Avizul 14/2021 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

CUPRINS

Comitetul european pentru protecția datelor,

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 (denumit în continuare „RGPD”),

având în vedere Acordul privind Spațiul Economic European (denumit în continuare „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[1],

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

ADOPTĂ PREZENTUL AVIZ:

1. REZUMAT

1. La 19 februarie 2021, Comisia Europeană a aprobat proiectul său de decizie de punere în aplicare (denumit în continuare „proiectul de decizie”) privind protecția adecvată a datelor cu caracter personal asigurată de Regatul Unit al Marii Britanii și Irlandei de Nord (denumit în continuare „Regatul Unit”) în temeiul RGPD[2]. Ulterior, Comisia Europeană a lansat procedura pentru adoptarea formală a acestuia.

2. La aceeași dată, Comisia Europeană a solicitat avizul Comitetului european pentru protecția datelor (denumit în continuare „CEPD”)[3]. Evaluarea CEPD cu privire la caracterul adecvat al nivelului de protecție asigurat în Regatul Unit a fost efectuată pe baza examinării proiectului de decizie, precum și pe baza unei analize a documentației puse la dispoziție de Comisia Europeană.

3. CEPD s-a axat atât pe evaluarea aspectelor generale ale proiectului de decizie referitoare la RGPD, cât și pe evaluarea accesului autorităților publice la datele cu caracter personal transferate din SEE în scopul asigurării respectării legii și al securității naționale, inclusiv în ceea ce privește căile de atac aflate la dispoziția persoanelor fizice din SEE. De asemenea, CEPD a evaluat punerea în aplicare a garanțiilor prevăzute de cadrul juridic al Regatului Unit, precum și eficacitatea acestora.

4. În acest demers, CEPD a folosit ca referință principală criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD[4], adoptate în februarie 2018, și Recomandările 02/2020 ale CEPD privind garanțiile esențiale europene pentru măsurile de supraveghere[5].

[1] Trimiterile la „statele membre” din prezentul aviz trebuie înțelese ca trimiteri la „statele membre ale SEE”.
[2] A se vedea comunicatul de presă al Comisiei Europene, Protecția datelor: Comisia Europeană lansează procesul privind fluxurile de date cu caracter personal către Regatul Unit, 19 februarie 2021, https://ec.europa.eu/commission/presscorner/detail/ro/ip_21_661.
[3] Idem.
[4] A se vedea Grupul de lucru „Articolul 29”, Criterii de referință privind caracterul adecvat al nivelului de protecție, adoptate la 28 noiembrie 2017, astfel cum au fost revizuite ultima dată și adoptate la 6 februarie 2018, WP254 rev.01 (aprobate de CEPD, a se vedea https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines); (denumite în continuare „Criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD”).

1.1. Domenii de convergență

5. Obiectivul principal urmărit de CEPD este de a emite un aviz pentru Comisia Europeană cu privire la caracterul adecvat al nivelului de protecție oferit persoanelor fizice în Regatul Unit. Este important să se recunoască faptul că CEPD nu se așteptă să aibă loc o reproducere a legislației europene privind protecția datelor în cadrul juridic aplicat în Regatul Unit.

6. Cu toate acestea, CEPD reamintește faptul că, în conformitate cu articolul 45 din RGPD și cu jurisprudența Curții de Justiție a Uniunii Europene (denumită în continuare „CJUE"), se consideră că legislația unei țări terțe oferă un nivel de protecție adecvat atunci când legislația respectivă este aliniată la esența principiilor fundamentale consacrate în RGPD. Cadrul de protecție a datelor din Regatul Unit se bazează în mare parte pe cadrul de protecție a datelor din UE [în special RGPD și Directiva (UE) 2016/680 a Parlamentului European și a Consiliului, (denumită în continuare „Directiva UE privind protecția datelor în materie de aplicare a legii" sau „LED")], situație care rezultă din faptul că Regatul Unit a fost stat membru al UE până la 31 ianuarie 2020. În plus, pe lângă faptul că transpune Directiva UE privind protecția datelor în materie de aplicare a legii, conferă competențe autorității naționale de supraveghere a protecției datelor și impune obligații în sarcina acesteia, și anume Biroul comisarului pentru informații din Regatul Unit (denumit în continuare „ICO"), Legea Regatului Unit privind protecția datelor din 2018, care a intrat în vigoare la 23 mai 2018 și a abrogat Legea Regatului Unit privind protecția datelor din 1998, descrie în detaliu aplicarea RGPD în dreptul Regatului Unit. Prin urmare, CEPD recunoaște că Regatul Unit a reflectat, în cea mai mare parte, RGPD în cadrul său de protecție a datelor.

7. **Întrucât procesul de analiză a vizat legislația și practicile unei țări terțe care a fost până de curând stat membru al UE, este evident că CEPD a identificat numeroase aspecte ca fiind în esență echivalente.**

8. În ceea ce privește protecția datelor, CEPD constată că există o strânsă aliniere între cadrul prevăzut în RGPD și cadrul juridic din Regatul Unit cu privire la anumite dispoziții esențiale, cum ar fi: concepte (de exemplu, „date cu caracter personal"; „prelucrarea datelor cu caracter personal"; „operator"); motive care justifică prelucrarea legală și echitabilă în scopuri legitime; limitarea scopului; calitatea și proporționalitatea datelor; păstrarea, securitatea și confidențialitatea datelor; transparența; categoriile speciale de date; marketingul direct; procesul decizional automatizat și crearea de profiluri.

1.2. Provocări

9. Regatul Unit a fost, până de curând, stat membru al UE; prin urmare, în analiza legislației și a practicilor sale, CEPD a identificat numeroase aspecte care sunt în esență echivalente. În același timp, având în vedere rolul care îi revine în procesul de adoptare a unei constatări cu privire la caracterul adecvat al nivelului de protecție, însă și constrângerile legate de timp, CEPD a decis să își concentreze atenția asupra acelor aspecte cu privire la care consideră că se impune o analiză mai atentă și mai detaliată.

[5] A se vedea Recomandările 02/2020 ale CEPD privind garanțiile esențiale europene pentru măsurile de supraveghere, adoptate la 10 noiembrie 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_ro.pdf.

10. Cu toate acestea, există în continuare provocări, iar CEPD consideră că următoarele elemente ar trebui analizate suplimentar pentru a se asigura că nivelul de protecție în esență echivalent este atins și ar trebui să fie monitorizat îndeaproape în Regatul Unit de către Comisia Europeană.

1.2.1. Considerații generale

11. O primă provocare de ordin general se referă la monitorizarea evoluției sistemului juridic din Regatul Unit privind protecția datelor în ansamblul său. Într-adevăr, Guvernul Regatului Unit și-a exprimat intenția de a elabora politici separate și independente în domeniul protecției datelor, cu o posibilă intenție de a se abate de la legislația europeană privind protecția datelor. Astfel de declarații politice nu s-au materializat încă în cadrul juridic al Regatului Unit. Cu toate acestea, o astfel de **posibilă divergență viitoare ar putea crea riscuri pentru menținerea nivelului de protecție oferit datelor cu caracter personal transferate din UE. Prin urmare, Comisia Europeană este invitată să monitorizeze îndeaproape aceste evoluții de la intrarea în vigoare a deciziei sale privind caracterul adecvat al nivelului de protecție și să ia măsurile necesare, inclusiv prin modificarea și/sau suspendarea deciziei, dacă este necesar.**

1.2.2. Aspecte generale privind protecția datelor

12. În primul rând, așa-numita „**derogare privind imigrația**”, prevăzută în **anexa 2 la Legea privind protecția datelor din 2018, partea 1**, punctul 4, **este formulată „în sens larg”**. În special, aceasta se aplică și în cazul în care datele cu caracter personal nu sunt colectate în scopul controlului imigrației de către un operator, ci sunt puse de acesta din urmă la dispoziția unui alt operator care prelucrează astfel de date cu caracter personal în scopul controlului imigrației.

13. CEPD invită Comisia Europeană să verifice stadiul procedurilor în cauza *Open Rights Group și alții, R (în baza cererii înaintate de aceasta)/Secretary of State for the Home Department și alții, 2019, Înalta Curte de Justiție (EWHC) 2562 (secția de contencios administrativ)* și, întrucât această hotărâre nu este definitivă (nu are autoritate de lucru judecat), să verifice dacă este confirmată sau revizuită prin hotărârea pronunțată în apel, ținând seama de orice actualizare în această privință și specificând-o în decizie. **De asemenea, CEPD solicită Comisiei Europene să furnizeze în decizia privind caracterul adecvat al nivelului de protecție informații suplimentare în legătură cu derogarea privind imigrația[6], în special în ceea ce privește necesitatea și proporționalitatea unei astfel de derogări extinse în legislația Regatului Unit, mai ales având în vedere domeniul larg de aplicare *ratione personae*.** În același timp, CEPD invită Comisia Europeană să analizeze în continuare dacă există garanții suplimentare în cadrul juridic din Regatul Unit sau dacă acestea ar putea fi avute în vedere, de exemplu, prin intermediul unor instrumente obligatorii din punct de vedere juridic care ar completa derogarea privind imigrația prin sporirea previzibilității acesteia și a garanțiilor pentru persoanele vizate, permițând, de asemenea, o evaluare și o monitorizare mai bună și promptă a cerințelor privind necesitatea și proporționalitatea.

[6] De asemenea, ca rezultat al revizuirii în curs a aplicării derogării privind imigrația menționate la pagina 5 din documentul emis de Guvernul Regatului Unit intitulat „Explanatory Framework for Adequacy Discussions” (Cadru explicativ privind dezbaterile pe tema caracterului adecvat al nivelului de protecție), secțiunea E3: anexa 2 Restricții, 13 martie 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf.

14. În al doilea rând, deși CEPD recunoaște că Regatul Unit a reflectat, în cea mai mare parte, capitolul V din RGPD în cadrul său de protecție a datelor, **în ceea ce privește transferurile ulterioare**, CEPD a identificat anumite aspecte ale cadrului juridic din Regatul Unit care ar putea submina nivelul de protecție a datelor cu caracter personal transferate din SEE.

15. Într-adevăr, articolul 44 din RGPD[7] prevede că transferurile și transferurile ulterioare de date cu caracter personal au loc doar dacă nivelul de protecție a persoanelor fizice garantat de RGPD nu este subminat. **Aceasta înseamnă nu numai că legislația Regatului Unit trebuie să fie „în esență echivalentă" cu legislația UE în ceea ce privește prelucrarea datelor cu caracter personal transferate către Regatul Unit în temeiul viitoarei decizii privind caracterul adecvat al nivelului de protecție, ci și că normele aplicabile în Regatul Unit cu privire la transferul ulterior al acestor date către țări terțe trebuie să asigure în continuare un nivel de protecție în esență echivalent.**

16. Deși CEPD ia act de capacitatea Regatului Unit, în temeiul cadrului său juridic, de a recunoaște teritoriile ca oferind un nivel de protecție a datelor adecvat în lumina cadrului de protecție a datelor din Regatul Unit, CEPD dorește să sublinieze că ar putea fi posibil ca aceste teritorii să nu beneficieze, până în prezent, de o decizie privind caracterul adecvat al nivelului de protecție adoptată de Comisia Europeană și să nu asigure un nivel de protecție „în esență echivalent" cu cel garantat în SEE. Acest lucru ar putea conduce la posibile riscuri în ceea ce privește protecția oferită datelor cu caracter personal transferate din SEE, în special în cazul în care, în viitor, cadrul de protecție a datelor din Regatul Unit se va abate de la acquis-ul UE. În plus, Regatul Unit consideră deja că țările terțe care beneficiază de o constatare a caracterului adecvat al nivelului de protecție din partea Comisiei Europeană în temeiul Directivei 95/46/CE[8] asigură un nivel de protecție adecvat, deși Comisia Europeană va revizui în curând aceste constatări, iar concluziile acestei revizuiri nu sunt încă cunoscute.

17. **În ceea ce privește situațiile de mai sus, Comisia Europeană ar trebui să își îndeplinească rolul de monitorizare și, în cazul în care nu se menține nivelul în esență echivalent de protecție a datelor cu caracter personal transferate din SEE, Comisia Europeană ar trebui să aibă în vedere modificarea deciziei privind caracterul adecvat al nivelului de protecție în sensul introducerii unor garanții specifice pentru datele transferate din SEE și/sau în sensul suspendării deciziei privind caracterul adecvat al nivelului de protecție.**

18. **Referitor la acordurile internaționale încheiate între Regatul Unit și țări terțe,** Comisia Europeană este invitată să examineze interacțiunea dintre cadrul de protecție a datelor din Regatul Unit și angajamentele sale internaționale dincolo de Acordul între Guvernul Regatului Unit al Marii Britanii și Irlandei de Nord și Guvernul Statelor Unit ale Americii (denumite în continuare „SUA") privind

[7] „Orice date cu caracter personal care fac obiectul prelucrării sau care urmează a fi prelucrate după ce sunt transferate într-o țară terță sau către o organizație internațională pot fi transferate doar dacă, sub rezerva celorlalte dispoziții ale prezentului regulament, condițiile prevăzute în prezentul capitol sunt respectate de operator și de persoana împuternicită de operator, inclusiv în ceea ce privește transferurile ulterioare de date cu caracter personal din țara terță sau de la organizația internațională către o altă țară terță sau către o altă organizație internațională. Toate dispozițiile din prezentul capitol se aplică pentru a se asigura că nivelul de protecție a persoanelor fizice garantat prin prezentul regulament nu este subminat".

[8] Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (JO L 281, 23.11.1995, p. 31).

accesul la datele electronice în scopul combaterii formelor grave de criminalitate[9] (denumit în continuare „Acordul în temeiul legii CLOUD dintre Regatul Unit și SUA"), în special pentru a asigura continuitatea nivelului de protecție în cazul în care datele cu caracter personal sunt transferate din UE în Regatul Unit în baza deciziei privind caracterul adecvat al nivelului de protecție referitoare la Regatul Unit și apoi transferate mai departe către alte țări terțe. Comisia Europeană este invitată, de asemenea, să monitorizeze în permanență și să ia măsuri, dacă este necesar, în cazul în care încheierea de acorduri internaționale între Regatul Unit și țări terțe riscă să submineze nivelul de protecție a datelor cu caracter personal asigurat în UE.

19. În plus, Comisia Europeană este invitată să monitorizeze dacă Acordul în temeiul legii CLOUD dintre Regatul Unit și SUA asigură garanții suplimentare adecvate, ținând seama de nivelul de sensibilitate al categoriilor de date în cauză și de faptul că singurele cerințe cu privire la transferul de probe electronice prevăd ca acesta să se realizeze direct de către furnizorii de servicii și nu între autorități, analizând, de asemenea, circumstanțele în care pot fi oferite garanții printr-o punere în aplicare corespunzătoare a Acordului-cadru UE-SUA adaptat[10].

20. În plus, CEPD observă că transferurile ulterioare se pot realiza, de asemenea, din Regatul Unit către o altă țară terță pe baza **instrumentelor de transfer în temeiul legislației aplicabile a Regatului Unit privind protecția datelor[11]**. În urma hotărârii *Schrems II*[12], CEPD invită Comisia Europeană să ofere asigurări în decizia privind caracterul adecvat al nivelului de protecție că garanțiile necesare vor fi puse efectiv în aplicare, ținând seama, de asemenea, de legislația țării terțe destinatare.

21. În ceea ce privește absența din legislația Regatului Unit **a măsurilor de protecție prevăzute la articolul 48 din RGPD**, CEPD invită Comisia Europeană să furnizeze asigurări suplimentare și trimiteri specifice la legislația Regatului Unit care să asigure un nivel de protecție în temeiul cadrului juridic al Regatului Unit în esență echivalent cu nivelul de protecție garantat în SEE.

22. În ceea ce privește **mecanismele procedurale și de aplicare a legii,** CEPD constată că existența și funcționarea eficace a unei autorități de supraveghere independente, existența unui sistem care să asigure un bun nivel de conformitate și un sistem de acces la mecanisme adecvate de recurs care să ofere persoanelor din SEE mijloacele necesare pentru a-și exercita drepturile și pentru a obține reparații, fără a întâmpina dificultăți semnificative în ceea ce privește accesarea căilor de atac administrative și judiciare sunt elemente-cheie prin care trebuie să se caracterizeze un cadru de protecție a datelor coerent cu cel european.

23. CEPD recunoaște că Regatul Unit a reflectat în majoritatea cazurilor dispozițiile relevante ale RGPD în RGPD al Regatului Unit și în Legea privind protecția datelor din 2018; cu toate acestea, Comisia Europeană este invitată să monitorizeze în permanență orice evoluție a cadrului juridic și a practicii din Regatul Unit, care ar putea avea efecte negative asupra acestor domenii.

---

[9] A se vedea Acordul între Guvernul Regatului Unit al Marii Britanii și Irlandei de Nord și Guvernul Statelor Unite ale Americii privind accesul la datele electronice în scopul combaterii formelor grave de criminalitate, Washington DC, SUA, 3 octombrie 2019, https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019.

[10] A se vedea Acordul între Statele Unite ale Americii și Uniunea Europeană privind protecția informațiilor cu caracter personal în ceea ce privește prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor, decembrie 2016 (denumit în continuare „Acordul-cadru UE-SUA"), https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=LEGISSUM%3A3104_8.

[11] A se vedea articolele 46 și 47 din RGPD al Regatului Unit.

[12] A se vedea hotărârea *Schrems II*.

1.2.3. Aspecte referitoare la accesul autorităților publice la datele transferate în Regatul Unit

24. CEPD ia act de modificările semnificative ale cadrului juridic din Regatul Unit aplicabil serviciilor de securitate și de informații, în special în ceea ce privește interceptarea și obținerea datelor de comunicații. CEPD înțelege că modificările în cauză reprezintă, printre altele, un răspuns la procedurile inițiate în fața CJUE și a Curții Europene a Drepturilor Omului (denumită în continuare „CEDO"), precum și la hotărârile pronunțate recent de acestea în contextul respectiv.

25. În special, CEPD salută faptul că Regatul Unit a instituit Investigatory Powers Tribunal (Tribunalul competențelor de investigare) (denumit în continuare „IPT"). IPT are competența nu numai de a audia cauze privind utilizarea competențelor de investigare de către autoritățile de aplicare a legii, ci și cauze care vizează utilizarea acestora de către serviciile de informații. Prin urmare, CEPD consideră că IPT funcționează ca o instanță adecvată în sensul articolului 47 din Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „Carta UE").

26. În plus, CEPD ia act cu satisfacție de introducerea „comisarilor judiciari" în Legea privind competențele de investigare din 2016 (denumită în continuare „IPA 2016"), pe care o consideră o îmbunătățire semnificativă. Acesta înțelege că o funcție importantă a comisarilor judiciari este de a aproba *ex ante*, în cazuri individuale, diferite măsuri de supraveghere, inclusiv interceptarea specifică și obținerea în masă a datelor de comunicații (așa-numita procedură de „protecție dublă").

27. Cu toate acestea, pentru a evalua eficacitatea acestui nivel suplimentar de supraveghere, CEPD consideră că este necesar să se precizeze scenariile în care este posibilă o interceptare legală fără aprobarea comisarului pentru utilizarea competențelor de investigare (denumit în continuare „IPC") sau a comisarilor judiciari și invită Comisia Europeană să evalueze în continuare și să demonstreze că, chiar și în cazurile în care nu se aplică procedura de protecție dublă, cadrul juridic din Regatul Unit oferă garanții adecvate, inclusiv prin intermediul unei supravegheri *ex post* și al unor căi de atac eficace aflate la dispoziția persoanelor, asigurând astfel un nivel de protecție în esență echivalent cu cel oferit la nivelul UE.

28. În plus, CEPD invită Comisia Europeană să evalueze în continuare condițiile în care poate fi invocată urgența și să ofere clarificări cu privire la posibilele căi de exercitare a drepturilor persoanelor vizate în cauză și la posibilele căi de atac care le sunt oferite acestora în contextul operațiunilor de intervenție asupra echipamentelor, în special în cazul unei derogări de la procedura de protecție dublă.

