermediar atunci când DPRC solicită informații suplimentare. Prin urmare, accesul DPRC la informațiile necesare pentru a soluționa în mod independent o cerere de reexaminare se bazează, într-o anumită măsură, pe furnizarea informațiilor necesare de către Responsabilul pentru protecția libertăților civile. CEPD recunoaște că Responsabilul pentru protecția libertăților civile are obligația de a „oferi orice sprijin necesar” DPRC, iar serviciile de informații sunt obligate să ofere Responsabilului pentru protecția libertăților civile acces la informațiile necesare pentru ca DPRC să

[220] Considerentul 212 din proiectul de decizie.
[221] CJUE, Hotărârea din 18 iulie 2013, Comisia Europeană și alții/Yassin Abdullah Kadi, cauzele conexate C-584/10 P, C-593/10 P și C-595/10 P („hotărârea Kadi II a CJUE”), punctul 119.
[222] Hotărârea Kadi II a CJUE, punctul 120.
[223] Hotărârea Kadi II a CJUE, punctul 125.

desfășoare activitatea de reexaminare[224]. CEPD constată, de asemenea, că Responsabilul pentru protecția libertăților civile nu este independent și efectuează investigarea inițială a unei plângeri în prima etapă a procedurii de recurs. Prin urmare, CEPD salută faptul că PCLOB va verifica, în cursul revizuirilor sale anuale ale mecanismului de recurs, dacă DPRC a obținut acces deplin la toate informațiile necesare[225]. În plus, CEPD invită Comisia să includă acest aspect în revizuirile comune, în cazul în care proiectul de decizie este adoptat, pentru a examina implicațiile acestui sistem în practică.

3.2.4.3.2 Competențe de remediere

231. Una dintre deficiențele centrale ale Scutului de confidențialitate care a condus la declararea nevalidității sale de către CJUE în cauza Schrems II a fost lipsa unor competențe de remediere obligatorii pentru Ombudsman. CJUE a constatat că „[decizia menționată] nu conține nicio indicație potrivit căreia acest Ombudsman ar fi abilitat să adopte decizii obligatorii în privința respectivelor servicii”[226]. Simplul angajament (politic) din partea guvernului SUA potrivit căruia Comunitatea Serviciilor de Informații ar remedia orice încălcare a normelor aplicabile detectată de Ombudsman nu a fost suficient pentru a asigura un nivel de protecție în esență echivalent cu cel garantat la articolul 47 din Cartă.

232. În schimb, în cadrul noului mecanism de recurs, deciziile luate de Responsabilul pentru protecția libertăților civile și de DPRC au efect obligatoriu[227]. CEPD recunoaște, pe de o parte, că această autoritate nu se limitează la măsuri specifice, ci permite „remedierea adecvată” pentru a se „acorda reparații depline” în legătură cu o încălcare eligibilă identificată. În special, secțiunea 4 litera (a) din OE nr. 14086 menționează în mod explicit ștergerea datelor colectate în mod ilegal. Pe de altă parte, CEPD constată că formularea secțiunii 4 litera (a) din OE nr. 14086 creează o anumită incertitudine în ceea ce privește procesul de stabilire a unei astfel de „remedieri adecvate”. Deși o măsură ar trebui să fie concepută pentru a acorda reparații depline în legătură cu o încălcare, ar trebui să se aibă în vedere, de asemenea, „modalitățile prin care a fost abordată în mod obișnuit o încălcare de tipul celei identificate”[228]. Sensul și efectul unei astfel de cerințe sunt neclare. Prin urmare, CEPD invită Comisia să monitorizeze îndeaproape aplicarea măsurilor de remediere adoptate.

3.2.4.4 Depunerea unei plângeri în temeiul noului mecanism de recurs

233. Mecanismul de recurs instituit în temeiul OE nr. 14086 se aplică numai plângerilor eligibile transmise de autoritatea publică competentă dintr-un stat eligibil cu privire la activitățile de colectare de informații pe baza semnalelor electromagnetice desfășurate de Statele Unite în legătură cu orice încălcare eligibilă[229]. Prin urmare, pentru a beneficia de această protecție juridică, trebuie îndeplinite mai multe condiții.