29. Mai mult, CEPD consideră că este nevoie de clarificări și evaluări suplimentare ale interceptărilor în masă, în special în ceea ce privește selecția și aplicarea selectorilor, pentru a clarifica măsura în care accesul la datele cu caracter personal respectă pragul stabilit de CJUE și ce garanții sunt instituite pentru a proteja drepturile fundamentale ale persoanelor ale căror date sunt interceptate în acest context, inclusiv în ceea ce privește perioadele de păstrare a datelor. O evaluare independentă din partea autorităților de supraveghere competente din Regatul Unit ar fi deosebit de utilă. CEPD subliniază, de asemenea, că este cu atât mai important faptul că termenul de „comunicații transmise din/primite în străinătate" care intră în domeniul de aplicare al practicilor de interceptare în masă pare să sugereze că datele ar putea fi interceptate în mod direct și colectate în masă în UE de către Regatul Unit, inclusiv în ceea ce privește datele în tranzit între UE și Regatul Unit, care ar intra în domeniul de aplicare al proiectului de decizie. Având în vedere importanța acestui aspect, CEPD solicită Comisiei Europene să monitorizeze îndeaproape evoluțiile în acest sens.

30. Tot în ceea ce privește interceptarea în masă, CEPD subliniază consecvența aprecierii CEDO și CJUE în această privință și reamintește preocupările exprimate în legătură cu datele secundare, care ar trebui să beneficieze de garanții specifice datorită sensibilității lor. Prin urmare, CEPD solicită Comisiei Europene să evalueze cu atenție dacă garanțiile prevăzute de legislația Regatului Unit pentru o astfel de categorie de date cu caracter personal asigură un nivel de protecție în esență echivalent cu cel garantat în SEE.

31. În acest context, CEPD este conștient de faptul că raportul public din 2016 al Comitetului pentru informații și securitate privind utilizarea competențelor de interceptare în masă[13] se referă la practici din cadrul juridic anterior, care a fost înlocuit ulterior de IPA 2016. Cu toate acestea, CEPD consideră că este nevoie de o evaluare și o supraveghere independentă suplimentară a utilizării instrumentelor de prelucrare automată a datelor de către autoritățile de supraveghere competente din Regatul Unit și invită Comisia Europeană să evalueze în continuare acest aspect, precum și garanțiile care ar fi acordate și/sau care ar putea fi acordate persoanelor vizate din SEE în acest context.

32. CEPD împărtășește părerea exprimată de IPC, respectiv că sunt necesare revizuiri și monitorizări suplimentare pentru a se asigura că garanțiile aplicate în practică de autoritățile competente în domeniul securității naționale și al informațiilor pentru a remedia neconformitățile cu aplicarea legislației relevante sunt menținute și vor continua să fie îmbunătățite. De asemenea, CEPD salută faptul că, în consecință, IPC a efectuat o revizuire a abordării sale privind verificarea practicilor de interceptare în masă în 2019, „care a inclus o revizuire atentă a modalităților complexe din punct de vedere tehnic de punere efectivă în aplicare a interceptării în masă” și s-a angajat să includă „o examinare detaliată a selectorilor și a criteriilor de căutare menționate de CEDO și la care se face referire în cele de mai sus” în verificările practicilor de interceptare în masă începând cu 2020. Având în vedere importanța acestui aspect, CEPD își exprimă îngrijorarea cu privire la faptul că IPC nu a efectuat încă o examinare detaliată a selectorilor și a criteriilor de căutare și invită Comisia Europeană să monitorizeze îndeaproape evoluțiile în acest sens, în special având în vedere că formatul concret al unei astfel de supravegheri nu a fost clarificat încă.

33. CEPD subliniază că, în ceea ce privește divulgările de informații în străinătate, aplicarea derogării în materie de securitate națională prevăzută de legislația Regatului Unit poate duce la absența unor garanții prin care să se asigure respectarea principiilor limitării scopului, necesității și proporționalității sau să se prevadă acordarea sau respectarea drepturilor persoanelor, a mecanismelor de supraveghere și de recurs într-o măsură suficientă și în țara terță de destinație. Prin urmare, CEPD recomandă Comisiei Europene să examineze în continuare garanțiile generale prevăzute de legislația Regatului Unit în ceea ce privește divulgarea de informații în străinătate, în special având în vedere aplicarea derogărilor în materie de securitate națională.

34. În cele din urmă, CEPD își exprimă îngrijorarea cu privire la alte forme de schimb și de divulgare de informații, pe baza altor instrumente, în special a diferitelor acorduri internaționale încheiate de Regatul Unit cu alte țări terțe, mai ales în cazul în care aceste instrumente rămân inaccesibile publicului, cum este cazul Acordului privind serviciile de informații în domeniul comunicațiilor

[13] A se vedea raportul intitulat „Report of the bulk powers review” (Raport în urma evaluării competențelor de interceptare în masă), realizat de evaluatorul independent al legislației privind terorismul, august 2016, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf.

dintre Regatul Unit și SUA. Efectul unui astfel de acord ar putea duce la o eludare a garanțiilor identificate în ceea ce privește accesul la datele cu caracter personal și utilizarea acestora în scopuri de securitate națională. CEPD consideră că încheierea de acorduri bilaterale sau multilaterale cu țări terțe în scopul cooperării în domeniul serviciilor de informații, prin care se asigură un temei juridic pentru interceptarea și obținerea directă de date cu caracter personal sau pentru transferul de date cu caracter personal către aceste țări, poate afecta, de asemenea, în mod semnificativ condițiile de utilizare ulterioară a informațiilor colectate, întrucât astfel de acorduri pot afecta cadrul juridic privind protecția datelor din Regatul Unit, astfel cum a fost acesta evaluat.

1.3. Concluzie

35. CEPD consideră că evaluarea caracterului adecvat al nivelului de protecție asigurat în Regatul Unit este unică, având în vedere statutul anterior al Regatului Unit de stat membru al UE. În plus, aceasta ar fi, de asemenea, prima decizie privind caracterul adecvat al nivelului de protecție care ar include o clauză de încetare de drept a efectelor juridice.

36. În consecință, CEPD recunoaște numeroase domenii de convergență între cadrul de protecție a datelor din Regatul Unit și cel al UE. Cu toate acestea, în același timp și în urma unei analize atente a proiectului de decizie a Comisiei Europene și a legislației Regatului Unit privind protecția datelor, CEPD a identificat o serie de provocări, care sunt examinate pe larg în prezentul aviz. În acest context, CEPD dorește să sublinieze rolul esențial al Comisiei Europene în monitorizarea tuturor evoluțiilor relevante din Regatul Unit.

37. Având în vedere cele de mai sus, CEPD recomandă Comisiei Europene să abordeze provocările menționate în prezentul aviz. De asemenea, CEPD invită Comisia Europeană să monitorizeze îndeaproape toate evoluțiile relevante din Regatul Unit care ar putea avea un impact asupra echivalenței în esență a nivelului de protecție a datelor cu caracter personal și să ia rapid măsurile adecvate, dacă este necesar.

2. INTRODUCERE

2.1. Cadrul de protecție a datelor din Regatul Unit

38. Cadrul de protecție a datelor din Regatul Unit se bazează în mare parte pe cadrul UE privind protecția datelor (în special RGPD și LED), situație care rezultă din faptul că Regatul Unit a fost stat membru al UE până la 31 ianuarie 2020. În plus, pe lângă faptul că transpune Directiva UE privind protecția datelor în materie de aplicare a legii, conferă competențe autorității naționale de supraveghere a protecției datelor și impune obligații în sarcina acesteia, și anume ICO din Regatul Unit, Legea Regatului Unit privind protecția datelor din 2018, care a intrat în vigoare la 23 mai 2018 și a abrogat Legea Regatului Unit privind protecția datelor din 1998, descrie în detaliu aplicarea RGPD în dreptul Regatului Unit.

39. Astfel cum se menționează în considerentul 12 din proiectul de decizie a Comisiei Europene, Guvernul Regatului Unit a adoptat Legea din 2018 privind Uniunea Europeană (retragere), care încorporează legislația UE direct aplicabilă în dreptul Regatului Unit. În temeiul legii menționate, miniștrii Regatului Unit au competența de a introduce legislație secundară, prin intermediul instrumentelor statutare, pentru a aduce modificările necesare dreptului Uniunii menținut în dreptul intern în urma retragerii Regatului Unit din UE, astfel încât această legislație să corespundă contextului național.

40. În consecință, cadrul juridic relevant aplicabil în Regatul Unit după încheierea perioadei de tranziție[14] constă în:

- Regulamentul general privind protecția datelor al Regatului Unit (denumit în continuare „RGPD al Regatului Unit"), astfel cum a fost încorporat în dreptul Regatului Unit în temeiul Legii din 2018 privind Uniunea Europeană (retragere) și modificat prin Regulamentele DPPEC din 2019 [protecția datelor, a vieții private și a comunicațiilor electronice (modificare etc.) (ieșirea din UE)];
- Legea privind protecția datelor din 2018 (denumită în continuare „DPA 2018"), astfel cum a fost modificată prin Regulamentele DPPEC din 2019 și Regulamentele DPPEC din 2020 privind protecția datelor, a vieții private și a comunicațiilor electronice (modificări etc.) (ieșirea din UE); și
- IPA 2016.

(denumite împreună „cadrul de protecție a datelor din Regatul Unit").

2.2. Domeniul de aplicare al evaluării CEPD

41. Proiectul de decizie a Comisiei Europene este rezultatul unei evaluări a cadrului de protecție a datelor din Regatul Unit, urmate de discuții purtate cu Guvernul Regatului Unit. În conformitate cu articolul 70 alineatul (1) litera (s) din RGPD, se așteaptă ca CEPD să prezinte un aviz independent cu privire la constatările Comisiei Europene, să identifice deficiențele cadrului de adecvare, dacă este cazul, și să depună eforturi de formulare a unor propuneri pentru abordarea acestora.

42. Astfel cum se menționează în Criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD, „informațiile furnizate de Comisia Europeană ar trebui să fie exhaustive și să acorde CEPD posibilitatea de a efectua o evaluare proprie în ceea ce privește nivelul de protecție a datelor în țara terță"[15].

43. În acest sens, trebuie remarcat faptul că CEPD a primit numai o parte dintre documentele relevante pentru examinarea la timp a cadrului juridic din Regatul Unit. CEPD a primit cea mai mare parte a legislației Regatului Unit menționată în proiectul de decizie sub formă de linkuri inserate în acesta din urmă. Comisia Europeană nu a fost în măsură să furnizeze CEPD explicații și angajamente scrise din partea Regatului Unit în ceea ce privește schimburile de date care prezintă relevanță pentru acest exercițiu, realizate între autoritățile Regatului Unit și Comisia Europeană[16].

---

[14] Perioada de tranziție se încheie la 31 decembrie 2020, dată după care dreptul UE nu se mai aplică în Regatul Unit. „Perioada de grație" (perioada „bridge") se încheie la 30 iunie 2021 cel târziu și se referă la perioada suplimentară în care transmiterea datelor cu caracter personal din SEE către Regatul Unit nu este considerată transfer.

[15] A se vedea WP 254 rev.01, p. 3.

[16] În ceea ce privește: articolul 48 din RGPD (nota de subsol 78 din proiectul de decizie); garanții și măsuri de securitate sporite aplicate de operatori atunci când prelucrează date în contextul securității naționale (nota de subsol 64 din proiectul de decizie); cerința ca operatorul să analizeze dacă este necesar să apeleze la derogare de la caz la caz, chiar și în cazul în care a fost emis un certificat de securitate națională (considerentul 126 și nota de subsol 172 din proiectul de decizie); faptul că măsurile de protecție conferite în temeiul Acordului-cadru UE-SUA se vor aplica tuturor informațiilor cu caracter personal produse sau păstrate în conformitate cu Acordul în temeiul legii CLOUD dintre Regatul Unit și SUA, indiferent de natura sau de tipul de organism care formulează cererea, în ceea ce privește detaliile punerii în aplicare concrete a garanțiilor privind protecția datelor care fac încă obiectul discuțiilor dintre Regatul Unit și SUA, confirmarea faptului că

44. Ținând seama de cele de mai sus și având în vedere intervalul de timp limitat (două luni) în care CEPD trebuie să adopte acest aviz, CEPD a ales să se concentreze asupra unor puncte specifice prezentate în proiectul de decizie și să își prezinte analiza și avizul asupra acestora.

45. Întrucât procesul de analiză a vizat legislația și practicile unei țări terțe care a fost până de curând stat membru al UE, este evident că CEPD a identificat numeroase aspecte ca fiind în esență echivalente. Având în vedere rolul care îi revine în procesul de adoptare a unei constatări cu privire la caracterul adecvat al nivelului de protecție, precum și volumul de legi și practici care trebuie analizate, CEPD a decis să își concentreze atenția asupra acelor aspecte cu privire la care a considerat că se impune o analiză mai atentă. În plus, în conformitate cu jurisprudența CJUE, o parte foarte importantă a analizei acoperă regimul juridic al accesului în contextul securității naționale la datele cu caracter personal transferate în Regatul Unit și practica aparatului de securitate națională din Regatul Unit. Cu toate acestea, trebuie să se țină seama de faptul că securitatea națională este în mod evident un domeniu de drept și de practică în care legislația statelor membre nu este armonizată la nivelul UE și, prin urmare, poate fi diferită.

46. CEPD a luat în considerare cadrul european de protecție a datelor aplicabil, inclusiv articolele 7, 8 și 47 din Carta UE, și anume protejarea dreptului la viață privată 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 articolul 8 din Convenția pentru apărarea drepturilor omului și a libertăților fundamentale (denumită în continuare „Convenția europeană a drepturilor omului") care prevede protejarea dreptului la viață privată și de familie. În plus față de cele de mai sus, CEPD a luat în considerare cerințele RGPD, precum și jurisprudența relevantă.

47. Obiectivul acestui exercițiu este de a oferi Comisiei Europene un aviz pentru evaluarea caracterului adecvat al nivelului de protecție din Regatul Unit. Acest concept de „nivel de protecție adecvat", care era deja prevăzut în temeiul Directivei 95/46/CE, a fost dezvoltat în continuare de CJUE. Este important de reamintit standardul stabilit de CJUE în *cauza Schrems I*, și anume 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"[17]. 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 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

---

autoritățile Regatului Unit vor permite intrarea în vigoare a acordului respectiv numai după ce se asigură că punerea sa în aplicare respectă obligațiile juridice prevăzute în acesta, inclusiv claritatea cu privire la respectarea standardelor de protecție a datelor în legătură cu orice date solicitate în baza acordului respectiv (considerentul 153 din proiectul de decizie); situațiile în care datele sunt transferate din UE în Regatul Unit în cadrul domeniului de aplicare al acestui proiect de decizie și faptul că ar exista întotdeauna o „conexiune cu Insulele Britanice" și orice intervenție asupra echipamentelor care acoperă astfel de date ar face, prin urmare, obiectul cerinței privind mandatul obligatoriu de la secțiunea 13 alineatul (1) din IPA 2016 (considerentul 206 din proiectul de decizie); și exemplele de scopuri operaționale furnizate (considerentul 216 și nota de subsol 369 din proiectul de decizie).

[17] A se vedea CJUE, C-362/14, *Maximilian Schrems/Data Protection Commissioner*, 6 octombrie 2015, ECLI:EU:C:2015:650 (denumită în continuare „hotărârea Schrems I"), punctele 73-74.

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[18].

2.3. Observații și preocupări de natură generală

2.3.1. Angajamente internaționale la care a aderat Regatul Unit

48. 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[19], atunci când evaluează caracterul adecvat al nivelului de protecție asigurat de o țară terță, Comisia Europeană 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. În plus, ar trebui să se țină seama de aderarea țării terțe respective la Convenția Consiliului Europei din 28 ianuarie 1981 pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (denumită în continuare „Convenția 108”)[20] și la protocolul adițional[21] la aceasta.

49. **În acest sens, CEPD salută faptul că Regatul Unit a aderat la Convenția europeană a drepturilor omului și se află sub jurisdicția CEDO. În plus, Regatul Unit a aderat, de asemenea, la „Convenția 108” și la protocolul adițional la aceasta, a semnat „Convenția 108+”[22] în 2018 și lucrează în prezent la ratificarea acesteia.**

2.3.2. Posibila divergență viitoare a cadrului de protecție a datelor din Regatul Unit

50. Astfel cum se menționează în considerentul 281 din proiectul de decizie, Comisia Europeană trebuie să țină seama de faptul că, odată cu încheierea perioadei de tranziție prevăzute în Acordul de retragere[23], Regatul Unit administrează, aplică și asigură respectarea propriului regim de protecție a datelor și, de îndată ce dispoziția provizorie (dispoziția „bridge”) prevăzută la articolul FINPROV.10A din Acordul comercial și de cooperare UE-Regatul Unit[24] încetează să se aplice, acest lucru poate implica, în special, modificări ale cadrului de protecție a datelor evaluat în proiectul de decizie, precum și alte evoluții relevante.

[18] A se vedea WP 254 rev.01, p. 2.
[19] A se vedea WP 254 rev.01, p. 2.
[20] A se vedea Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, „Convenția 108”, 28 ianuarie 1981.
[21] A se vedea Protocolul adițional la Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, cu privire la autoritățile de control și fluxul transfrontalier al datelor, deschis spre semnare la 8 noiembrie 2001.
[22] A se vedea Protocolul de modificare a Convenției pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (denumit în continuare „Convenția 108+”), 18 mai 2018.
[23] A se vedea Acordul privind retragerea Regatului Unit al Marii Britanii și Irlandei de Nord din Uniunea Europeană și din Comunitatea Europeană a Energiei Atomice (JO L 029, 31.1.2020, p. 7).
[24] A se vedea Acordul comercial și de cooperare între Uniunea Europeană și Comunitatea Europeană a Energiei Atomice, pe de o parte, și Regatul Unit al Marii Britanii și Irlandei de Nord, pe de altă parte (JO L 444, 31.12.2020, p. 14).

51. Prin urmare, Comisia Europeană a decis să includă o clauză de încetare de drept a efectelor juridice în proiectul său de decizie[25], stabilind data expirării la patru ani de la intrarea în vigoare a deciziei.

52. Este important de remarcat faptul că posibilitatea miniștrilor Regatului Unit și a secretarului de stat al Regatului Unit de a introduce legislație secundară după încheierea perioadei de grație poate conduce, în viitor, la o divergență semnificativă a cadrului de protecție a datelor din Regatul Unit față de cadrul de protecție a datelor din UE.

53. Într-adevăr, Guvernul Regatului Unit și-a exprimat intenția de a elabora politici separate și independente în domeniul protecției datelor, care pot conduce ulterior la divergențe față de legislația europeană privind protecția datelor[26]. Această intenție vizează includerea aspectelor legate de datele cu caracter personal în acordurile comerciale[27], ceea ce implică riscul reducerii nivelului de protecție a datelor cu caracter personal asigurat de Regatul Unit[28].

54. În cele din urmă, nu numai de la încheierea perioadei de tranziție, jurisprudența CJUE nu mai este obligatorie pentru Regatul Unit, iar hotărârile deja adoptate ale CJUE, considerate jurisprudență reținută în cadrul juridic al Regatului Unit, ar putea să nu mai fie obligatorii pentru Regatul Unit, deoarece, în special, Regatul Unit are posibilitatea de a modifica dreptul Uniunii menținut în

---

[25] A se vedea articolul 4 din proiectul de decizie. A se vedea, de asemenea, considerentul 282 din proiectul de decizie.

[26] Strategia națională a Regatului Unit privind datele (actualizată ultima dată la 9 decembrie 2020, https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy) include următoarele aspecte în cadrul misiunilor sale: „Promovarea fluxului internațional de date. Fluxul transfrontalier de informații alimentează operațiunile comerciale, lanțurile de aprovizionare și comerțul la nivel mondial, stimulând creșterea economică în întreaga lume. Acesta are, de asemenea, un rol mai amplu în societate. Transferul datelor cu caracter personal garantează plata salariilor și contribuie la păstrarea contactului cu cei dragi de la distanță. În plus, astfel cum a demonstrat pandemia de COVID-19, schimbul de date privind sănătatea poate contribui la cercetarea științifică vitală în domeniul bolilor, reprezentând în același timp un factor unificator al răspunsului statelor la urgențele sanitare globale. **După ce a părăsit Uniunea Europeană, Regatul Unit va promova beneficiile pe care le pot oferi datele.** Vom promova cele mai bune practici pe plan intern și vom colabora cu partenerii internaționali **pentru a ne asigura că datele nu sunt limitate în mod necorespunzător de frontierele naționale și de regimuri de reglementare fragmentate**, astfel încât acestea să poată fi utilizate la întregul lor potențial” (subliniere adăugată).

[27] Ibidem: „Facilitarea fluxurilor transfrontaliere de date: **Vom depune eforturi la nivel mondial pentru a elimina barierele inutile din calea fluxurilor internaționale de date. Vom conveni asupra unor dispoziții ambițioase privind datele în cadrul negocierilor noastre comerciale** și vom utiliza noua noastră poziție independentă în cadrul Organizației Mondiale a Comerțului pentru a influența pozitiv normele comerciale privind datele. **Vom elimina obstacolele din calea transferurilor internaționale de date**, care sprijină creșterea și inovarea, inclusiv prin dezvoltarea unei noi capacități a Regatului Unit care să ofere mecanisme noi și inovatoare pentru transferurile internaționale de date. Vom colabora, de asemenea, cu parteneri din cadrul G20 pentru a crea interoperabilitate între regimurile naționale de date în vederea reducerii la minimum a fricțiunilor în momentul transferului de date între diferite țări” (subliniere adăugată).

[28] A se vedea Rezoluția Parlamentului European din 12 decembrie 2017 „Către o strategie în domeniul comerțului digital” [2017/2065(INI)], secțiunea V, în care se subliniază că „protecția datelor cu caracter personal nu este negociabilă în cadrul acordurilor comerciale [ale UE]”, disponibilă la adresa: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0488_RO.pdf. A se vedea, de asemenea, Rezoluția Parlamentului European din 25 martie 2021 referitoare la raportul de evaluare al Comisiei privind punerea în aplicare a Regulamentului general privind protecția datelor, la doi ani de la aplicarea acestuia, punctul 28, în care se afirmă următoarele: „sprijină practica Comisiei Europene de a trata protecția datelor și fluxurile de date cu caracter personal separat de acordurile comerciale”, https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_RO.html.

dreptul intern după încheierea perioadei de grație și Curtea Supremă a Regatului Unit nu se mai supune jurisprudenței UE reținute în jurisprudența internă[29].

55. **Având în vedere riscurile legate de posibila abatere a cadrului de protecție a datelor din Regatul Unit de la acquis-ul UE după încheierea perioadei de grație, CEPD salută decizia Comisiei Europene de a introduce în proiectul de decizie o clauză de încetare de drept a efectelor juridice cu un termen de patru ani. Cu toate acestea, CEPD ar dori să sublinieze în acest context importanța rolului de monitorizare al Comisiei Europene[30]. Într-adevăr, Comisia Europeană ar trebui să monitorizeze toate evoluțiile relevante din Regatul Unit care ar putea avea un impact asupra echivalenței în esență a nivelului de protecție a datelor cu caracter personal transferate în temeiul deciziei privind caracterul adecvat al nivelului de protecție referitoare la Regatul Unit, în mod continuu și permanent, de la intrarea în vigoare a acestei decizii. În plus, Comisia Europeană ar trebui să ia măsuri corespunzătoare prin suspendarea, modificarea sau abrogarea deciziei privind caracterul adecvat al nivelului de protecție, în funcție de circumstanțele specifice, în cazul în care, după adoptarea deciziei privind caracterul adecvat al nivelului de protecție, Comisia Europeană are indicii că în Regatul Unit nu se mai asigură un nivel de protecție adecvat.**

56. La rândul său, CEPD va depune toate eforturile pentru a informa Comisia Europeană cu privire la orice acțiune relevantă întreprinsă de autoritățile de supraveghere a protecției datelor (denumite în continuare „AS") din statele membre în sectorul comercial sau în cel privat, în special cu privire la plângerile formulate de persoanele vizate din SEE în legătură cu transferul datelor cu caracter personal din SEE către Regatul Unit.

3. ASPECTE GENERALE PRIVIND PROTECȚIA DATELOR

3.1. Principii referitoare la conținut

57. Capitolul 3 din Criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD este dedicat principiilor referitoare la conținut. Sistemul unei țări terțe trebuie să conțină aceste principii pentru ca nivelul său de protecție a datelor să fie considerat în esență echivalent cu cel garantat în UE. CEPD recunoaște faptul că Regatul Unit nu are o constituție codificată, respectiv că nu există niciun document unic care să stabilească normele sale fundamentale de reglementare. Cu toate acestea, dreptul la respectarea vieții private și de familie (și dreptul la protecția datelor ca parte a acestui drept), precum și dreptul la un proces echitabil[31] sunt incluse în Legea privind drepturile omului din 1998, iar valoarea constituțională a acestui statut a fost recunoscută de instanțele din Regatul Unit. Într-adevăr, Legea privind drepturile omului din 1998 încorporează drepturile prevăzute în Convenția europeană a drepturilor omului[32]. În plus, Legea privind drepturile omului din 1998 include o dispoziție foarte importantă, și anume că orice acțiune a autorităților publice trebuie să fie compatibilă cu Convenția europeană a drepturilor omului[33].

58. Lăsând la o parte diferențele structurale și de formă dintre legislația Regatului Unit și cea a UE, CEPD observă, după cum este de așteptat, că abordarea Regatului Unit în materie de protecție a

[29] A se vedea articolul 6 alineatele (3)-(6) din Legea din 2018 privind Uniunea Europeană (retragere).
[30] A se vedea articolul 45 alineatul (4) din RGPD.
[31] A se vedea articolele 6 și 8 din Convenția europeană a drepturilor omului (anexa 1 la Legea privind drepturile omului din 1998).
[32] Pentru mai multe informații, a se vedea considerentele 8-10 din proiectul de decizie.
[33] A se vedea articolul 6 din Legea privind drepturile omului din 1998.

datelor este similară cu cea din UE, ca urmare a faptului că Regatul Unit a fost stat membru al UE până la 31 ianuarie 2020. Prin urmare, numeroase principii referitoare la conținut sunt aliniate la principiile RGPD și, astfel, asigură un nivel de protecție în esență echivalent cu cel oferit de UE. CEPD a decis să nu dezvolte în continuare analiza cu privire la acele principii referitoare la conținut care sunt aliniate la legislația UE și este satisfăcut de analiza furnizată de Comisia Europeană în proiectul său de decizie. Astfel de principii referitoare la conținut includ, de exemplu, următoarele: concepte (de exemplu, „date cu caracter personal"; „prelucrarea datelor cu caracter personal"; „operator"); motive care justifică prelucrarea legală și echitabilă în scopuri legitime; limitarea scopului; calitatea și proporționalitatea datelor; păstrarea, securitatea și confidențialitatea datelor; transparența; categoriile speciale de date; marketingul direct; procesul decizional automatizat și crearea de profiluri. CEPD ia act, de asemenea, de faptul că RGPD al Regatului Unit și DPA 2018 includ principii referitoare la conținut care depășesc ceea ce este necesar potrivit criteriilor de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD și reflectă principiile incluse în RGPD, asigurând astfel un nivel mai ridicat de protecție în Regatul Unit. Astfel de principii referitoare la conținut sunt, de exemplu, cele legate de notificările privind încălcarea securității datelor cu caracter personal, responsabilul cu protecția datelor, evaluările impactului asupra protecției datelor, protecția datelor începând cu momentul conceperii și protecția implicită a datelor.

59. Cu toate acestea, astfel cum s-a menționat în introducere, CEPD dorește să abordeze în mod specific în prezentul aviz anumite puncte cu privire la care CEPD își exprimă îngrijorarea și ar dori să solicite clarificări din partea Comisiei Europene.

3.1.1. Dreptul de acces, la rectificare, la ștergere și la opoziție

60. Așa-numita „derogare privind imigrația", prevăzută în **anexa 2 la DPA 2018, partea 1**, punctul 4 permite operatorilor implicați în „controlul imigrației" să nu aplice anumite drepturi ale persoanelor vizate prevăzute de DPA 2018 în cazul în care acest lucru ar putea „prejudicia menținerea unui control eficace al imigrației" sau „investigarea sau detectarea activităților care ar submina menținerea unui control eficace al imigrației".

61. Astfel cum a recunoscut Comisia Europeană în proiectul său de decizie[34] și cum s-a menționat în avizul Comisiei pentru libertăți civile, justiție și afaceri interne a Parlamentului European referitor la încheierea, în numele Uniunii, a Acordului comercial și de cooperare UE-Regatul Unit[35], această derogare este formulată **„în sens larg"**. Derogarea se aplică următoarelor drepturi: dreptului de a fi

[34] A se vedea considerentele 62-65 din proiectul de decizie.

[35] În acest sens, în legătură cu **formularea în sens larg** a derogării privind imigrația, a se vedea Avizul Comisiei pentru libertăți civile, justiție și afaceri interne referitor la încheierea, în numele Uniunii, a Acordului comercial și de cooperare dintre Uniunea Europeană și Comunitatea Europeană a Energiei Atomice, pe de o parte, și Regatul Unit al Marii Britanii și Irlandei de Nord, pe de altă parte, și a Acordului dintre Uniunea Europeană și Regatul Unit al Marii Britanii și Irlandei de Nord privind procedurile de securitate pentru schimbul de informații clasificate și protecția acestora [2020/0382(NLE)], 5 februarie 2021, https://www.europarl.europa.eu/doceo/document/LIBE-AL-680848_RO.pdf, punctul 10: „reamintește, în acest sens, rezoluțiile Parlamentului din februarie și iunie 2020, care subliniază **excepția generală și extinsă** pentru prelucrarea datelor cu caracter personal în scopuri legate de imigrație prevăzută de Legea Regatului Unit privind protecția datelor" și punctul 11: „consideră că **excepția generală și extinsă** pentru prelucrarea datelor cu caracter personal în scopul imigrației prevăzută de Legea Regatului Unit privind protecția datelor [...] trebuie modificată înainte de a se putea lua o decizie valabilă privind adecvarea" (subliniere adăugată).

informat, dreptului de acces, dreptului la ștergerea datelor, dreptului la restricționarea prelucrării și dreptului la opoziție.

62. În plus, este important de remarcat faptul că această derogare se aplică și în cazul în care datele cu caracter personal nu sunt colectate în scopul controlului imigrației de către un operator („operatorul 1"), dar sunt totuși puse de acesta din urmă la dispoziția unui alt operator („operatorul 2"), care prelucrează astfel de date cu caracter personal în scopul controlului imigrației (de exemplu, Ministerul de Interne din Regatul Unit)[36].

63. În cauza *Open Rights Group și alții, R (în baza cererii înaintate de aceasta)/Secretary of State for the Home Department și alții, 2019, Înalta Curte de Justiție (EWHC) 2562 (secția de contencios administrativ) (3 octombrie 2019)*, reclamanții au contestat legalitatea derogării privind imigrația pe motiv că aceasta contravine articolului 23 din RGPD și este incompatibilă cu drepturile garantate de articolele 7 și 8 din Carta UE privind viața privată și protecția datelor cu caracter personal. Înalta Curte de Justiție (denumită în continuare „Înalta Curte") a examinat legalitatea derogării privind imigrația prevăzută la punctul 4 din partea 1 a anexei 2 la DPA 2018 și a concluzionat în favoarea legalității acesteia.

64. În special, Înalta Curte a apreciat că:

- „[...] derogarea privind imigrația este în mod clar o chestiune de «interes public important» și urmărește un scop legitim. [...]", punctul 30;
- „derogarea privind imigrația îndeplinește cerințele în baza cărora o măsură este considerată «în conformitate cu legea». […]", punctul 38;
- „Derogarea privind imigrația poate fi aplicată numai dacă și în măsura în care respectarea «dispozițiilor enumerate din RGPD» **ar putea prejudicia** menținerea unui control eficace al imigrației sau investigarea sau detectarea activităților care ar submina menținerea unui control eficace al imigrației. Cuvintele «ar putea prejudicia», în contextul Legii privind protecția datelor din 1998 (care a precedat DPA 2018), au fost interpretate ca însemnând

[36] A se vedea exemplul oferit în ghidul ICO intitulat „Guide to the General Data Protection Regulation (GDPR)" [Ghidul privind Regulamentul general privind protecția datelor (RGPD)], v. 1 ianuarie 2021, p. 307 (subliniere adăugată): „O organizație privată (operatorul 1) informează Ministerul de Interne (operatorul 2) cu privire la un angajat despre care se crede că a prezentat documente false pentru a-și dovedi identitatea și calificările în vederea obținerii unui loc de muncă. Angajatorul furnizează Ministerului de Interne informațiile relevante. Dreptul persoanei respective de a fi informată că datele sale cu caracter personal au fost transmise Ministerului de Interne este limitat în măsura în care punerea sa în aplicare ar putea prejudicia investigația.
Prin urmare, **angajatorul nu are obligația de a informa persoana respectivă că informațiile sale au fost transmise Ministerului de Interne** și, la rândul său, **Ministerul de Interne** nu are obligația de a-i transmite persoanei respective o declarație de confidențialitate prin care o informează că îi prelucrează datele cu caracter personal. Derogarea se aplică ambilor operatori în aceeași măsură.
Cu toate acestea, angajatul solicită o copie a datelor sale cu caracter personal de la Ministerul de Interne, care desfășoară investigația cu privire la acesta. **Ministerul de Interne se poate baza pe derogare** pentru a refuza divulgarea unei părți din datele acestuia în cazul în care aceasta ar putea prejudicia investigația. În cazul în care angajatul adresează o cerere similară **angajatorului său, acesta ar putea, de asemenea, să aplice derogarea** în aceeași măsură."
Cu alte cuvinte, astfel cum s-a clarificat la pagina 300: „În majoritatea cazurilor, Ministerul de Interne sau una dintre agențiile sale/unul dintre contractanții săi va fi operatorul care aplică această derogare. Cu toate acestea, este important de remarcat faptul că aplicarea acestei derogări nu se limitează doar la Ministerul de Interne. Aceasta poate fi, de asemenea, relevantă pentru alți operatori, cum ar fi angajatorii, universitățile și poliția, care colaborează cu Ministerul de Interne în materie de imigrație."

«există o șansă foarte semnificativă de prejudiciere a interesului public specific. Gradul de risc trebuie să fie de așa natură încât prejudicierea acestor interese «să fie foarte probabilă», chiar dacă riscul este departe de a fi mai degrabă probabil decât improbabil […]", punctul 39 (subliniere adăugată).

65. Trebuie remarcat faptul că, potrivit informațiilor deținute de CEPD, această hotărâre nu este definitivă și a făcut obiectul unui recurs.

66. Astfel cum se specifică în Orientările CEPD privind restricțiile în temeiul articolului 23 din RGPD (denumite în continuare „Orientările privind articolul 23 din RGPD")[37], „[...] în contextul RGPD, restricțiile sunt **prevăzute într-o măsură legislativă**, se referă la un **număr limitat de drepturi ale persoanelor vizate și/sau de obligații ale operatorului** enumerate la articolul 23 din RGPD, **respectă esența** drepturilor și a libertăților fundamentale în cauză, constituie o **măsură necesară și proporțională** într-o societate democratică și asigură unul dintre temeiurile prevăzute la articolul 23 alineatul (1) din RGPD [...]".[38]

67. CEPD reamintește, de asemenea, că, în considerentul 41 din RGPD, se prevede că „[o]ri de câte ori prezentul regulament face trimitere la **un temei juridic sau la o măsură legislativă**, aceasta nu necesită neapărat un act legislativ adoptat de către un parlament, fără a aduce atingere cerințelor care decurg din ordinea constituțională a statului membru în cauză. Cu toate acestea, un astfel de temei juridic sau o astfel de măsură legislativă ar trebui să fie **clară și precisă, iar aplicarea acesteia ar trebui să fie previzibilă pentru persoanele vizate de aceasta**, în conformitate cu jurisprudența Curții de Justiție a Uniunii Europene [...] și a Curții Europene a Drepturilor Omului" (subliniere adăugată).

68. Deși CEDO a precizat că „[î]n ceea ce privește termenul «prevăzut de lege», care figurează la articolele 8-11 din Convenție, [CEDO] observă că a înțeles întotdeauna termenul «lege» în sensul său «material» și nu în sensul său «formal»; acesta a inclus atât «legea scrisă», care cuprinde acte legislative de rang inferior, cât și măsuri de reglementare luate de organismele de reglementare profesionale în temeiul competențelor independente de reglementare care le-au fost delegate de parlament, precum și legi nescrise. Termenul de «lege» trebuie înțeles ca incluzând atât dreptul statutar, **cât și jurisprudența"**[39]. Orientările privind articolul 23 din RGPD reamintesc că „[p]otrivit jurisprudenței CJUE, orice **măsură legislativă** adoptată în temeiul articolului 23 alineatul (1) [din] RGPD trebuie să respecte, în special, **cerințele specifice prevăzute la articolul 23 alineatul (2) din RGPD**. Articolul 23 alineatul (2) [din] RGPD prevede că măsurile legislative care impun restricții asupra drepturilor persoanelor vizate și a obligațiilor operatorilor conțin, după caz, **dispoziții specifice în ceea ce privește o serie de criterii enumerate mai jos**. Ca regulă generală, toate cerințele detaliate mai jos **ar trebui să fie incluse în măsura legislativă** care impune restricții în temeiul articolului 23 [din] RGPD"[40].

---

[37] A se vedea Orientările CEPD 10/2020 privind restricțiile în temeiul articolului 23 din RGPD, versiunea 1.0, adoptate la 15 decembrie 2020, în curs de finalizare în urma procedurii de consultare publică, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-102020-restrictions-under-article-23_en.

[38] A se vedea Orientările privind articolul 23 din RGPD, punctul 9, p. 5.

[39] A se vedea CEDO, *Sanoma Uitgevers B.V./Țările de Jos*, 14 septembrie 2010, EC:ECHR:2010:0914JUD003822403, punctul 83 (subliniere adăugată).

[40] A se vedea Orientările privind articolul 23, punctele 45 și 46, p. 11. Potrivit articolului 52 alineatul (3) din Carta UE, „[î]n măsura în care prezenta cartă conține drepturi ce corespund unor drepturi garantate prin

69. În această privință, se poate observa că **derogarea privind imigrația nu specifică următoarele elemente menționate la articolul 23 alineatul (2) din RGPD**:

- „garanțiile pentru a preveni abuzurile sau accesul sau transferul ilegal” [litera (d)];
- „operatorul sau categoriile de operatori” [litera (e)][41];
- „riscurile pentru drepturile și libertăților persoanelor vizate” [litera (g)];
- „dreptul persoanelor vizate de a fi informate cu privire la restricție, cu excepția cazului în care acest lucru poate aduce atingere scopului restricției” [litera (h)].

70. Ghidul ICO intitulat „Guide to the General Data Protection Regulation (GDPR)” [Ghidul privind Regulamentul general privind protecția datelor (RGPD)][42], care include un capitol despre „derogarea privind imigrația”, nu prevede clarificări asupra acesteia, însă **nu poate** în sine să prevadă norme obligatorii care să vină în completarea sa. În plus, problema „calității legii” este deosebit de relevantă, având în vedere importanța drepturilor restricționate și extinderea derogării[43].

Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale, înțelesul și întinderea lor sunt aceleași ca și cele prevăzute de convenția menționată. Această dispoziție nu împiedică dreptul Uniunii să confere o protecție mai largă”. În ceea ce privește noțiunea „**prevăzut de lege**”, în temeiul articolului 52 alineatul (1) din Carta UE, ar trebui utilizate criteriile elaborate de CEDO, astfel cum s-a sugerat în mai multe concluzii ale avocatului general al CJUE (a se vedea, de exemplu, concluziile prezentate în cauzele conexate C-203/15 și C-698/15, *Tele2 Sverige AB*, ECLI:EU:C:2016:572, punctele 137-154 și în cauza C-70/10, *Scarlet Extended*, ECLI:EU:C:2011:255, punctele 88-114). Prin urmare, se poate face trimitere, printre altele, la hotărârea CEDO în cauza *Weber și Saravia/Germania*, punctul 84: „Curtea reiterează că expresia «**prevăzut de lege**» în înțelesul articolului 8 alineatul (2) [din Convenția europeană a drepturilor omului] impune, în primul rând, ca măsura contestată să fi avut vreun temei stabilit în conformitate cu **legislația internă**, referindu-se, de asemenea, la **calitatea legii** în cauză și impunând ca aceasta să fie accesibilă persoanei în cauză, care, în plus, trebuie să fie în măsură să prevadă consecințele acesteia pentru ea, precum și să fie compatibilă cu statul de drept.” (subliniere adăugată).
A se vedea, de asemenea, considerentul 41 din RGPD: „Cu toate acestea, [un astfel de temei juridic] sau o astfel de măsură legislativă ar trebui să fie **clară** și **precisă**, iar aplicarea acesteia ar trebui să fie **previzibilă pentru persoanele vizate** de aceasta, în conformitate cu jurisprudența Curții de Justiție a Uniunii Europene [...] și a Curții Europene a Drepturilor Omului” (subliniere adăugată).

[41] A se vedea cauza aflată pe rolul Înaltei Curți menționată anterior, punctul 54: „În opinia mea, nu există nicio neregularitate cu privire la faptul că derogarea privind imigrarea este disponibilă **pentru toți operatorii de date** care prelucrează date în scopurile specificate. Astfel cum subliniază pârâții, în absența alineatelor 4 punctele (3)-(4), derogarea privind imigrația ar fi lipsită de efect util în cazurile în care datele sunt obținute de la terți (cum ar fi o autoritate locală sau administrația fiscală și vamală a Regatului Unit) în scopul menținerii unui control eficace al imigrației” (subliniere adăugată), confirmându-se astfel aplicarea **generalizată** a restricțiilor.

[42] Ghidul ICO intitulat „Guide to the General Data Protection Regulation (GDPR)” [Ghidul privind Regulamentul general privind protecția datelor (RGPD)], v. 1 ianuarie 2021, p. 299-307.

[43] A se vedea punctul 57 din cauza aflată pe rolul Înaltei Curți menționată mai sus: „Dl Knight mă informează că, în ceea ce privește orientările privind derogarea, acestea sunt în curs de finalizare de către comisar, însă ele vor fi considerate exclusiv «statutare», în sensul că sunt emise în baza competențelor comisarului în temeiul articolului 57 alineatul (1) din RGPD. Acestea nu vor avea niciun statut juridic în conformitate cu *DPA 2018*.”
Justificarea introducerii unor orientări obligatorii din punct de vedere juridic susținute de ICO este menționată în special la punctele 56-60 din hotărâre:
„56. În sfârșit, vom aborda argumentul comisarului potrivit căruia, în absența unor orientări statutare care să o însoțească și care să ofere garanții cu privire la sensul și aplicarea derogării privind imigrația, derogarea nu

71. *A fortiori*, „testul prejudiciilor” nu prevede garanțiile pentru a preveni abuzurile sau accesul sau transferul ilegal, care să fie puse în aplicare, de exemplu, de Ministerul de Interne.

72. Având în vedere toate cele de mai sus, CEPD remarcă faptul că sunt necesare clarificări suplimentare cu privire la aplicarea derogării privind imigrația.

73. În plus, CEPD remarcă lipsa unui instrument obligatoriu din punct de vedere juridic care să clarifice derogarea privind imigrația pentru a analiza dacă aceasta este în esență echivalentă cu articolul 23 din RGPD și cu articolele 7 și 8 din Carta UE. În același timp, CEPD consideră că necesitatea și proporționalitatea domeniului larg de aplicare *ratione personae* al derogării privind imigrația trebuie să fie demonstrate în continuare de Comisia Europeană și susținute de probe.

---

ar reprezenta o punere în aplicare proporțională a articolului 23 alineatul (1) din RGPD. Dl Knight afirmă că dispoziția este proporțională, în cazul în care este completată de astfel de orientări.
57. Dl Knight mă informează că, în ceea ce privește orientările privind derogarea, acestea sunt în curs de finalizare de către comisar, însă ele vor fi considerate exclusiv «statutare», în sensul că sunt emise în baza competențelor comisarului în temeiul articolului 57 alineatul (1) din RGPD. Acestea nu vor avea niciun statut juridic în conformitate cu *DPA 2018*. Înțeleg, de asemenea, că Ministerul de Interne a elaborat un proiect de orientări interne pentru personal în legătură cu derogarea privind imigrația (a se vedea punctul 22 de mai sus). În practică, orientările emise de comisar au impact, indiferent de temeiul lor juridic. Cu toate acestea, comisarul nu deține competența de a emite orientări «obligatorii» de tipul celor avute în vedere de Curtea Supremă în *cauza Christian Institute* (la punctele 101 și 107). Se pare că legislația primară ar fi necesară în cazul în care s-ar considera necesar să existe orientări care să vizeze derogarea privind imigrația cu același statut precum codurile de practică prevăzute în prezent la *articolele 121-124 din DPA 2018*.
58. În argumentația sa privind orientările statutare, domnul Knight susține că respectivul context în care se înscrie utilizarea derogării privind imigrația vizează în mod necesar preocupările cu privire la necesitatea și proporționalitatea existenței și a utilizării sale. El atrage atenția asupra a două aspecte, în special în context juridic. În primul rând, datele cu caracter personal cărora li se aplică derogarea privind imigrația sunt în mod inerent susceptibile să implice date din categorii speciale în sensul articolului 9 alineatul (1) din RGPD (și anume date „care dezvăluie originea rasială sau etnică”). Astfel de date sunt identificate în RGPD deoarece necesită un nivel de protecție mai ridicat (*Avizul 1/15, 2019, 3 CMLR 25*, punctul 141). În al doilea rând, este o propunere de bază a legislației privind protecția datelor ca dreptul de acces al persoanelor vizate să fie deosebit de important în calitate de cale de acces la exercitarea celorlalte drepturi conferite persoanelor vizate [*a se vedea Hotărârea YS/Minister voor Immigratie, Integratie en Asiel, C-141/12, EU:C:2014:2081;, 2015, 1 CMLR 18 punctul 44).*
59. Dl Knight identifică patru aspecte de ordin practic. În primul rând, situația în care operatorii nu explică persoanelor vizate că s-au bazat pe o derogare statutară și nici nu furnizează un rezumat amplu al motivelor pentru care persoana vizată nu va fi informată cu privire la aplicarea derogării și nu va putea să o conteste în mod eficace în consecință. În al doilea rând, persoanele vizate vor depinde în special de operatori în ceea ce privește aplicarea cu atenție a derogării și numai în măsura în care este necesară. Deși orice persoană vizată are dreptul de a adresa o plângere comisarului cu privire la aplicarea derogării sau de a introduce o acțiune în justiție, este probabil ca persoana vizată să nu își cunoască drepturile și să nu dispună de fonduri pentru a lua măsuri legale, în cazul în care este necesară respectarea promptă și exactă a drepturilor de protecție a datelor. În al treilea rând, în calitate de imigrant, este probabil ca persoana vizată să se afle într-o situație vulnerabilă. În al patrulea rând, aceasta nu este o problemă abstractă, având în vedere probele prezentate de pârâți în legătură cu utilizarea derogării privind imigrația (a se vedea punctul 4 de mai sus).
60. Dl Knight sugerează că există o paralelă strânsă între prezenta contestație a derogării privind imigrația și motivarea Curții în cauza *Christian Institute, 2016, UKSC 51*. La fel ca în cauza *Christian Institute*, acesta susține că derogarea privind imigrația este largă, utilizează termeni care nu au fost definiți, aplică un prag scăzut, face obiectul unor controale care nu sunt evidente la prima vedere și se aplică unei game foarte largi de contexte și drepturi. Spre deosebire de cauza *Christian Institute*, nu există orientări publice disponibile, cu atât mai puțin orientări statutare de care să trebuiască să se țină seama, în legătură cu derogarea privind imigrația.”

74. **În concluzie, CEPD invită Comisia Europeană să verifice stadiul procedurilor în cauza *Open Rights Group și alții, R (în baza cererii înaintate de aceasta)/Secretary of State for the Home Department și alții, 2019, Înalta Curte de Justiție (EWHC) 2562 (secția de contencios administrativ)* menționată mai sus și, întrucât această hotărâre nu este definitivă (nu are autoritate de lucru judecat), să verifice dacă este confirmată sau revizuită prin hotărârea pronunțată în apel, ținând seama de orice actualizare în această privință și specificând-o în decizia privind caracterul adecvat al nivelului de protecție. CEPD solicită, de asemenea, Comisiei Europene să furnizeze informații suplimentare cu privire la necesitatea și proporționalitatea derogării privind imigrația, în special având în vedere domeniul larg de aplicare *ratione personae*.**

75. **În același timp, CEPD invită Comisia Europeană să analizeze în continuare dacă există garanții suplimentare în cadrul juridic din Regatul Unit sau dacă acestea ar putea fi avute în vedere, de exemplu, prin intermediul unor instrumente obligatorii din punct de vedere juridic care ar completa derogarea privind imigrația, sporind previzibilitatea acesteia și garanțiile pentru persoanele vizate și permițând, de asemenea, o evaluare și o monitorizare mai bună și promptă a cerințelor privind necesitatea și proporționalitatea.**

3.1.2. Restricții privind transferurile ulterioare de date

76. Articolul 44 din RGPD prevede că transferurile și transferurile ulterioare de date cu caracter personal au loc doar dacă nivelul de protecție a persoanelor fizice garantat de RGPD nu este subminat. Prin urmare, datele cu caracter personal transferate din SEE în Regatul Unit pe baza deciziei privind caracterul adecvat al nivelului de protecție beneficiază de un nivel de protecție în esență echivalent cu cel oferit în temeiul cadrului UE privind protecția datelor. **Aceasta înseamnă nu numai că legislația Regatului Unit trebuie să fie „în esență echivalentă" cu legislația UE în ceea ce privește prelucrarea datelor cu caracter personal transferate către Regatul Unit în temeiul proiectului de decizie, ci și că normele aplicabile în Regatul Unit cu privire la transferul ulterior al acestor date către țări terțe trebuie să asigure în continuare un nivel de protecție în esență echivalent.**

77. Prin urmare, este important ca orice transfer ulterior din Regatul Unit către o altă țară terță de date cu caracter personal din SEE să fie protejat în mod corespunzător prin garanții sau să fie efectuat în conformitate cu normele privind derogările[44] pentru a asigura continuitatea protecției oferite de legislația UE. **Într-adevăr, dacă nu se poate oferi o astfel de protecție, transferurile ulterioare de date cu caracter personal din SEE nu ar trebui să aibă loc.**

78. CEPD recunoaște că Regatul Unit a reflectat, în cea mai mare parte, capitolul V din RGPD în RGPD al Regatului Unit (articolele 44-49) și în DPA 2018[45]. **Cu toate acestea, CEPD a identificat anumite aspecte ale cadrului legislativ din Regatul Unit în ceea ce privește transferurile ulterioare care ar putea submina nivelul de protecție a datelor cu caracter personal transferate din SEE.**

79. **Prima provocare** identificată de CEPD se referă la recunoașterea de către Regatul Unit, în urma procedurii elaborate în cadrul DPA 2018, a țărilor terțe, a organizațiilor internaționale sau a teritoriilor[46] ca beneficiari adecvați. Într-adevăr, transferurile ulterioare de date cu caracter

[44] A se vedea articolul 49 din RGPD al Regatului Unit.
[45] A se vedea articolele 17A, 17B, 17C și 18 din DPA 2018.
[46] A se vedea articolul 17A din DPA 2018.

personal din SEE pot avea loc din Regatul Unit către alte țări terțe, pe baza unei eventuale reglementări viitoare a Regatului Unit cu privire la caracterul adecvat al nivelului de protecție[47].

80. Mai exact, astfel cum s-a explicat în considerentul 77 al proiectului de decizie, secretarul de stat al Regatului Unit are competența de a recunoaște o țară terță (sau un teritoriu sau un sector dintr-o țară terță), o organizație internațională sau o descriere a țării, a teritoriului, a sectorului sau a organizației respective, ca asigurând un nivel adecvat de protecție a datelor cu caracter personal, în urma consultării ICO[48]. Atunci când evaluează caracterul adecvat al nivelului de protecție, secretarul de stat al Regatului Unit trebuie să ia în considerare aceleași elemente pe care Comisia Europeană trebuie să le evalueze în temeiul articolului 45 alineatul (2) literele (a)-(c) din RGPD, interpretat în coroborare cu considerentul 104 din RGPD și cu jurisprudența UE reținută în jurisprudența internă. Aceasta înseamnă că, atunci când se evaluează nivelul adecvat de protecție al unei țări terțe, standardul relevant va fi dacă țara terță în cauză asigură un nivel de protecție „în esență echivalent" cu cel garantat în Regatul Unit. Deși CEPD ia act de capacitatea Regatului Unit, în temeiul RGPD al Regatului Unit, de a recunoaște teritoriile ca oferind un nivel de protecție adecvat în lumina cadrului de protecție a datelor din Regatul Unit, CEPD dorește să sublinieze că ar putea fi posibil ca aceste teritorii să nu beneficieze, până în prezent, de o decizie privind caracterul adecvat al nivelului de protecție, adoptată de Comisia Europeană, prin care se recunoaște un nivel de protecție „în esență echivalent" cu cel garantat în UE. Acest lucru ar putea conduce la posibile riscuri în ceea ce privește protecția oferită datelor cu caracter personal transferate din SEE, în special în cazul în care, în viitor, cadrul de protecție a datelor din Regatul Unit s-ar abate de la acquis-ul UE. Trebuie remarcat faptul că, în iulie 2020, cauza de referință *Schrems II* a CJUE[49] s-a soluționat cu declararea ca nevalidă a Deciziei SUA cu privire la scutul de confidențialitate, deoarece, potrivit CJUE, cadrul juridic al SUA nu a putut fi considerat ca oferind un nivel de protecție în esență echivalent cu cel al UE. Cu toate acestea, hotărârile CJUE deja adoptate, considerate ca fiind jurisprudență reținută în cadrul juridic al Regatului Unit, ar putea să nu mai fie obligatorii pentru Regatul Unit, întrucât, în special, Regatul Unit are posibilitatea de a modifica dreptul Uniunii menținut în dreptul intern după încheierea perioadei de grație, iar Curtea Supremă nu are obligația de a se supune jurisprudenței UE reținute în jurisprudența internă[50].

81. **CEPD invită Comisia Europeană să monitorizeze îndeaproape procesul și criteriile de evaluare a caracterului adecvat al nivelului de protecție utilizate de autoritățile din Regatul Unit cu privire la alte țări terțe, în special în ceea ce privește țările terțe pe care UE nu le recunoaște ca asigurând un nivel de protecție adecvat în temeiul RGPD. În cazul în care Comisia Europeană constată că o țară terță cu privire la care Regatul Unit consideră că asigură un nivel de protecție adecvat nu oferă un nivel de protecție în esență echivalent cu cel garantat în UE, CEPD invită Comisia Europeană să ia toate măsurile necesare, cum ar fi, de exemplu, modificarea deciziei privind caracterul adecvat al nivelului de protecție referitoare la Regatul Unit, pentru a introduce garanții specifice privind datele cu caracter personal care provin din SEE și/sau pentru a lua în considerare suspendarea deciziei privind caracterul adecvat al nivelului de protecție referitoare la Regatul**

[47] Echivalentul unei decizii privind caracterul adecvat al nivelului de protecție în temeiul RGPD în Regatul Unit.
[48] A se vedea articolul 182 alineatul (2) din DPA 2018. A se vedea, de asemenea, memorandumul de înțelegere privind rolul ICO în legătură cu noile evaluări cu privire la caracterul adecvat al nivelului de protecție asigurat în Regatul Unit, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/03/secretary-of-state-for-the-department-for-dcms-and-the-information-commissioner-sign-memorandum-of-understanding/.
[49] A se vedea hotărârea *Schrems II*.
[50] A se vedea articolul 6 alineatele (3)-(6) din Legea din 2018 privind Uniunea Europeană (retragere).

Unit, în cazul în care datele cu caracter personal transferate din SEE către Regatul Unit fac obiectul unor transferuri ulterioare către țara terță în cauză în baza unei reglementări a Regatului Unit cu privire la caracterul adecvat al nivelului de protecție.

82. **A doua provocare** se referă la viitoarea revizuire a deciziilor deja existente privind caracterul adecvat al nivelului de protecție adoptate de Comisia Europeană în temeiul Directivei 95/46/CE. În urma acestei revizuiri, Comisia Europeană ar putea decide că anumite țări care au beneficiat până în prezent de o decizie privind caracterul adecvat al nivelului de protecție nu mai asigură un nivel de protecție în esență echivalent, ținând seama de legislația actuală a UE și de jurisprudența recentă. Cu toate acestea, astfel cum se prevede la punctul 4 din anexa 21 la DPA 2018, Regatul Unit a recunoscut deja aceste țări ca oferind un nivel de protecție adecvat. Chiar dacă secretarul de stat al Regatului Unit trebuie să efectueze o revizuire a acestor constatări privind caracterul adecvat al nivelului de protecție în termen de patru ani, Comisia Europeană observă în proiectul său de decizie că aceste constatări privind caracterul adecvat al nivelului de protecție nu vor înceta în mod automat să existe în cazul în care secretarul de stat al Regatului Unit nu efectuează revizuirea necesară în termenul prevăzut de patru ani[51].

83. **CEPD invită Comisia Europeană să monitorizeze dacă, odată finalizată revizuirea de către UE a deciziilor deja existente privind caracterul adecvat al nivelului de protecție, o țară în legătură cu care se consideră că nu mai asigură un nivel de protecție adecvat este considerată în continuare ca asigurând un nivel de protecție adecvat de către Regatul Unit. În acest caz, CEPD invită Comisia Europeană, pe baza considerentelor 277-280 din proiectul de decizie, să ia orice măsuri adecvate pentru a remedia situația, de exemplu prin modificarea deciziei privind caracterul adecvat al nivelului de protecție pentru a adăuga cerințe specifice pentru datele cu caracter personal care provin din SEE și/sau prin suspendarea deciziei privind caracterul adecvat al nivelului de protecție, în cazul în care datele cu caracter personal transferate din SEE către Regatul Unit fac obiectul unor transferuri ulterioare către țara terță în cauză. CEPD invită Comisia Europeană să continue acest exercițiu de monitorizare pe durata de valabilitate a deciziei privind caracterul adecvat al nivelului de protecție referitoare la Regatul Unit.**

84. **A treia provocare** se referă la transferul ulterior de date cu caracter personal din SEE către țări care nu asigură un nivel de protecție adecvat, pe baza instrumentelor de transfer prevăzute la articolele 46 și 47 din RGPD al Regatului Unit. Deși RGPD al Regatului Unit prevede aceleași instrumente de transfer precum cele prevăzute de RGPD, CEPD subliniază necesitatea asigurării faptului că garanțiile pe care le conțin oferă o protecție eficace în țara terță, în special având în vedere hotărârea *Schrems II*.

85. În urma hotărârii *Schrems II*, în care CJUE reamintește că protecția acordată datelor cu caracter personal în UE trebuie să urmeze datele oriunde sunt transferate, CEPD a adoptat deja recomandări inițiale privind o serie de măsuri suplimentare[52] pentru a ajuta exportatorii, atunci când este necesar, să se asigure că persoanele vizate beneficiază de un nivel de protecție în esență echivalent cu cel garantat în UE.

[51] A se vedea considerentul 82 din proiectul de decizie.

[52] A se vedea Recomandările CEPD 01/2020 privind măsurile care completează instrumentele de transfer pentru a asigura conformitatea cu nivelul UE de protecție a datelor cu caracter personal, adoptate la 10 noiembrie 2020, în curs de finalizare în urma procedurii de consultare publică, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_ro.pdf.