3.2.4.4.1 Desemnarea ca stat eligibil

234. În primul rând, țara sau organizația de integrare economică regională de unde au fost transferate datele către Statele Unite ale Americii trebuie să fi fost desemnată drept stat eligibil înainte de transferul de date care stă la baza plângerii[230]. În mod evident, este esențial ca mecanismul de recurs

[224] A se vedea secțiunea 3 litera (c) punctul (i) partea H și secțiunea 3 litera (d) punctul (iii) din OE nr. 14086.
[225] Secțiunea 3 litera (e) punctul (i) din OE nr. 14086.
[226] Hotărârea Schrems II a CJUE, punctul 196.
[227] A se vedea secțiunea 3 litera (c) punctul (ii), respectiv secțiunea 3 litera (d) punctul (ii) din OE nr. 14086.
[228] Secțiunea 4 litera (a) din OE nr. 14086.
[229] Secțiunea 3 litera (a) din OE nr. 14086.
[230] Secțiunea 4 litera (d) punctul (i) și secțiunea 4 litera (k) punctul (i) din OE nr. 14086.

prevăzut să fie disponibil la momentul intrării în vigoare a deciziei privind caracterul adecvat al nivelului de protecție. În consecință, considerentul 196 din proiectul de decizie prevede că intrarea în vigoare a deciziei este condiționată, printre altele, de desemnarea Uniunii ca entitate eligibilă în sensul mecanismului de recurs. În fapt, Comisia pare să presupună că desemnarea va avea loc înainte de adoptarea deciziei, întrucât proiectul de decizie include deja un spațiu rezervat pentru desemnarea de către procurorul general a UE[231] (spre deosebire de includerea desemnării ca o condiție prealabilă în partea dispozitivă a proiectului de decizie).

3.2.4.4.2 Afectarea intereselor din perspectiva vieții private și a libertăților civile și „calitatea procesuală"

235. O „plângere eligibilă" trebuie să se întemeieze pe o presupusă „încălcare eligibilă", care, la rândul său, implică necesitatea ca încălcarea să afecteze interesele individuale ale reclamantului din perspectiva vieții private și a libertăților civile[232]. CEPD înțelege, pe baza unor explicații suplimentare din partea Comisiei, că „afectarea" nu implică nicio formă de restricționare a admisibilității unei plângeri. Mai degrabă, astfel cum a afirmat Comisia, o astfel de afectare ar privi orice plângere referitoare la prelucrarea datelor cu caracter personal pentru activități de colectare de informații pe baza semnalelor electromagnetice desfășurate cu încălcarea dispozițiilor menționate în secțiunea 4 litera (d) punctul (iii), de exemplu a garanțiilor prevăzute de OE nr. 14086. CEPD regretă faptul că acest lucru nu este specificat în textul proiectului de decizie și invită Comisia să clarifice în continuare noțiunea de „afectare" pentru a se asigura că orice încălcare a drepturilor persoanelor vizate este evaluată și remediată și că nu există niciun nivel de „gravitate" care trebuie demonstrat pentru a avea acces la calea de atac și la o remediere adecvată.

236. Astfel cum s-a menționat anterior, o plângere înaintată în temeiul OE nr. 14086 nu impune reclamantului să își demonstreze calitatea procesuală (a se vedea punctul 215)[233]. CEPD salută clarificarea din secțiunea 4 litera (k) din OE nr. 14086, potrivit căreia se va aplica un „test de încredere", nefiind necesar să se demonstreze că datele reclamantului au fost în fapt accesate prin activități de colectare de informații pe baza semnalelor electromagnetice. Instituirea mecanismului de recurs este un pas important, deoarece cerința privind calitatea procesuală face foarte dificilă contestarea măsurilor de supraveghere în fața instanțelor de drept comun din Statele Unite.