86. Potrivit CJUE, exportatorii de date au responsabilitatea de a verifica, de la caz la caz și, dacă este necesar, în colaborare cu importatorul de date din țara terță, dacă dreptul sau practica țării terțe afectează eficacitatea garanțiilor adecvate conținute de instrumentele de transfer prevăzute la articolul 46 din RGPD[53]. În cazul în care intervine o astfel de situație, exportatorii de date ar trebui să pună în aplicare măsuri suplimentare care să acopere aceste lacune în materie de protecție și să o aducă la nivelul impus de legislația UE.

87. **Pentru a asigura continuitatea protecției, CEPD invită Comisia Europeană să introducă în proiectul de decizie asigurări că, atunci când instrumentele de transfer prevăzute la articolele 46 și 47 din RGPD al Regatului Unit sunt utilizate de exportatorii de date din Regatul Unit pentru transferuri ulterioare către alte țări terțe ale datelor transferate din SEE, acești exportatori de date evaluează, de la caz la caz, cadrul de protecție a datelor din țara terță și, dacă este necesar, iau măsurile corespunzătoare pentru a asigura respectarea efectivă a garanțiilor conținute de instrumentul de transfer ales, pentru a asigura un nivel de protecție în esență echivalent cu cel garantat în cadrul UE. Fără aceste asigurări, CEPD subliniază că există riscul ca nivelul de protecție în esență echivalent cu cel garantat în UE să fie diminuat prin transferuri ulterioare din Regatul Unit.**

88. **A patra provocare** legată de transferurile ulterioare se referă la acordurile internaționale încheiate sau care urmează să fie încheiate în viitor de Regatul Unit și la eventualul acces direct al autorităților din țara terță care este parte/țările terțe care sunt părți la astfel de acorduri la date cu caracter personal din SEE. Într-adevăr, CEPD își exprimă profunda îngrijorare cu privire la Acordul în temeiul legii CLOUD dintre Regatul Unit și SUA, deja încheiat, iar Comisia Europeană recunoaște această provocare, subliniind că „o posibilă intrare în vigoare a acordului poate avea un impact asupra nivelului de protecție evaluat în prezenta decizie”[54]. Într-adevăr, în baza acestui acord, după intrarea sa în vigoare, datele cu caracter personal transferate din SEE către Regatul Unit în temeiul proiectului de decizie ar face apoi obiectul dispozițiilor acestui acord care stabilesc condițiile pentru accesul direct al autorităților SUA, cu impact asupra cadrului de protecție a datelor din Regatul Unit, inclusiv asupra dispozițiilor privind transferurile ulterioare. Prin urmare, nivelul de protecție oferit datelor transferate din SEE poate fi afectat în mod substanțial de dispozițiile acordului încheiat cu SUA și poate avea un impact asupra nivelului de protecție a acestor date. CEPD ia act, în acest context, de faptul că Comisia Europeană face trimitere la explicațiile oferite de autoritățile Regatului Unit în considerentul 153 din proiectul său de decizie, fără a cita sau a furniza vreo asigurare sau vreun angajament scris concret și fără a indica dispoziții juridice specifice din legislația Regatului Unit, care ar pune în aplicare astfel de explicații.

89. CEPD și-a exprimat anterior îngrijorarea în această privință într-o scrisoare adresată Parlamentului European din data de 15 iunie 2020[55]. CEPD a subliniat că, pe baza „acquis-ului UE în domeniul protecției datelor și, în special, a RGPD și a Directivei privind aplicarea legii”, CEPD are rezerve cu privire la posibilitatea aplicării garanțiilor din acord pentru accesul la datele cu caracter personal din Regatul Unit în anumite circumstanțe care impun obligații de divulgare către SUA, precum și cu privire la suficiența acestor garanții, având în vedere standardele UE, astfel încât să nu fie subminat nivelul de protecție asigurat în UE.

[53] A se vedea hotărârea *Schrems II*, punctul 134.
[54] A se vedea considerentul 153 din proiectul de decizie.
[55] A se vedea răspunsul CEPD adresat deputaților în Parlamentul European Sophie in’t Veld și Moritz Körner cu privire la Acordul în temeiul legii Cloud dintre Regatul Unit și SUA, adoptat la 15 iunie 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf.

90. În plus, dispozițiile Acordului în temeiul legii CLOUD dintre Regatul Unit și SUA pot afecta în mod semnificativ condițiile de fond și procedurale în care datele cu caracter personal deținute de operatori sau de persoanele împuternicite de operatori în Regatul Unit pot fi accesate direct de către autoritățile SUA, având astfel impact asupra nivelului de protecție garantat de legislația Regatului Unit. Pentru a asigura un nivel de protecție în esență echivalent cu cel garantat de legislația UE, este, de exemplu, „esențial ca garanțiile prevăzute în acest acord să includă o autorizare judiciară prealabilă obligatorie, ca o garanție esențială pentru accesul la metadate și date referitoare la conținut. Pe baza evaluării sale preliminare și observând că acordul se referă la aplicarea dreptului intern, CEPD nu a putut identifica o astfel de dispoziție clară în acordul încheiat între Regatul Unit și SUA”[56].

91. Deși Comisia Europeană subliniază că datele obținute în temeiul acestui acord ar beneficia de măsuri de protecție echivalente cu garanțiile specifice prevăzute de așa-numitul „Acord-cadru UE-SUA”, CEPD își exprimă îngrijorarea deoarece nu este sigur dacă încorporarea acestor garanții în Acordul în temeiul legii CLOUD dintre Regatul Unit și SUA printr-o simplă trimitere care se aplică *mutatis mutandis* ar îndeplini criteriile unor norme clare, precise și accesibile în ceea ce privește accesul la datele cu caracter personal sau ar consacra în mod suficient astfel de garanții ca fiind eficace și ca putând da naștere unei acțiuni în justiție în temeiul legislației Regatului Unit.

92. **Prin urmare, CEPD recomandă Comisiei Europene să clarifice modul în care și pe baza cărui instrument juridic ar fi puse în aplicare și ar avea caracter obligatoriu în temeiul legislației Regatului Unit măsuri de protecție echivalente cu garanțiile specifice prevăzute de Acordul-cadru UE-SUA.**

93. CEPD observă, de asemenea, că dispozițiile Acordului în temeiul legii CLOUD dintre Regatul Unit și SUA, coroborate cu secțiunea 3 din Legea CLOUD din SUA[57], ridică semne de întrebare cu privire la aplicarea efectivă a garanțiilor oferite de acord pentru accesul autorităților de aplicare a legii din SUA la datele cu caracter personal din Regatul Unit prelucrate de furnizorii de servicii de comunicații electronice sau de servicii informatice la distanță (denumiți în continuare „furnizori de servicii cloud”) care intră sub jurisdicția SUA. Într-adevăr, în cazul în care un furnizor de servicii cloud situat în Regatul Unit se supune legislației SUA (de exemplu, deoarece este filiala unei societăți din SUA), rămâne de stabilit dacă autoritățile SUA ar fi obligate să recurgă la Acordul în temeiul legii CLOUD dintre Regatul Unit și SUA pentru a obține datele respective. După cum subliniază Comisia Europeană, „se va acorda o atenție specială aplicării și adaptării măsurilor de protecție prevăzute în Acordul-cadru în funcție de tipul specific de transferuri vizate de Acordul dintre Regatul Unit și SUA”; CEPD subliniază că, pe baza evaluării sale preliminare, nu este clar dacă garanțiile consacrate în Acordul în temeiul legii CLOUD dintre Regatul Unit și SUA și, prin urmare, cele prevăzute de Acordul-cadru UE-SUA s-ar aplica, dacă este cazul, tuturor cererilor de acces la date din Regatul Unit formulate de autoritățile SUA în temeiul Legii CLOUD din SUA.

94. Ar putea exista și alte acorduri sau angajamente internaționale viitoare cu țări terțe pe care Regatul Unit le-ar putea încheia în viitor și care s-ar aplica datelor cu caracter personal transferate din SEE către Regatul Unit în temeiul proiectului de decizie[58]. În funcție de dispozițiile acestor acorduri și de aplicarea clauzelor de salvgardare specifice, prin faptul că afectează cadrul de protecție a datelor din Regatul Unit, aceste acorduri internaționale pot avea, de asemenea, un impact semnificativ

[56] A se vedea scrisoarea CEPD menționată mai sus.
[57] A se vedea Legea CLOUD din SUA, https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.
[58] A se vedea secțiunea 2.3.3 de mai sus.

asupra condițiilor de fond și procedurale pentru accesul autorităților din țări terțe la datele cu caracter personal din Regatul Unit. Acest lucru este valabil în special în cazul proiectului celui de al doilea protocol adițional la Convenția Consiliului Europei privind criminalitatea informatică (denumită în continuare „Convenția de la Budapesta"), aflat în prezent în curs de negociere între părțile la această convenție, care includ mai multe țări din afara UE. Într-adevăr, proiectul de protocol include clauze care pot fi activate în mod discreționar de către părți, de exemplu în ceea ce privește autorizarea sau neautorizarea accesului la datele referitoare la conținut. Deși toate statele membre ale UE ar activa clauzele în conformitate cu normele UE privind protecția datelor, nu a fost furnizată nicio garanție în ceea ce privește Regatul Unit, care s-ar putea abate în mod substanțial de la nivelul de protecție care ar fi oferit la momentul respectiv în cadrul UE. Un alt exemplu în sensul celor prezentate mai sus îl reprezintă Acordul dintre Regatul Unit și Japonia pentru un parteneriat economic cuprinzător[59] (denumit în continuare „CEPA"), primul acord comercial al Regatului Unit post-Brexit, care a intrat în vigoare la 1 ianuarie 2021[60] și care include dispoziții privind datele cu caracter personal[61]. CEPD ia act, de asemenea, de faptul că, la 1 februarie 2021, Regatul Unit și-a anunțat oficial cererea de aderare la Acordul de parteneriat transpacific cuprinzător și progresiv (denumit în continuare „CPTPP"), care include Acordul de parteneriat transpacific (TPP)[62].

95. CEPD constată că, în afară de Acordul în temeiul legii CLOUD dintre Regatul Unit și SUA, acordurile internaționale menționate mai sus nu sunt abordate în proiectul de decizie.

96. **CEPD invită Comisia Europeană:**

- **să examineze interacțiunea dintre cadrul de protecție a datelor din Regatul Unit și angajamentele sale internaționale, dincolo de Acordul în temeiul legii CLOUD dintre Regatul Unit și SUA, în special pentru a asigura continuitatea nivelului de protecție în cazul în care datele cu caracter personal transferate din SEE în Regatul Unit în baza unei decizii privind caracterul adecvat al nivelului de protecție referitoare la Regatul Unit sunt transferate ulterior către alte țări terțe și să monitorizeze în permanență și să ia măsuri, dacă este necesar, cu privire la încheierea de alte acorduri internaționale între Regatul Unit și țări terțe, care prezintă riscul subminării nivelului de protecție a datelor cu caracter personal asigurat în UE;**

- **să furnizeze CEPD angajamente scrise din partea autorităților Regatului Unit și să identifice dispoziții specifice în legislația Regatului Unit în legătură cu explicația referitoare la posibila**

[59] A se vedea Regatul Unit/Japonia: Acordul pentru un parteneriat economic cuprinzător [CS Japonia nr. 1/2020], https://www.gov.uk/government/publications/ukjapan-agreement-for-a-comprehensive-economic-partnership-cs-japan-no12020.

[60] A se vedea orientările Guvernului Regatului Unit privind acordurile comerciale ale Regatului Unit cu țări din afara UE, https://www.gov.uk/guidance/uk-trade-agreements-with-non-eu-countries.

[61] În conformitate cu articolul 8.80 alineatul (5) din CEPA, părțile se angajează să încurajeze dezvoltarea unor mecanisme de promovare a compatibilității între diferitele lor abordări juridice în materie de protecție a datelor (cu caracter personal). În temeiul articolului 8.84, părțile se angajează să nu interzică sau să nu restricționeze transferul transfrontalier de informații prin mijloace electronice, inclusiv de informații cu caracter personal, atunci când această activitate este destinată desfășurării activității comerciale a unei persoane vizate în înțelesul CEPA.

[62] În temeiul articolului 14.11 alineatul (2) din TPP, fiecare parte permite transferul transfrontalier de informații prin mijloace electronice, inclusiv de informații cu caracter personal, atunci când această activitate este destinată desfășurării activității comerciale a unei persoane vizate.

aplicare și punere în aplicare a Acordului în temeiul legii CLOUD dintre Regatul Unit și SUA, astfel cum se menționează în considerentul 153 din proiectul de decizie;

- **să monitorizeze, în acest context, dacă, în plus față de garanțiile care ar putea fi oferite de o punere în aplicare corespunzătoare a Acordului-cadru UE-SUA adaptat, Acordul în temeiul legii CLOUD dintre Regatul Unit și SUA asigură garanții suplimentare adecvate care să țină seama de nivelul de sensibilitate al categoriilor de date în cauză și de cerințele unice ale transferului de probe electronice direct de către furnizorii de servicii cloud și nu între autorități;**

- **să evalueze impactul și riscurile potențiale ale dispozițiilor privind datele cu caracter personal cuprinse în acordurile internaționale semnate recent de Regatul Unit, cum ar fi CEPA.**

97. **A cincea provocare** identificată se referă la aplicarea de derogări pentru transferurile de date cu caracter personal către o țară terță. Deși derogările disponibile în temeiul RGPD al Regatului Unit sunt aceleași cu cele prevăzute în RGPD, este important ca ICO să aplice și să continue să aplice în ceea ce privește utilizarea acestor derogări o interpretare aliniată la cea a CEPD. În caz contrar sau dacă Regatul Unit se îndepărtează de această interpretare în viitor, ar exista riscul ca nivelul de protecție a datelor transferate din SEE către țări terțe prin Regatul Unit să fie subminat.

98. **CEPD invită Comisia Europeană, ca parte a sarcinii sale de monitorizare, să verifice în mod specific dacă interpretarea Regatului Unit privind utilizarea derogărilor rămâne aliniată la interpretarea UE. Cu toate acestea, în cazul în care Regatul Unit ar avea în vedere o interpretare diferită a utilizării derogărilor, care subminează nivelul de protecție, este esențial ca Comisia Europeană să ia măsurile necesare prin modificarea deciziei privind caracterul adecvat al nivelului de protecție, pentru a se asigura că nivelul de protecție oferit datelor cu caracter personal transferate din SEE către Regatul Unit nu va fi subminat atunci când aceste date sunt transferate ulterior din Regatul Unit către țări terțe pe baza unei interpretări diferite a derogărilor.**

99. **A șasea provocare**, ultima din această secțiune, se referă la absența măsurilor de protecție prevăzute la articolul 48 din RGPD din cadrul de protecție a datelor din Regatul Unit.

100. În proiectul său de decizie, Comisia Europeană într-adevăr clarifică faptul că, în absența unor garanții adecvate sau a unor reglementări cu privire la caracterul adecvat al nivelului de protecție, transferurile se pot realiza numai în baza unor derogări prevăzute la articolul 49 din RGPD al Regatului Unit, „cu excepția articolului 48 din Regulamentul (UE) 2016/679, pe care Regatul Unit a ales să nu îl includă în RGPD al Regatului Unit”.[63] Absența unei dispoziții în esență echivalente cu articolul 48 din RGPD, consacrată în cadrul de protecție a datelor din Regatul Unit, în ceea ce privește transferurile sau divulgările de date în urma unei hotărâri a unei instanțe sau a unui tribunal sau a unei decizii a unei autorități administrative dintr-o altă țară terță poate conduce la insecuritate juridică în legătură cu posibilitatea afectării semnificative a nivelului de protecție a datelor cu caracter personal transferate din SEE în Regatul Unit în temeiul proiectului de decizie.

101. În Criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD, CEPD subliniază că, în ceea ce privește transferurile ulterioare, „transferurile ulterioare de date cu caracter personal efectuate de destinatarul inițial al transferului de date ar trebui să fie autorizate

[63] A se vedea considerentul 78 din proiectul de decizie.

numai în cazul în care noul destinatar [...] face, de asemenea, obiectul unor norme [...] care asigură un nivel adecvat de protecție și urmează instrucțiunile relevante atunci când prelucrează date în numele operatorului de date”[64]. În plus, CEPD subliniază că „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”[65]. În cadrul capitolului V din RGPD, articolul 48 trebuie să fie luat pe deplin în considerare atunci când se evaluează dacă, la nivelul cadrului juridic din Regatul Unit, se asigură un nivel de protecție în esență echivalent în această privință[66].

102. CEPD subliniază, în acest context, jurisprudența CJUE în ceea ce privește riscul de abuz sau de acces și utilizare ilicită a datelor, precizând, în special, că „[r]eferitor la nivelul de protecție a libertăților și a drepturilor fundamentale garantat în cadrul Uniunii, o reglementare a acesteia care implică o ingerință în drepturile fundamentale garantate la articolele 7 și 8 din cartă trebuie, potrivit jurisprudenței constante a Curții, să prevadă norme clare și precise care să reglementeze conținutul și aplicarea unei măsuri și care să impună o serie de cerințe minime, astfel încât persoanele ale căror date cu caracter personal sunt vizate să dispună de garanții suficiente care să permită protejarea în mod eficient a datelor lor împotriva riscurilor de abuz, precum și împotriva oricărei accesări și a oricărei utilizări ilicite a acestor date. Necesitatea de a dispune de asemenea garanții este cu atât mai importantă în cazul în care datele cu caracter personal sunt supuse unei prelucrări automate și există un risc important de acces ilicit la aceste date”[67].

103. CEPD observă în această privință că, în baza informațiilor disponibile în proiectul de decizie, cadrul de protecție a datelor din Regatul Unit nu prevede în mod clar că orice hotărâre a unei instanțe sau a unui tribunal și orice decizie a unei autorități administrative a unei țări terțe care impun unui operator sau persoanei împuternicite de operator să transfere sau să divulge date cu caracter personal poate fi recunoscută sau executată în orice fel numai dacă se bazează pe un acord internațional în vigoare între țara terță solicitantă și Regatul Unit. Articolul 48 din RGPD reprezintă o dispoziție esențială a capitolului V din RGPD, deoarece prevede că un transfer sau o divulgare de date cu caracter personal în urma unei hotărâri a unei instanțe sau a unui tribunal sau a unei decizii a unei autorități administrative dintr-o țară terță poate fi recunoscut(ă) sau executat(ă) numai dacă se bazează pe un acord internațional în vigoare între țara terță solicitantă și Uniune sau un stat membru, fără a se aduce atingere altor motive de transfer în temeiul capitolului V din RGPD. Într-adevăr, CEPD reamintește că „o cerere din partea unei autorități străine nu constituie în sine un temei juridic pentru transfer. Ordinul poate fi recunoscut «numai dacă se bazează pe un acord internațional, cum ar fi un tratat de asistență judiciară reciprocă, în vigoare între țara terță solicitantă și Uniune sau un stat membru»”[68]. Prin urmare, este foarte important ca dispozițiile în esență echivalente să poată fi identificate în legislația Regatului Unit.

[64] A se vedea WP 254 rev.01, p. 6.
[65] A se vedea WP 254 rev.01, p. 6.
[66] A se vedea articolul 44 din RGPD, ultima teză, în special: „Toate dispozițiile din prezentul capitol se aplică pentru a se asigura că nivelul de protecție a persoanelor fizice garantat prin prezentul regulament nu este subminat.”
[67] A se vedea hotărârea *Schrems I*, punctul 91.
[68] A se vedea anexa la Răspunsul comun al CEPD și AEPD către Comisia LIBE cu privire la implicațiile Legii Cloud a SUA asupra cadrului juridic al UE privind protecția datelor cu caracter personal, adoptat la

104. În proiectul de decizie, Comisia Europeană prezintă explicații din partea autorităților Regatului Unit conform cărora, în temeiul dreptului comun sau al statutelor, o hotărâre judecătorească străină prin care se solicită date nu este executorie în Regatul Unit în absența unui acord internațional, iar orice transfer de date la cererea unei instanțe judecătorești sau a unei autorități administrative străine necesită un instrument de transfer, cum ar fi o reglementare cu privire la caracterul adecvat al nivelului de protecție sau garanții adecvate, cu excepția cazului în care se aplică o derogare în temeiul articolului 49 din RGPD al Regatului Unit. Cu toate acestea, Comitetului european pentru protecția datelor nu i s-au pus la dispoziție comunicările dintre Comisia Europeană și autoritățile Regatului Unit[69] în această privință și, prin urmare, nu este în măsură să analizeze și să evalueze în mod independent dacă garanțiile oferite de autoritățile Regatului Unit sunt suficiente pentru a asigura un nivel de protecție în esență echivalent în ceea ce privește garanțiile prevăzute la articolul 48 din RGPD.