237. Pe baza celor de mai sus, CEPD nu consideră că sesizarea instanțelor de drept comun, la care se referă, de asemenea, proiectul de decizie[234], oferă un nivel adecvat de protecție[235]. În acest sens, CEPD reamintește preocupările sale deja exprimate în mai multe rânduri în legătură cu cerința privind calitatea procesuală în fața instanțelor de drept comun[236]. În plus, în baza unor declarații suplimentare ale guvernului SUA, CEPD înțelege că, deși OE nr. 14086 nu împiedică sesizarea instanțelor cu competență generală, nu este clar cum ar aplica o astfel de instanță acest ordin. Această chestiune ar putea fi analizată suplimentar în cadrul viitoarelor revizuiri, în cazul adoptării proiectului de decizie.

---

[231] Nota de subsol 320 din proiectul de decizie.
[232] Secțiunea 4 litera (k) punctul (i) și secțiunea 4 litera (d) punctul (ii) din OE nr. 14086.
[233] Clapper/Amnesty International USA, 568 U.S. 398 (2013) II. p. 10.
[234] Considerentul 187 și următoarele din proiectul de decizie.
[235] A se vedea, de asemenea, hotărârea Schrems II a CJUE, punctele 191 și 192.
[236] A se vedea Avizul 01/2016 al GL29, p. 43.

3.2.4.4.3 Procedura de înaintare a unei plângeri

238. CEPD sprijină, în principiu, procedura de direcționare a unei plângeri prin intermediul autorităților de supraveghere ale statelor membre și consideră în continuare că identificarea reclamantului ar trebui să aibă loc pe teritoriul UE. Cu toate acestea, la fel ca în temeiul mecanismului Ombudsmanului pentru Scutul de confidențialitate, proiectul de decizie prevede că o persoană vizată care dorește să înainteze o astfel de plângere trebuie să o depună la o autoritate de supraveghere dintr-un stat membru al UE competentă să supravegheze serviciile naționale de securitate și/sau prelucrarea datelor cu caracter personal de către autoritățile publice[237]. În acest sens, CEPD reamintește preocupările sale deja exprimate în avizul GL29 privind Scutul de confidențialitate, de exemplu dificultățile potențiale cu care se confruntă persoanele în identificarea autorității competente, având în vedere diversitatea mecanismelor de supraveghere a serviciilor naționale de securitate din statele membre[238]. Având în vedere implicarea autorităților naționale pentru protecția datelor în aplicarea și supravegherea CCD UE-SUA, este mai adecvat ca plângerile să se înainteze prin intermediul acestora.

3.2.4.5 Decizia DPRC

239. După finalizarea reexaminării cererii reclamantului, DPRC nu trebuie să dezvăluie dacă reclamantul a făcut sau nu obiectul activităților SUA de colectare de informații pe baza semnalelor electromagnetice. În schimb, reclamantului i se notifică faptul că „reexaminarea fie nu a identificat încălcări eligibile, fie Curtea de Reexaminare a Protecției Datelor a emis o decizie care impune o remediere adecvată”[239]. Acest răspuns standard servește scopului în general legitim de protejare a informațiilor sensibile cu privire la activitățile SUA de colectare de informații. Cu toate acestea, CEPD își exprimă îngrijorarea cu privire la faptul că OE nr. 14086 nu prevede nicio derogare de la răspunsul standard al DPRC.