105. **CEPD invită Comisia Europeană să furnizeze asigurări suplimentare și trimiteri specifice la legislația Regatului Unit, prin care să se asigure că nivelul de protecție în temeiul cadrului juridic din Regatul Unit este în esență echivalent cu cel garantat în SEE. Prin urmare, CEPD invită Comisia Europeană să furnizeze explicații și angajamente scrise din partea autorităților Regatului Unit cu privire la punerea în aplicare a unor măsuri de protecție echivalente în esență cu cele prevăzute la articolul 48 din RGPD.**

106. **CEPD consideră că identificarea dispozițiilor din legislația Regatului Unit care asigură un nivel de protecție în esență echivalent în ceea ce privește garanțiile prevăzute la articolul 48 din RGPD este cu atât mai importantă având în vedere preocupările exprimate anterior cu privire la cererile de acces la date din Regatul Unit formulate de autoritățile din SUA sau din alte țări terțe și având în vedere că, în conformitate cu decizia privind caracterul adecvat al nivelului de protecție, datele cu caracter personal ar putea fi transferate din SEE în Regatul Unit fără nicio altă garanție și fără niciun alt angajament obligatoriu din partea destinatarului în ceea ce privește cererile de acces la date din partea autorităților din alte țări terțe.**

3.2. Mecanisme procedurale și de aplicare a legii

107. Pe baza criteriilor de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD, CEPD a analizat următoarele aspecte ale cadrului de protecție a datelor din Regatul Unit, astfel cum sunt avute în vedere în proiectul de decizie: existența și funcționarea eficace a unei autorități de supraveghere independente, existența unui sistem care să asigure un bun nivel de conformitate și un sistem de acces la mecanisme adecvate de recurs care să ofere persoanelor din UE mijloacele necesare pentru a-și exercita drepturile și pentru a obține reparații, fără a întâmpina dificultăți semnificative în ceea ce privește accesarea căilor de atac administrative și judiciare.

3.2.1. Autoritatea independentă competentă de supraveghere

108. CEPD salută eforturile Comisiei Europene de a examina în mod cuprinzător instituirea, funcționarea și competențele autorității de supraveghere din Regatul Unit în capitolul 2.6 din proiectul de decizie. În Regatul Unit, comisarul pentru informații (denumit în continuare „IC") este însărcinat cu supravegherea și asigurarea respectării RGPD al Regatului Unit și a DPA 2018. În conformitate cu

10 iulie 2019, https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en.

[69] A se vedea considerentul 78 din proiectul de decizie.

anexa 12 la DPA 2018, IC se circumscrie noțiunii de „corporation sole", fiind o entitate juridică separată constituită dintr-o singură persoană, sprijinită de un birou, respectiv ICO.

109. În ceea ce privește independența IC, CEPD subliniază că articolul 51 din RGPD al Regatului Unit nu conține o clarificare explicită a faptului că IC este o autoritate publică independentă, astfel cum se prevede la articolul 51 din RGPD în ceea ce privește autoritățile de supraveghere. Cu toate acestea, CEPD recunoaște că RGPD al Regatului Unit reflectă, la articolul 52, în mod similar normele corespunzătoare în ceea ce privește independența, astfel cum se prevede la articolul 52 alineatele (1)-(3) din RGPD.

110. În plus, CEPD subliniază că articolul 52 din RGPD al Regatului Unit nu prevede obligații care să corespundă celor prevăzute la articolul 52 alineatele (4)-(6) din RGPD și care să asigure în mod expres faptul că autoritatea de supraveghere respectivă dispune de resursele necesare pentru îndeplinirea sarcinilor și exercitarea efectivă a competențelor sale. Cu toate acestea, CEPD recunoaște că DPA 2018 conține dispoziții care vizează asigurarea unei finanțări adecvate a ICO[70], precum și faptul că ICO este în prezent una dintre cele mai mari autorități de supraveghere în comparație cu autoritățile de supraveghere din UE/SEE. Întrucât alocarea continuă de resurse adecvate, în special în ceea ce privește personalul și bugetul[71], este imperios necesară pentru a asigura funcționarea corespunzătoare a unei autorități de supraveghere în vederea îndeplinirii tuturor sarcinilor care i-au fost atribuite și a fost, de asemenea, considerată recent de Parlamentul European ca fiind de importanță majoră[72], CEPD consideră că este esențial să se acorde o atenție deosebită evoluțiilor viitoare din acest domeniu.

111. **Prin urmare, CEPD invită Comisia Europeană să observe orice evoluții în ceea ce privește alocarea de resurse către ICO, care ar fi în detrimentul îndeplinirii corespunzătoare a sarcinilor ICO.**

3.2.2. Existența unui sistem de protecție a datelor care să asigure un bun nivel de conformitate

112. Proiectul de decizie efectuează o examinare cuprinzătoare a competențelor cu care este învestit ICO în temeiul articolului 58 din RGPD al Regatului Unit și DPA 2018 pentru a asigura monitorizarea și aplicarea legislației. CEPD recunoaște că articolul 58 din RGPD al Regatului Unit reflectă îndeaproape normele corespunzătoare celor prevăzute la articolul 58 din RGPD în ceea ce privește competențele autorităților de supraveghere. În ceea ce privește competența de a impune amenzi administrative în funcție de circumstanțele fiecărui caz în parte, articolul 83 din RGPD al Regatului Unit conține dispoziții și cuantumuri maxime similare celor prevăzute la articolul 83 din RGPD. Prin urmare, CEPD consideră că, în prezent, cadrul juridic al Regatului Unit în acest domeniu este în conformitate cu standardele prevăzute în legislația relevantă a UE. În această privință, CEPD subliniază totuși că existența unor sancțiuni *eficace* joacă un rol important în asigurarea respectării normelor[73].

[70] A se vedea articolele 137, 138, 182 și anexa 12 punctul 9 din DPA 2018.
[71] A se vedea WP 254 rev.01, p. 7.
[72] Rezoluția Parlamentului European din 25 martie 2021 referitoare la raportul de evaluare al Comisiei privind punerea în aplicare a Regulamentului general privind protecția datelor, la doi ani de la aplicarea acestuia, punctul 15, https://www.europarl.europa.eu/doceo/document/B-9-2021-0211_RO.html.
[73] A se vedea WP 254 rev.01, p. 7.

113. **Având în vedere cele de mai sus, CEPD invită Comisia Europeană să monitorizeze eficacitatea sancțiunilor și a căilor de atac relevante prevăzute de cadrul de protecție a datelor din Regatul Unit.**

3.2.3. Sistemul de protecție a datelor trebuie să furnizeze asistență și sprijin persoanelor vizate în exercitarea drepturilor acestora și mecanisme adecvate de recurs

114. Un mecanism eficace de supraveghere, care să permită investigarea independentă a plângerilor, astfel încât să se identifice și să se pedepsească în practică încălcările drepturilor persoanelor vizate, precum și o cale de atac administrativă și judiciară eficace (inclusiv despăgubiri pentru prejudiciile cauzate de prelucrarea ilegală a datelor cu caracter personal ale persoanei vizate) sunt elemente esențiale pentru a evalua dacă un sistem de protecție a datelor oferă un nivel de protecție adecvat.

115. CEPD salută faptul că ICO furnizează informații și orientări cuprinzătoare pe site-ul său, care vizează sensibilizarea operatorilor și a persoanelor împuternicite de operatori cu privire la obligațiile și sarcinile ce le revin, precum și sprijinirea persoanelor vizate pentru a fi informate cu privire la drepturile lor în materie de date cu caracter personal și pentru a-și exercita drepturile individuale în temeiul RGPD al Regatului Unit și al DPA 2018.

116. **În pofida situației actuale, CEPD invită Comisia Europeană să observe în permanență nivelul de sprijin pe care ICO îl acordă în mod specific persoanelor ale căror date cu caracter personal au fost transferate în Regatul Unit în temeiul deciziei privind caracterul adecvat al nivelului de protecție, pentru a le ajuta să își exercite drepturile în temeiul regimului de protecție a datelor din Regatul Unit.**

4. ACCESAREA ȘI UTILIZAREA DATELOR CU CARACTER PERSONAL TRANSFERATE DIN UE DE CĂTRE AUTORITĂȚILE DIN REGATUL UNIT

4.1. Accesul și utilizarea de către autoritățile publice din Regatul Unit în scopuri de aplicare a legii

4.1.1. Temeiurile juridice și limitările/garanțiile aplicabile

117. În ceea ce privește evaluarea efectuată de Comisia Europeană și documentată în considerentul 132 și următoarele din proiectul de decizie **privind accesul în scopuri de aplicare a legii**, Comisia Europeană furnizează informații nuanțate și detaliate și ajunge, în general, la concluzii ușor de înțeles. Prin urmare, CEPD se abține de la reproducerea majorității constatărilor și evaluărilor factuale în prezentul aviz. Cu toate acestea, există anumite situații în care prezentarea faptelor și explicarea concluziilor nu sunt suficiente pentru ca CEPD să și le poată însuși.

4.1.1.1. Utilizarea consimțământului

118. CEPD ia act de faptul că Comisia Europeană afirmă în nota de subsol 184 din proiectul de decizie[74] că **utilizarea consimțământului** nu este relevantă într-un scenariu privind caracterul adecvat al nivelului de protecție, deoarece, în situațiile de transfer, datele nu sunt colectate direct de la o persoană vizată de către o autoritate de aplicare a legii din Regatul Unit pe baza consimțământului.

[74] A se vedea pagina 37 din proiectul de decizie.

În consecință, utilizarea consimțământului ca temei juridic în activitățile polițienești nu este evaluată de Comisia Europeană.

119. În acest sens, CEPD reamintește că articolul 45 alineatul (2) litera (a) din RGPD impune evaluarea unei game largi de elemente care nu se limitează la situația transferului, inclusiv „statul de drept, respectarea drepturilor omului și a libertăților fundamentale, legislația relevantă, atât generală, cât și sectorială, inclusiv [...] dreptul penal".

120. CEPD observă, inclusiv pe baza informațiilor furnizate de Comisia Europeană în considerentul 38 din proiectul său de decizie de punere în aplicare a Comisiei în temeiul Directivei (UE) 2016/680 a Parlamentului European și a Consiliului privind protecția adecvată a datelor cu caracter personal asigurată de Regatul Unit (denumită în continuare „decizia privind caracterul adecvat al nivelului de protecție în temeiul LED"), că utilizarea consimțământului, astfel cum este încadrată în regimul aplicabil din Regatul Unit în contextul asigurării respectării legii, ar necesita întotdeauna invocarea unui temei juridic. Acest lucru înseamnă că, în pofida faptului că autoritatea polițienească are competențe statutare de a prelucra datele în scopul unei anchete, în anumite circumstanțe specifice (de exemplu, pentru prelevarea unei probe ADN), poliția poate considera oportun să solicite consimțământul persoanei vizate.

121. **CEPD invită Comisia Europeană să introducă în decizia privind caracterul adecvat al nivelului de protecție o analiză asupra posibilității de utilizare a consimțământului într-un context de aplicare a legii, astfel cum se prevede în proiectul de decizie privind caracterul adecvat al nivelului de protecție în temeiul LED**.

4.1.1.2. Mandate de percheziție și ordine de divulgare

122. Deși, în general, CEPD nu are observații cu privire la recuperarea probelor de către poliție prin mandate de percheziție și ordine de divulgare, din considerentul 136 al proiectului de decizie reiese că Comisia Europeană și-a concentrat considerațiile privind accesul în scopul aplicării legii în jurul poliției și că prelucrarea datelor cu caracter personal de către alte agenții de aplicare a legii a fost examinată într-o mai mică măsură.

123. De exemplu, în „UK Explanatory Framework for Adequacy Discussions" (Cadrul explicativ al Regatului Unit pentru dezbateri privind caracterul adecvat al nivelului de protecție), secțiunea F: Aplicarea legii[75], se sugerează, la pagina 11, că **Agenția Națională de Combatere a Criminalității** (denumită în continuare „NCA") ar putea fi o autoritate de aplicare a legii de interes deosebit, care, printre altele, are o funcție mai vastă în ceea ce privește datele operative în materie penală. Conform propriei descrieri, NCA are misiunea de a centraliza date operative dintr-o serie de surse, cu scopul de a maximiza oportunitățile de analiză, de evaluare și cu caracter tactic, provenite inclusiv din interceptarea cu mijloace tehnice a comunicațiilor, de la parteneri în domeniul asigurării respectării legii din Regatul Unit și din străinătate, de la agenții de securitate și de la agenții de informații[76]. NCA este, de asemenea, unul dintre principalii interlocutori pentru

[75] A se vedea Guvernul Regatului Unit, Explanatory Framework for Adequacy Discussions (Cadrul explicativ al Regatului Unit pentru dezbateri privind caracterul adecvat al nivelului de protecție), secțiunea F: Aplicarea legii, 13 martie 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

[76] A se vedea site-ul Agenției Naționale de Combatere a Criminalității, Intelligence: enhancing the picture of serious organised crime affecting the UK (Date operative: evidențierea imaginii formelor grave de

partenerii internaționali din domeniul aplicării legii și joacă un rol esențial în schimbul de date operative în materie penală[77].

124. CEPD observă că, de asemenea, Comandamentul de comunicații al guvernului (denumit în continuare „GCHQ"), ale cărui activități intră de obicei sub incidența părții 4 din DPA 2018, și anume securitatea națională, își asumă și un rol activ în reducerea prejudiciilor societale și financiare cauzate Regatului Unit de infracțiunile grave și de criminalitatea organizată, colaborând îndeaproape cu Ministerul de Interne, NCA, Administrația Fiscală și Vamală („HMRC") și alte departamente guvernamentale[78]. Activitățile sale vizează combaterea abuzului sexual asupra copiilor, a fraudei, a altor tipuri de infracțiuni economice, inclusiv spălarea banilor, a utilizării ilicite a tehnologiei, a criminalității cibernetice, a criminalității organizate în domeniul imigrației, inclusiv traficul de persoane precum și a traficului de droguri și de arme de foc și a altor activități ilegale de contrabandă.

125. **CEPD solicită Comisiei Europene să își completeze analiza cu o examinare a autorităților care își desfășoară activitatea în domeniul aplicării legii și care par să fi făcut din colectarea și analizarea datelor, inclusiv a datelor cu caracter personal, un punct central al operațiunilor lor de zi cu zi, în special în cazul NCA. În plus, CEPD invită Comisia Europeană să analizeze cu mai mare atenție agențiile precum GCHQ, ale căror activități intră atât sub incidența aplicării legii, cât și a securității naționale, precum și cadrul juridic aplicabil acestora pentru prelucrarea datelor cu caracter personal.**

4.1.1.3. Competențe de investigare în scopuri de aplicare a legii

126. În capitolul 4 din Criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD, intitulat „Garanții esențiale în **țările terțe cu privire la accesul în scopuri legate de aplicarea legii** și de securitatea națională pentru a limita interferențele cu drepturile fundamentale", CEPD reamintește că „[î]n acest context, Curtea a remarcat, de asemenea, că decizia anterioară privind sfera de siguranță «nu cuprinde nicio constatare în privința existenței în Statele Unite a unor norme cu caracter statal destinate să limiteze eventualele ingerințe în drepturile fundamentale ale persoanelor ale căror date sunt transferate din Uniune către Statele

---

criminalitate organizată care afectează Regatul Unit), https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/intelligence-enhancing-the-picture-of-serious-organised-crime-affecting-the-uk.

[77] Deși nu toate datele operative prelucrate de NCA sunt date cu caracter personal, o parte substanțială ar putea consta în informații cu caracter personal, iar activitățile descrise în acest sens diferă de cele ale activităților polițienești clasice, astfel încât o evaluare a accesului la date cu caracter personal de către autoritățile de aplicare a legii din Regatul Unit ar fi incompletă fără o evaluare temeinică a activităților derulate de NCA. Pare rezonabil să se asigure faptul că principiile în materie de protecție a datelor au aceeași semnificație pentru toate autoritățile de aplicare a legii, oferind astfel clarificări în ceea ce privește o agenție care se bazează în mod special pe date, așa cum este NCA. În plus, la secțiunea „privind spre viitor", explicația continuă astfel: „căutăm în permanență noi oportunități de a atrage, dezvolta și consolida capabilitățile tradiționale pentru a spori cantitatea și calitatea datelor operative disponibile care pot fi exploatate atât în Regatul Unit, cât și în străinătate". „În acest demers, dezvoltăm noua capabilitate națională de exploatare a datelor, utilizând competențele conferite agenției prin Legea privind criminalitatea și instanțele, pentru a corela, accesa și exploata datele deținute la nivel guvernamental." [...] „Toate acestea ne vor spori agilitatea și flexibilitatea în reacția la noi amenințări și ne vor permite să acționăm în mod proactiv, să colectăm și să analizăm informații și date operative cu privire la amenințările emergente, astfel încât să putem acționa înainte ca amenințările să devină realitate."

[78] A se vedea site-ul GCHQ, Misiune, Infracțiuni grave și criminalitate organizată, https://www.gchq.gov.uk/section/mission/serious-crime.

Unite**, ingerințe pe care entități de stat din această țară ar fi autorizate să le practice atunci când urmăresc scopuri legitime**, precum securitatea națională»"[79]. În Criteriile de referință privind caracterul adecvat al nivelului de protecție, CEPD afirmă că respectivele **patru garanții europene esențiale**[80] **trebuie să fie respectate pentru accesul la date, fie** în scopuri legate de securitatea națională, fie **în scopuri de aplicare a legii, de către toate țările terțe, pentru ca nivelul de protecție să fie considerat adecvat și,** în special, **trebuie să se demonstreze necesitatea și proporționalitatea în ceea ce privește obiectivele legitime urmărite.**

127. În cadrul acestei secțiuni a proiectului de decizie, Comisia Europeană concluzionează astfel (în considerentul 139): „întrucât competențele de investigare conferite de IPA 2016 sunt aceleași cu cele de care dispun agențiile naționale de securitate, condițiile, limitările și garanțiile aplicabile acestor competențe sunt abordate în detaliu în secțiunea privind accesul și utilizarea datelor cu caracter personal de către autoritățile publice din Regatul Unit în scopuri de securitate națională". Cu toate acestea, din jurisprudența CJUE rezultă că, atunci când se aplică testul de necesitate și proporționalitate legislației statelor membre care permite păstrarea și accesul autorităților publice la datele cu caracter personal, obiectivele legitime, cum ar fi securitatea națională sau combaterea infracțiunilor grave, sunt diferite și, prin urmare, unul dintre acestea ar putea justifica un anumit tip de ingerință, în timp ce celelalte nu ar putea să justifice ingerințele respective[81].

128. **Prin urmare, CEPD ar saluta o evaluare specifică în cadrul deciziei privind necesitatea și proporționalitatea condițiilor, limitările și garanțiile descrise în considerentul 174 și următoarele – o secțiune dedicată măsurilor care urmăresc obiective de securitate națională – în ceea ce privește aplicarea acestor condiții, limitări și garanții în contextul unei măsuri care urmărește un obiectiv de aplicare a legii. Prin urmare, CEPD invită Comisia Europeană să clarifice în continuare dacă, astfel cum sunt descrise, păstrarea datelor cu caracter personal și accesul la acestea în scopuri de aplicare a legii sunt suficient de limitate, astfel încât să se asigure un nivel de protecție în esență echivalent cu cel garantat în UE.**

4.1.2. Utilizarea ulterioară a informațiilor colectate în scopuri de aplicare a legii (considerentele 140-154)

129. CEPD ia act de faptul că, în cadrul de protecție a datelor din Regatul Unit, se prevăd garanții și limitări similare celor prevăzute de legislația UE în ceea ce privește utilizarea ulterioară a informațiilor colectate în scopuri de aplicare a legii.