240. În cauza Kadi II, CJUE a trebuit să abordeze, interesele divergente aferente, pe de o parte, secretului de stat și, pe de altă parte, procedurilor echitabile și, în măsura posibilului, cu respectarea principiului contradictorialității. CJUE a stabilit că, în împrejurări în care considerații imperative având legătură cu securitatea națională se opun comunicării către persoana vizată a anumitor informații sau a anumitor elemente de probă, revine, totuși, instanțelor sarcina de a pune în aplicare, în cadrul controlului jurisdicțional pe care îl exercită, tehnici care să permită concilierea considerațiilor legitime legate de securitate în privința naturii și a surselor de informații și a necesității de a garanta persoanei în cauză în suficientă măsură respectarea drepturilor sale procedurale precum dreptul de a fi ascultat și principiul contradictorialității[240]. CJUE a precizat, de asemenea, că, atunci când procedează la o examinare a tuturor elementelor de fapt sau de drept furnizate de autoritatea competentă a Uniunii, instanțele trebuie să verifice temeinicia motivelor invocate de autoritatea menționată pentru a se opune unei asemenea comunicări[241]. În cazul în care se concluzionează că motivele invocate de autoritatea competentă a Uniunii se opun efectiv comunicării către persoana vizată a informațiilor sau a elementelor de probă prezentate, este necesar să se pună în balanță în mod corespunzător cerințele legate de dreptul la protecție jurisdicțională efectivă și cele care decurg din securitatea națională[242]. În scopul realizării unei asemenea puneri în balanță, este permis să se recurgă la posibilități precum

[237] Considerentul 169 din proiectul de decizie.
[238] Avizul 01/2016 al GL29, p. 48 și 49.
[239] Secțiunea 3 litera (d) punctul (i) partea H din OE nr. 14086. Secțiunea din OE nr. 14086 prevede acest răspuns și pentru Responsabilul pentru protecția libertăților civile.
[240] Hotărârea Kadi II a CJUE, punctul 125.
[241] Hotărârea Kadi II a CJUE, punctul 126.
[242] Hotărârea Kadi II a CJUE, punctul 128.

comunicarea unui rezumat al conținutului informațiilor sau al elementelor de probă în discuție[243]. Deși constatările instanței nu impun cerințe pentru decizia pronunțată de o instanță, ci se referă mai degrabă la decizia autorității competente și la desfășurarea procedurilor judiciare, acestea oferă indicații cu privire la punerea în balanță a intereselor menționate mai sus în contextul dreptului la o protecție jurisdicțională efectivă. Pentru orientări suplimentare, se poate face trimitere și la cauza Big Brother Watch, în care CEDO, făcând referire la caracterul echitabil al procedurilor și, în special, la principiul contradictorialității, a statuat că deciziile unui organism judiciar sau ale unui alt organism independent ar trebui să fie motivate[244].

241. CEPD recunoaște că deciziile DPRC sunt, într-adevăr, motivate. DPRC este obligată în mod expres să emită o decizie scrisă în care să își prezinte concluziile și să precizeze orice măsură de remediere adecvată[245]. În plus, CEPD observă că persoana în cauză urmează să fie notificată în cazul în care informațiile referitoare la o reexaminare efectuată de DPRC au fost declasificate[246]. CEPD recunoaște, de asemenea, rolul avocaților speciali prevăzuți de noul mecanism de recurs, care include promovarea interesului reclamantului în această chestiune[247]. Cu toate acestea, având în vedere implicațiile jurisprudenței CJUE și a CEDO prezentate mai sus și ținând seama de faptul că decizia DPRC nu poate fi atacată, ci este definitivă[248], CEPD își exprimă îngrijorarea cu privire la aplicarea generală a răspunsului standard al DPRC. CEPD reamintește că PCLOB va revizui în mod independent funcționarea noului mecanism de recurs și invită Comisia să acorde o atenție deosebită acestei chestiuni, inclusiv oricărei evaluări a acestui aspect de către PCLOB, în cursul viitoarelor revizuiri ale deciziei, în cazul adoptării sale.

4 PUNEREA ÎN APLICARE ȘI MONITORIZAREA PROIECTULUI DE DECIZIE

242. În ceea ce privește monitorizarea și revizuirea proiectului de decizie, CEPD observă că, în conformitate cu jurisprudența CJUE, „având în vedere că nivelul de protecție asigurat de o țară terță este susceptibil să evolueze, revine Comisiei, după adoptarea unei decizii în temeiul [articolului 45 din RGPD], sarcina de a verifica în mod periodic dacă constatarea referitoare la nivelul de protecție adecvat asigurat de țara terță în cauză este în continuare justificată în fapt și în drept. O astfel de verificare se impune, în orice caz, atunci când există indicii care dau naștere unei îndoieli în această privință”[249].