4.1.2.1. Utilizarea ulterioară în alte scopuri de aplicare a legii

130. Într-adevăr, DPA 2018 prevede că datele cu caracter personal colectate de o autoritate competentă într-un scop de aplicare a legii pot fi prelucrate ulterior (fie de către operatorul inițial, fie de către un alt operator) în orice alt scop de aplicare legii, cu condiția ca operatorul să fie autorizat prin lege să prelucreze date în celălalt scop, iar prelucrarea să fie necesară și proporțională cu scopul respectiv. Comisia Europeană ia act de faptul că toate garanțiile prevăzute în partea 3 din DPA 2018 se aplică prelucrării efectuate de autoritatea destinatară. Cu toate acestea, CEPD subliniază că, în partea 3 din DPA 2018, articolul 44 alineatul (4), articolul 45 alineatul (4), articolul 48 alineatul (3) și

[79] A se vedea WP 254 rev.01, p. 9.
[80] A se vedea Recomandările 02/2020 ale CEPD privind garanțiile esențiale europene pentru măsurile de supraveghere.
[81] A se vedea CJUE, cauzele conexate C-511/18, C-512/18 și C-520/18 *La Quadrature du Net și alții*, 6 octombrie 2020, ECLI:EU:C:2020:791.

articolul 68 alineatul (7) prevăd posibilitatea de restricționare a drepturilor persoanei vizate, iar articolul 79 prevede posibilitatea emiterii de certificate care să ateste că restricționarea este o măsură necesară și proporțională în scopul protejării securității naționale. **Prin urmare, CEPD recomandă Comisiei Europene să evalueze în continuare impactul posibil al unor astfel de restricții asupra nivelului de protecție a datelor cu caracter personal în ceea ce privește utilizarea ulterioară a informațiilor colectate. În mod similar, ar trebui furnizate clarificări suplimentare și în ceea ce privește cadrul juridic din Regatul Unit care permite o astfel de partajare ulterioară, în special Legea privind economia digitală din 2017, precum și Legea privind criminalitatea și instanțele din 2013, care permite schimbul de informații cu NCA.**

4.1.2.2. Utilizarea ulterioară în alte scopuri decât aplicare a legii în Regatul Unit

131. DPA 2018 prevede, de asemenea, că datele cu caracter personal colectate în orice scop de aplicare a legii pot fi prelucrate într-un scop care nu este unul de aplicare a legii atunci când prelucrarea este autorizată prin lege. În acest caz, temeiul juridic care autorizează o astfel de partajare este articolul 19 din Legea privind combaterea terorismului din 2008. În acest sens, CEPD constată că domeniul de aplicare și dispozițiile articolului 19 din Legea privind combaterea terorismului nu sunt abordate pe deplin în evaluarea Comisiei Europene și pot implica o utilizare ulterioară cu un caracter mai amplu, în special în ceea ce privește articolul 19 alineatul (2), care prevede că „informațiile obținute de oricare dintre serviciile de informații în legătură cu exercitarea oricăreia dintre funcțiile care îi revin pot fi utilizate de serviciul în cauză pentru exercitarea oricărei alte funcții din domeniul său de competență”.

132. CEPD observă, de asemenea, că referirea Comisiei Europene la faptul că autoritățile competente sunt autorități publice care trebuie să acționeze în conformitate cu Convenția europeană a drepturilor omului, inclusiv cu articolul 8 din aceasta, asigurându-se astfel că toate schimburile de date dintre agențiile de aplicare a legii și serviciile de informații respectă legislația privind protecția datelor și Convenția europeană a drepturilor omului, ar putea fi susținută suplimentar prin identificarea actelor și a legilor relevante din ordinea juridică a Regatului Unit care stabilesc astfel de limite în mod clar și precis.

4.1.2.3. Utilizarea ulterioară în contextul transferurilor ulterioare în afara Regatului Unit

133. Deși Comisia Europeană a făcut referire la faptul că Acordul în temeiul legii CLOUD dintre Regatul Unit și SUA poate afecta transferurile ulterioare de date către SUA dinspre furnizorii de servicii cloud din Regatul Unit, CEPD subliniază, de asemenea, că intrarea în vigoare a acestui acord poate afecta și utilizarea ulterioară a informațiilor colectate prin intermediul transferurilor ulterioare de date de la autoritățile de aplicare a legii ale Regatului Unit, în special în legătură cu emiterea și transmiterea de ordine în conformitate cu articolul 5 din Acordul în temeiul legii CLOUD dintre Regatul Unit și SUA.

134. În sens mai larg, CEPD consideră, de asemenea, că încheierea unor viitoare acorduri bilaterale cu țări terțe în scopul cooperării în materie de aplicare a legii, prin care se asigură un temei juridic pentru transferul datelor cu caracter personal către țările respective, poate afecta, de asemenea, în mod semnificativ condițiile pentru utilizarea ulterioară de informații colectate, întrucât astfel de acorduri pot afecta cadrul de protecție a datelor din Regatul Unit, astfel cum a fost acesta evaluat. Prin urmare, CEPD recomandă Comisiei Europene să evalueze suplimentar acest aspect, să identifice dacă există acorduri internaționale și să clarifice dacă prevederile acestor acorduri pot afecta aplicarea legislației privind protecția datelor din Regatul Unit, precum și să prevadă limitări sau excepțări suplimentare în ceea ce privește utilizarea ulterioară și divulgarea în străinătate a informațiilor colectate în scopuri de aplicare a legii. 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 Regatul Unit cu privire la divulgarea în străinătate și la utilizarea ulterioară a datelor.

4.1.3. Supraveghere

135. CEPD observă că supravegherea autorităților de aplicare a legii în materie penală este asigurată de o combinație de diferiți comisari, pe lângă ICO. În proiectul de constatări privind caracterul adecvat al nivelului de protecție sunt menționați IPC, comisarul pentru păstrarea și utilizarea materialelor biometrice, precum și comisarul pentru camere de supraveghere. În acest context, trebuie remarcat faptul că CJUE a subliniat în repetate rânduri necesitatea unei supravegheri independente. O importanță deosebită în ceea ce privește accesul la date cu caracter personal transferate către Regatul Unit revine activităților realizate de IPC. În înțelegerea CEPD, IPC este așa-numitul „comisar judiciar", la fel ca alți comisari judiciari, la care se face referire în contextul capitolului dedicat securității naționale, iar acești comisari judiciari se bucură de independența conferită judecătorilor, inclusiv atunci când exercită funcția de comisari. În ceea ce privește biroul IPC, Comisia Europeană explică, în considerentul 245 al proiectului de decizie, că acesta funcționează independent, sub forma unui așa-numit „organism ce funcționează în condiții obiective", deși este finanțat de Ministerul de Interne.

136. CEPD nu a identificat în proiectul de decizie indicații suplimentare pe baza cărora să poată evalua independența comisarului pentru păstrarea și utilizarea materialelor biometrice și a comisarului pentru camere de supraveghere.

137. **Comisia Europeană este invitată să evalueze în continuare independența comisarilor judiciari, inclusiv în cazurile în care comisarul nu (mai) îndeplinește funcția de judecător, și să evalueze independența comisarului pentru păstrarea și utilizarea materialelor biometrice și a comisarului pentru camere de supraveghere.**

4.2. Cadrul juridic general privind protecția datelor în domeniul securității naționale

4.2.1. Certificate de securitate națională

138. În conformitate cu articolul 111 din DPA 2018, operatorii pot solicita certificate de securitate națională eliberate de un ministru, de un membru al guvernului, de procurorul general sau de avocatul general în cazul Scoției, care să ateste că derogările de la obligațiile și drepturile consacrate în părțile 4- 6 din DPA 2018 reprezintă o măsură necesară și proporțională pentru protecția securității naționale. Aceste certificate sunt menite să confere operatorilor o mai mare securitate juridică și vor constitui dovezi concludente ale faptului că prelucrarea datelor cu caracter personal face obiectul securității naționale. Cu toate acestea, ar trebui menționat faptul că aceste certificate nu sunt obligatorii în sensul invocării unor derogări în materie de securitate națională, ci reprezintă, mai degrabă, o măsură de transparență[82].

[82] A se vedea Ministerul de Interne, „The Data Protection Act 2018 – National Security Certificates Guidance" (Legea privind protecția datelor din 2018 – Orientări cu privire la certificatele de securitate națională), august 2020, punctul 4, p. 3, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

139. CEPD înțelege din punctele 17 și 18 din anexa 20 la DPA 2018 că un certificat de securitate națională eliberat în temeiul Legii privind protecția datelor din 1998 (denumit în continuare „vechiul certificat") a avut un efect prelungit pentru prelucrarea datelor cu caracter personal în temeiul DPA 2018 până la 25 mai 2019. Până la această dată, cu excepția cazului în care au fost înlocuite sau revocate, vechile certificate au fost tratate ca și cum ar fi fost eliberate în temeiul DPA 2018.

140. Cu toate acestea, în cazul în care un certificat de securitate națională eliberat în temeiul Legii privind protecția datelor din 1998 nu are o dată de expirare explicită, CEPD înțelege că un astfel de certificat va continua să producă efecte în ceea ce privește prelucrarea datelor în temeiul Legii privind protecția datelor din 1998, cu excepția cazului în care respectivul certificat este revocat sau anulat[83]. Deși protecția asigurată de aceste vechi certificate se limitează la prelucrarea datelor cu caracter personal în temeiul Legii privind protecția datelor din 1998, CEPD constată că se pot emite noi certificate de securitate națională în temeiul Legii privind protecția datelor din 1998 pentru datele cu caracter personal care au fost prelucrate în temeiul Legii privind protecția datelor din 1998.[84]

141. **Pentru asigurarea unui caracter cuprinzător, CEPD invită Comisia Europeană să clarifice în proiectul său de decizie faptul că certificatele de securitate națională se pot elibera în continuare în temeiul Legii privind protecția datelor din 1998. În plus, CEPD invită Comisia Europeană să descrie în proiectul său de decizie mecanismele de recurs și de supraveghere în ceea ce privește certificatele eliberate în temeiul Legii privind protecția datelor din 1998. În cele din urmă, CEPD invită Comisia Europeană să includă în proiectul său de decizie numărul de certificate existente eliberate în temeiul Legii privind protecția datelor din 1998 și să monitorizeze cu atenție acest aspect.**

4.2.2. Dreptul la rectificare și la ștergere

142. În ceea ce privește dreptul la rectificare și la ștergere, CEPD ia act de faptul că, în conformitate cu articolele 100 și 149 din DPA 2018, persoanele vizate au posibilitatea de a solicita Înaltei Curți (în Scoția, *Court of Session*) să dispună rectificarea sau ștergerea datelor acestora de către operatori fără întârzieri nejustificate.

143. **CEPD subliniază că exercitarea drepturilor persoanelor vizate trebuie asigurată în mod eficace; prin urmare, CEPD invită Comisia Europeană să descrie în proiectul său de decizie modul în care se aplică articolul 100 din DPA 2018 și să monitorizeze îndeaproape aplicarea acestui articol.**

4.2.3. Derogări în materie de securitate națională

144. CEPD dorește să atragă atenția asupra articolului 110 din DPA 2018 și, în special, asupra anexei 11, care stabilește scopurile specifice în care serviciile de informații se pot abate de la anumite principii

[83] A se vedea Ministerul de Interne, „The Data Protection Act 2018 – National Security Certificates Guidance" (Legea privind protecția datelor din 2018 – Orientări cu privire la certificatele de securitate națională), august 2020, p. 5.
[84] A se vedea Ministerul de Interne, „The Data Protection Act 2018 – National Security Certificates Guidance" (Legea privind protecția datelor din 2018 – Orientări cu privire la certificatele de securitate națională), august 2020, punctul 8, p. 5.

de protecție a datelor, inclusiv în ceea ce privește drepturile persoanelor vizate, și nu sunt obligate să comunice ICO cazurile de încălcare a securității datelor cu caracter personal[85].

145. **CEPD solicită Comisiei Europene să clarifice în continuare domeniul de aplicare al derogărilor, întrucât se întreabă dacă toate derogările prevăzute în anexa 11 la DPA 2018 sunt relevante pentru activitatea serviciilor de informații și dacă acestea asigură echivalența cu principiul necesității și al proporționalității**. În special, **CEPD invită Comisia Europeană să ofere clarificări suplimentare cu privire la circumstanțele în care un serviciu de informații ar putea invoca punctul 10 din anexa 11 la DPA 2018, care prevede că „dispozițiile enumerate nu se aplică datelor cu caracter personal care constau în înregistrări ale intențiilor operatorului în legătură cu orice negocieri cu persoana vizată, în măsura în care aplicarea dispozițiilor enumerate ar putea afecta negocierile".**

4.3. Accesul și utilizarea de către autoritățile publice din Regatul Unit în scopuri de securitate națională

146. 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[86], 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[87]. 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 protecție pentru interpretarea drepturilor corespunzătoare din cartă[88]. 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".

147. 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.

---

[85] Aceste scopuri sunt prevenirea și detectarea „criminalității", „informații care trebuie divulgate prin lege etc. sau în legătură cu procedurile judiciare", „privilegiul parlamentar", „procedurile judiciare", „onoruri și demnități acordate de Coroană", „forțele armate", „bunăstarea economică", „secretul profesional al avocatului", „negocieri", „referințe confidențiale date de operator", „lucrările de examen și notele obținute", „cercetare și statistici" și „arhivarea în interes public".

[86] A se vedea Recomandările 02/2020 ale CEPD privind garanțiile esențiale europene pentru măsurile de supraveghere.

[87] A se vedea hotărârea *Schrems II*, punctul 98.

[88] A se vedea CJUE, cauzele conexate C-511/18, C-512/18 și C-520/18 *La Quadrature du Net și alții*, 6 octombrie 2020, ECLI:EU:C:2020:791, punctul 124.

4.3.1. Temeiuri juridice, limitări și garanții – competențe de investigare exercitate în contextul securității naționale

4.3.1.1. Observații generale

148. CEPD reamintește că IPA 2016 este o lege recentă, prin care s-au modificat o serie de dispoziții ale Legii privind serviciile de informații din 1994. Aceasta stabilește măsura în care pot fi utilizate anumite competențe de investigare pentru a aduce atingere vieții private[89]. În pofida a două rapoarte ale IPC care oferă informații utile privind aplicarea acestui nou cadru juridic, nu există încă o revizuire a anumitor aspecte, în special în ceea ce privește selectorii și criteriile de căutare utilizate.

149. De asemenea, ca observație generală privind IPA 2016 și domeniul său de aplicare, CEPD subliniază următoarele patru puncte de interes:

150. Referitor la primul **punct de interes**, în ceea ce privește caracteristicile legislației, CEPD ar dori să sublinieze două aspecte:

151. În primul rând, CEPD observă că legea respectivă se referă la scopuri generale de utilizare a procedurilor prevăzute în IPA 2016 și nu la categoriile de persoane care pot fi vizate de colectarea de date în baza părților 2-7 din IPA 2016. În această privință, CEPD reamintește că ar trebui să existe o legătură între categoriile de persoane care pot face obiectul măsurilor de supraveghere și scopurile urmărite de legislație pentru a defini domeniul personal de aplicare al legii.

152. În plus, CEPD subliniază că definiția termenilor „operatori de telecomunicații”, „serviciu de telecomunicații” și „sistem de telecomunicații”, care se circumscriu domeniului de aplicare al legii, este, de asemenea, foarte cuprinzătoare și neclară într-o anumită măsură. Într-adevăr, CEPD subliniază că aceste noțiuni, în domeniul IPA 2016, trebuie înțelese într-un mod mult mai cuprinzător decât în cadrul legislației privind telecomunicațiile, astfel cum sunt definite, de exemplu, în Codul european al comunicațiilor electronice[90]. CEPD ia act de faptul că definițiile termenilor „serviciu de telecomunicații” și „sistem de telecomunicații” din lege sunt considerate a fi în mod intenționat cuprinzătoare, astfel încât să rămână relevante pentru noile tehnologii. În mod similar, definiția unui operator de telecomunicații este, de asemenea, foarte cuprinzătoare și ar putea include, de exemplu, jocuri video online cu o funcție de chat sau alte site-uri online care includ doar astfel de ferestre de chat[91].

153. În plus, în timp ce procedurile și supravegherea privind evaluarea necesității și proporționalității colectării și accesului la date sunt, în general, furnizate, criteriile pentru efectuarea unei astfel de

[89] A se vedea articolul 1 din IPA 2016.

[90] A se vedea articolul 2 alineatul (5) din Codul european al comunicațiilor electronice, care definește, de exemplu, „serviciul de comunicații interpersonale” astfel: „un serviciu furnizat de regulă contra cost care permite schimbul direct de informații într-un mod interpersonal și interactiv prin intermediul rețelelor de comunicații electronice între un număr finit de persoane, în cadrul căruia persoanele care inițiază sau participă la comunicare își stabilesc destinatarul (destinatarii) și care nu include serviciile care permit comunicarea interpersonală și interactivă doar ca un simplu element auxiliar minor care este legat în mod intrinsec de un alt serviciu”.

[91] A se vedea Ministerul de Interne, „Interception of Communications Code of Practice” (Codul de practică privind interceptarea comunicațiilor), martie 2018, punctul 2.5 și următoarele, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

evaluări nu sunt definite în legislație. Elemente suplimentare pot fi identificate în alte documente, cum ar fi codurile de practică.

154. Cu toate acestea, astfel cum se reamintește în Recomandările 02/2020 ale CEPD privind garanțiile esențiale europene pentru măsurile de supraveghere, CJUE a indicat că „cerința [...] potrivit căreia orice restrângere a exercitării drepturilor fundamentale să fie prevăzută de lege presupune ca temeiul juridic care permite această ingerință să definească el însuși întinderea restrângerii exercitării dreptului vizat”[92]. Mai precis, CJUE a clarificat faptul că „[p]entru a respecta cerința proporționalității, o reglementare trebuie să prevadă norme clare și precise care să reglementeze conținutul și aplicarea măsurii respective și să impună o serie de cerințe minime astfel încât persoanele ale căror date cu caracter personal sunt vizate să dispună de garanții suficiente care să permită protejarea în mod eficient a acestor date împotriva riscurilor de abuz. Această reglementare trebuie să fie obligatorie din punct de vedere juridic în dreptul intern și în special să indice în ce împrejurări și în ce condiții o măsură care prevede prelucrarea unor asemenea date poate fi luată, garantând în acest mod că o ingerință este limitată la strictul necesar”[93].

155. CEDO a subliniat, de asemenea, importanța clarității legii pentru a „indica [cetățenilor] în mod corespunzător în ce împrejurări și în ce condiții abilitează autoritățile publice să adopte astfel de măsuri”[94].

156. **Prin urmare, CEPD solicită Comisiei Europene să evalueze în continuare aceste aspecte în ceea ce privește precizia, claritatea și exhaustivitatea legislației relevante și să furnizeze elemente suplimentare pentru a demonstra că aceasta oferă un nivel de protecție în esență echivalent cu cel garantat în UE în ceea ce privește caracteristicile legii. CEPD subliniază, de asemenea, că ar trebui evaluate definițiile cuprinzătoare și în ceea ce privește proporționalitatea măsurilor de interceptare.**

157. În plus, deși mai multe coduri interne ale autorităților competente ale serviciilor de informații dezvoltă parțial unele dintre aceste elemente, de exemplu în ceea ce privește evaluarea necesității și a proporționalității colectării datelor, CEPD subliniază că cerințele CJUE în ceea ce privește natura legii implică faptul că elementele esențiale, inclusiv posibilitatea invocării acestora de către persoane în contextul căilor de atac, trebuie să fie prevăzute în legislația care stabilește drepturi ce pot da naștere unei acțiuni în justiție[95]. Într-adevăr, punctul 6 din anexa 7 la IPA 2016 menționează faptul că instanțele (și autoritățile de supraveghere) „țin seama de neluarea în considerare de către o persoană a unui cod atunci când se pronunță asupra unui anumit aspect în cadrul unor astfel de proceduri”, fără a clarifica dacă persoana respectivă poate invoca o încălcare a codurilor în fața instanțelor (sau a autorităților de supraveghere). În plus, elementele furnizate până în prezent în proiectul de decizie se referă fie la recunoașterea de către CEDO a previzibilității normelor

[92] A se vedea hotărârea *Schrems II*, punctul 175 și jurisprudența citată, precum și hotărârea CJUE, C-623/17, *Privacy International/Secretary of State for Foreign and Commonwealth Affairs și alții*, 6 octombrie 2020, ECLI:EU:C:2020:790, (denumită în continuare „hotărârea Privacy International”), punctul 65.