243. În plus, CEPD observă că scrisoarea din partea DoC prevede că DoC și alte agenții ale SUA, după caz, vor organiza reuniuni periodice cu Comisia, cu APD din UE interesate și cu reprezentanții corespunzători ai CEPD[250].

244. CEPD consideră că aspecte precum protecția în temeiul legislației la nivel de stat în ceea ce privește accesul autorităților de aplicare a legii, derogarea pentru colectarea temporară în masă în vederea colectării direcționate de informații de către autoritățile de securitate națională din SUA, aplicarea în practică a principiilor recent introduse ale necesității și proporționalității, inclusiv în contextul programului UPSTREAM, interacțiunea dintre OE nr. 14086 și diversele instrumente juridice ale SUA

[243] Hotărârea Kadi II a CJUE, punctul 129.
[244] Hotărârea Big Brother Watch a CEDO, punctul 359.
[245] Articolul 201.9 litera (g) din Regulamentul PG.
[246] Secțiunea 3 litera (d) punctul (v) din OE nr. 14086.
[247] Articolul 201.8 litera (g) din Regulamentul PG.
[248] Articolul 201.9 litera (g) din Regulamentul PG.
[249] Hotărârea Schrems I a CJUE, punctul 76. A se vedea, de asemenea, articolul 3 alineatul (4) din proiectul de decizie.
[250] Anexa III la proiectul de decizie.

care permit serviciilor de informații din SUA să colecteze și să prelucreze ulterior date cu caracter personal, politicile și procedurile interne de punere în aplicare, modul în care aceste garanții vor fi, de asemenea, luate în considerare în contextul supravegherii realizate de FISC și modul de funcționare efectivă a mecanismului de recurs, precum și aspectele legate de transferurile ulterioare, deciziile automatizate, supravegherea materială și eficace a principiilor CCD, asigurarea respectării efective a acestora și căile de atac eficiente vor necesita o atenție deosebită în cursul următoarelor revizuiri periodice.

245. CEPD observă că revizuirea constatării în ceea ce privește caracterul adecvat al nivelului de protecție va avea loc după un an de la data notificării deciziei privind caracterul adecvat al nivelului de protecție către statele membre și, ulterior, cel puțin o dată la patru ani[251]. În vederea consolidării în continuare a monitorizării continue a deciziei privind caracterul adecvat al nivelului de protecție, CEPD invită Comisia să efectueze revizuirile ulterioare cel puțin o dată la trei ani.

246. În ceea ce privește implicarea practică a CEPD și a reprezentanților săi în pregătirea și desfășurarea revizuirilor periodice viitoare, CEPD reiterează că orice documentație relevantă, inclusiv corespondența, ar trebui comunicată în scris CEPD cu suficient timp înainte de desfășurarea revizuirilor. La fel ca în cazul revizuirilor efectuate în temeiul Scutului de confidențialitate, CEPD recomandă ca modalitățile de revizuire să fie stabilite și convenite între Comisie, administrația SUA și CEPD cel târziu cu trei luni înainte de revizuire.

247. În plus, CEPD constată și salută faptul că, în considerentul 212 din proiectul de decizie, se oferă exemple de modificări care subminează nivelul de protecție, acestea putând justifica inițierea unei „proceduri de abrogare de urgență" în legătură cu modificările care ar putea apărea în ceea ce privește Ordinul executiv nr. 14086 și Regulamentul PG aferent.

Pentru Comitetul European pentru Protecția Datelor,

Președinta

(Andrea Jelinek)

[251] A se vedea articolul 3 alineatul (4) din proiectul de decizie.