[93] A se vedea hotărârea *Privacy International*, punctul 68.

[94] A se vedea hotărârea CEDO *Zakharov/Rusia*, 4 decembrie 2015, CE:ECHR:2015:1204JUD004714306, punctul 229.

[95] În această privință, CJUE a considerat, de exemplu, că PPD 28 din SUA nu se califică în acest sens, deși prevede, de asemenea, anumite limitări în ceea ce privește colectarea în masă (a se vedea hotărârea Schrems II, punctul 181).

prevăzute[96] în aceste coduri, mai degrabă decât la „posibilitatea acestora de a da naștere unei acțiuni în justiție", astfel cum solicită CJUE, fie la faptul că, în unele cazuri, instanțele din Regatul Unit au făcut trimitere la coduri, în timp ce niciuna dintre cauzele menționate nu ilustrează posibilitatea ca persoanele să înainteze acțiuni în justiție în baza unor drepturi care decurg din coduri. **În cazul în care se concluzionează că legislația Regatului Unit nu indică în mod suficient circumstanțele și condițiile în care poate fi adoptată o măsură și că aceste elemente sunt de fapt furnizate de codurile interne ale autorităților serviciilor de informații**, **CEPD ar solicita astfel Comisiei Europene să evalueze în continuare dacă limitările și garanțiile prevăzute în diferitele coduri interne ale autorităților serviciilor de informații pot da naștere unei acțiuni a unei persoane în fața unei instanțe și pot fi puse în aplicare**.

158. **Al doilea punct de interes** se referă la faptul că dispozițiile care vizează, pe de o parte, obținerea și păstrarea unor date specifice referitoare la comunicații și, pe de altă parte, colectarea în masă, prevăzute fie de IPA 2016, fie de alte acte legislative, cum ar fi Legea privind serviciile de informații din 1994 sau Legea privind reglementarea competențelor de investigare din 2000, se vor aplica, de asemenea, datelor transferate din UE către Regatul Unit. În ceea ce privește colectarea în masă, CEPD subliniază că dispozițiile relevante din legislația Regatului Unit permit colectarea de date în afara Regatului Unit și, prin urmare, ar putea include datele în tranzit transferate din SEE către Regatul Unit pe baza deciziei privind caracterul adecvat al nivelului de protecție[97]. În plus, CEPD observă că, potrivit Comisiei Europene, „[a]r trebui remarcat faptul că păstrarea și obținerea datelor referitoare la comunicații nu se referă, în mod normal, la datele cu caracter personal ale persoanelor vizate din UE transferate în temeiul prezentei decizii către Regatul Unit. Obligația de a păstra sau de a divulga date referitoare la comunicații în temeiul părților 3 și 4 din IPA 2016 se referă la datele care sunt colectate de operatorii de telecomunicații din Regatul Unit direct de la utilizatorii unui serviciu de telecomunicații"[98]. Cu toate acestea, CEPD subliniază lipsa de claritate în ceea ce privește faptul că numai unitățile acestor operatori situate în Regatul Unit pot primi cereri din partea autorităților competente din Regatul Unit, deoarece definiția operatorului de telecomunicații prevăzută la articolul 261 alineatul (10) din IPA 2016 impune ca „un operator de telecomunicații să fie o persoană care oferă sau furnizează un serviciu de telecomunicații unor persoane din Regatul Unit sau care controlează sau furnizează un sistem de telecomunicații care se află (integral sau parțial) în sau este controlat din Regatul Unit". În consecință, datele cu caracter personal ale persoanelor vizate din SEE ar putea face efectiv obiectul unei astfel de situații, de exemplu, în cazul datelor colectate sau generate de o unitate a unui operator de telecomunicații din Regatul Unit situată în SEE, transferate către o unitate a aceluiași operator situată în Regatul Unit pe baza deciziei privind caracterul adecvat al nivelului de protecție (în scopuri comerciale) și apoi colectate, în Regatul Unit, de către autoritățile publice competente.

[96] A se vedea hotărârea CEDO *Big Brother Watch și alții/Regatul Unit*, 13 septembrie 2018, ECLI:CE:ECHR:2018:0913JUD005817013 (denumită în continuare „hotărârea Big Brother Watch"), punctul 325: „Întrucât Codul IC este un document public, făcând obiectul aprobării ambelor camere ale Parlamentului, și trebuie luat în considerare atât de către cei care exercită atribuții de interceptare, cât și de către instanțe, Curtea a acceptat în mod expres că dispozițiile acestuia ar putea fi luate în considerare la evaluarea previzibilității regimului Legii privind reglementarea competențelor de investigare (RIPA)."

[97] A se vedea punctul 183 și următoarele din hotărârea *Schrems II* privind evaluarea unei măsuri care prevede accesul la datele în tranzit între UE și o țară terță în contextul unei decizii privind caracterul adecvat al nivelului de protecție.

[98] A se vedea considerentul 196 din proiectul de decizie.

159. **Prin urmare, CEPD este de părere că evaluarea acestor dispoziții este, de asemenea, relevantă pentru evaluarea nivelului de adecvare a cadrului juridic din Regatul Unit și invită Comisia Europeană să clarifice acest aspect și să evalueze în continuare în ce măsură acest lucru este valabil. În special, CEPD solicită Comisiei Europene să clarifice modul în care înțelege domeniul de aplicare al acestei legislații, inclusiv în ceea ce privește noțiunea de „utilizatori de servicii de telecomunicații", și dacă ar putea fi solicitate date de la unități ale operatorilor de telecomunicații din afara Regatului Unit, în măsura în care sunt avute în vedere datele persoanelor vizate din SEE, ținând seama de definiția foarte cuprinzătoare a operatorilor de telecomunicații.**

160. **Al treilea punct de interes** se referă la procedura de „protecție dublă". CEPD ia act de faptul că o nouă procedură de „protecție dublă" a fost introdusă în IPA 2016. Cu toate acestea, CEPD înțelege, de asemenea, că, deși, în principiu, colectarea datelor sau accesul la acestea în scopuri de securitate națională sau de colectare de date operative poate avea loc numai cu un mandat aprobat de un comisar judiciar, IPA 2016 prevede că „în anumite cazuri limitate este posibilă interceptarea legală fără mandat și este necesară numai autorizarea prealabilă din partea autorităților competente IC [a se vedea secțiunea de mai jos privind supravegherea], inclusiv pentru interceptări în conformitate cu cererile din străinătate (articolul 52 din IPA 2016)". După cum se subliniază în continuare, acest lucru este, de asemenea, în concordanță cu îngrijorarea exprimată de CEPD în ceea ce privește, în special, divulgările în străinătate. În plus, CEPD observă, de asemenea, că, în ceea ce privește intervențiile asupra echipamentelor, indiferent dacă acestea vizează date specifice sau colectarea în masă, este posibilă și o derogare de la procedura de protecție dublă, iar comisarul judiciar are dreptul să aprobe numai reînnoirea mandatelor de colectare în masă după o perioadă inițială de maximum șase luni. **CEPD solicită Comisiei Europene să evalueze în continuare și să demonstreze că, chiar și în cazurile în care nu se aplică procedura de protecție dublă, cadrul juridic din Regatul Unit oferă garanții adecvate, inclusiv prin intermediul unei supravegheri *ex post* și al unor căi de atac eficace aflate la dispoziție persoanelor, asigurând astfel un nivel de protecție în esență echivalent cu cel oferit la nivelul UE (a se vedea, de asemenea, secțiunea 4.3.3 de mai jos privind supravegherea).**

161. În plus, deși IPA 2016 a introdus, într-adevăr, procedura de „protecție dublă", CEPD rămâne preocupat de anumite caracteristici ale noii legislații. În urma prezentării secțiunilor corespunzătoare din proiectul de decizie, CEPD a analizat următoarele tipuri de colectare și acces la date în aceeași ordine precum cea prezentată de Comisia Europeană. Prin urmare, ordinea elementelor evaluate în continuare nu reflectă o ierarhie în ceea ce privește nivelul de îngrijorare al CEPD.

4.3.1.2. Obținerea și păstrarea unor date specifice referitoare la comunicații

162. CEPD observă că există doi funcționari care pot acorda autorizații specifice pentru obținerea datelor referitoare la comunicații: funcționarul responsabil cu autorizarea din cadrul Oficiului pentru autorizațiile privind datele referitoare la comunicații (denumit în continuare „IPC"), un responsabil superior desemnat (o persoană care deține o funcție sau un rang stabilit într-o autoritate publică relevantă), în plus față un comisar judiciar, care acordă astfel de aprobări în anumite cazuri. Cu toate acestea, rămâne neclar pentru CEPD, în temeiul legii și al codului relevant,

exact ce funcționar autorizează ce tip de obținere a unor date specifice referitoare la comunicații și în ce măsură un funcționar desemnat ar fi suficient de independent[99].

163. **În consecință, CEPD solicită Comisiei Europene să evalueze în continuare acest aspect și să ofere explicații mai clare cu privire la aceste elemente.**

164. În ceea ce privește notificarea prin care se solicită păstrarea datelor referitoare la comunicații, CEPD observă, de asemenea, că astfel de notificări pot viza o „descriere a operatorilor". Această noțiune pare să însemne că mai multor operatori li se poate solicita în același timp să păstreze toate datele. Într-adevăr, caracterul specific al operațiunii de obținere a datelor nu se referă la numărul de operatori, ci la numele sau descrierea persoanelor, a organizațiilor, a amplasamentului sau a grupului de persoane care constituie „ținta" vizată, la o descriere a naturii investigației și la o descriere a activităților pentru care este utilizat echipamentul. Prin urmare, CEPD subliniază că, în funcție de numărul de operatori vizați de o astfel de „categorie de operatori", notificarea poate fi mai cuprinzătoare decât ceea ce ar putea părea să implice procedura specifică de păstrare a datelor. **CEPD invită Comisia Europeană să evalueze în continuare acest aspect și să ofere asigurări suplimentare că, chiar și atunci când notificările se adresează mai multor operatori, acestea rămân limitate la ceea ce este strict necesar și proporțional.**

4.3.1.3. Intervențiile asupra echipamentelor

165. CEPD observă că, în situații de urgență, „intervențiile asupra echipamentelor" se pot abate de la procedura de protecție dublă[100]. Prin urmare, CEPD este preocupat de faptul că scopurile în care se poate solicita o intervenție asupra echipamentelor sunt ample, iar criteriile prin care se stabilește situația de urgență (în care caz comisarul judiciar nu are obligația de a furniza o autorizare *ex ante* în urma evaluării necesității și a proporționalității operațiunii de intervenție asupra echipamentelor) rămân neclare. Întrucât, în această din urmă situație, „mandatul încetează să mai producă efecte și nu poate fi reînnoit", în cazul în care comisarul judiciar nu aprobă *ex post* intervenția asupra echipamentelor, CEPD înțelege că datele colectate între timp sunt considerate colectate în mod legal. Pentru ca aceste date să fie șterse, comisarul judiciar poate emite un ordin specific[101].

166. **CEPD solicită Comisiei Europene să evalueze în continuare condițiile în care poate fi invocată o situație de urgență și să ofere clarificări cu privire la posibilele căi de exercitare a drepturilor persoanelor vizate în cauză și la posibilele căi de atac care le sunt oferite în contextul operațiunilor de intervenție asupra echipamentelor, în special atunci când acestea au loc în contextul unei situații de urgență care conduce la o derogare de la procedura de protecție dublă.**

4.3.1.4. Interceptarea în masă a datelor de la purtători

167. Astfel cum se descrie în raportul în urma evaluării competențelor de interceptare în masă[102] „[b]interceptarea în masă implică, de regulă, colectarea comunicațiilor pe măsură ce acestea tranzitează anumiți purtători (conexiuni de comunicare)". Fișa informativă oficială a IPA 2016 descrie „interceptarea în masă" drept „procesul de colectare a unui volum de comunicații, urmat

[99] A se vedea, de asemenea, considerațiile de mai jos privind evaluarea procedurii de protecție dublă și independența comisarului judiciar.
[100] A se vedea articolul 109 din IPA 2016.
[101] A se vedea articolul 110 alineatul (3) litera (b) din IPA 2016.
[102] A se vedea raportul intitulat „Report of the bulk powers review" (Raport în urma evaluării competențelor de interceptare în masă), realizat de evaluatorul independent al legislației privind terorismul, august 2016.

de selectarea unor comunicații specifice, care urmează să fie citite, vizualizate sau ascultate, în măsura în care acest lucru este necesar și proporțional". CEPD observă că „interceptarea în masă" a datelor presupune, de fapt, colectarea acestora chiar înainte de aplicarea vreunor filtre de către selectori (fie simple, în contextul monitorizării persoanelor cunoscute deja ca reprezentând o amenințare, fie complexe, în contextul identificării unor noi amenințări sau a unor persoane de interes necunoscute anterior).

168. Obținerea în masă a datelor referitoare la comunicații a fost, de asemenea, unul dintre aspectele examinate de CJUE în cauza Privacy International, care a condus la pronunțarea unei hotărâri a Marii Camere la 6 octombrie 2020 (în plus față de faptul dacă o astfel de colectare de date a fost efectuată în contextul dreptului Uniunii, chiar și în scopuri de securitate națională). IPA 2016 a înlocuit legislația care a făcut obiectul acestei hotărâri.

169. CEPD ia act de faptul că, odată cu introducerea IPA 2016 în legislația Regatului Unit, în prezent este necesar un mandat de interceptare în masă a datelor. Procesul de emitere a acestui mandat se bazează pe stabilirea unor „scopuri operaționale". Lista acestor scopuri operaționale este stabilită de șefii serviciilor de informații și apoi aprobată de secretarul de stat. Decizia în acest sens este aprobată, la rândul său, de un comisar judiciar independent, care trebuie să verifice dacă mandatul este necesar și proporțional cu scopurile operaționale. CEPD înțelege că respectivul comisar judiciar nu are competența de a evalua scopurile operaționale în sine, ci dacă mandatul este necesar și proporțional cu scopurile operaționale enumerate în mandat. Comitetul parlamentar pentru informații și securitate primește o copie a listei o dată la trei luni, iar prim-ministrul revizuiește lista scopurilor operaționale cel puțin o dată pe an.

170. Cu toate acestea, pe baza elementelor furnizate de Comisia Europeană în proiectul de decizie, pare dificil să se evalueze domeniul de aplicare al acestor scopuri operaționale prevăzute în listă și dacă respectiva colectare a datelor pe care o permit respectă pragul stabilit de CJUE (de exemplu, circumscrierea colectării datelor la o zonă geografică ar putea să vizeze o suprafață restrânsă de câteva străzi, însă și colectarea de date din întregul SEE).

171. În plus, CEPD subliniază faptul că datele colectate în masă pot fi păstrate pe perioade lungi (pentru a fi disponibile pentru acces ulterior în vederea examinării). Într-adevăr, CEPD observă că articolul 150 alineatele (5) și (6) din IPA 2016 prevede numai distrugerea copiilor datelor colectate și numai în cazul în care păstrarea acestora nu este necesară sau nu este probabil să devină necesară în interesul securității naționale sau în baza oricăror alte motive care intră sub incidența articolului 138 alineatul (2) din IPA 2016 sau dacă păstrarea lor nu este necesară în alte scopuri[103]. CEPD subliniază că aceste motive par foarte cuprinzătoare și, în orice caz, este vorba doar de copii ale datelor obținute.

172. În plus, CEPD observă că, în situații de urgență, IPA 2016 permite, de asemenea, modificarea mandatelor fără aprobarea prealabilă a unui comisar judiciar și că, în cazul în care comisarul judiciar consultat *ex post* în termen de trei zile lucrătoare de la data modificării refuză să aprobe modificarea, mandatul ar trebui să producă efecte ca și cum modificarea respectivă nu ar fi fost efectuată, însă datele colectate între timp sunt considerate colectate în mod legal[104]. Pentru ca aceste date să fie șterse, comisarul judiciar poate emite un ordin specific[105].

[103] A se vedea articolul 150 alineatele (3) și (6) din IPA 2016.
[104] A se vedea articolul 147 din IPA 2016 (partea 6, capitolul I).
[105] A se vedea articolul 181 alineatul (3) litera (b) din IPA 2016.

173. **Prin urmare, CEPD solicită Comisiei Europene clarificări și evaluări suplimentare cu privire la interceptarea în masă, în special cu privire la selectarea și aplicarea selectorilor în contextul acestor proceduri de interceptare în masă, pentru a clarifica măsura în care accesul la datele cu caracter personal respectă pragul stabilit de CJUE (a se vedea, de asemenea, secțiunea 4.3.1.7 de mai jos, în special cu privire la supravegherea selectorilor) și ce garanții sunt instituite pentru a proteja drepturile fundamentale ale persoanelor ale căror date sunt interceptate în acest context, inclusiv în ceea ce privește perioadele de păstrare a datelor. O evaluare independentă din partea autorităților de supraveghere competente din Regatul Unit ar fi deosebit de utilă.**

174. **CEPD subliniază, de asemenea, că este cu atât mai important faptul că termenul de „comunicații transmise din/primite în străinătate" care intră în domeniul de aplicare al practicilor de interceptare în masă pare să sugereze că datele ar putea fi interceptate în mod direct și colectate în masă în SEE de către Regatul Unit, inclusiv în ceea ce privește datele în tranzit între SEE și Regatul Unit, care ar intra în domeniul de aplicare al proiectului de decizie (a se vedea secțiunea 4.3.2. de mai jos cu privire la utilizarea ulterioară a informațiilor colectate în scopuri de securitate națională și divulgările în străinătate).**

4.3.1.5. Protecția și garanțiile în ceea ce privește datele secundare

175. În plus, CEPD este preocupat de faptul că legislația relevantă din Regatul Unit privind interceptarea în masă nu prevede același nivel de protecție pentru toate datele referitoare la comunicații. „Datele secundare", care pot fi obținute printr-un mandat de interceptare în masă, reprezintă, în conformitate cu articolul 137 din IPA 2016, atât „datele privind sistemele" – „date conținute de, incluse în, atașate sau asociate logic comunicației (de către expeditor sau în alt mod)", cât și „datele de identificare" – „date conținute de, incluse în, atașate sau asociate logic comunicației (de către expeditor sau în alt mod), care pot fi separate logic de restul comunicației și care, în cazul unei astfel de separări, nu ar dezvălui nicio informație ce ar putea fi considerată în mod rezonabil drept înțeles al comunicației (dacă acesta există), fără a ține seama de vreun înțeles care ar putea rezulta din transmiterea însăși a comunicației sau din orice fel de date care au legătură cu transmiterea comunicației"[106].

176. CEPD observă că aceste „date secundare", cunoscute și sub denumirea de „metadate"[107], colectate în masă, par să nu beneficieze de aceleași garanții precum datele colectate cu mandat specific sau datele referitoare la conținut colectate în masă. Într-adevăr, CEPD constată că selectarea oricărui conținut interceptat beneficiază de mai multe garanții[108] decât selectarea datelor secundare[109].

177. În plus, CEPD subliniază că atât CEDO[110], cât și CJUE[111] au pus sub semnul întrebării faptul că astfel de date sunt mai puțin sensibile decât alte date, în special decât datele referitoare la conținut.

[106] „Datele privind sistemele" și „datele de identificare" sunt definite în articolul 263 din IPA 2016.
[107] A se vedea raportul intitulat „Report of the bulk powers review" (Raport în urma evaluării competențelor de interceptare în masă), realizat de evaluatorul independent al legislației privind terorismul, august 2016.
[108] A se vedea articolul 152 alineatul (1) litera (c) și alineatul (3) și următoarele din IPA 2016.
[109] A se vedea articolul 152 alineatul (1) literele (a) și (b) din IPA 2016.
[110] A se vedea hotărârea CEDO *Big Brother Watch*, punctul 357, cauză în curs de examinare de Marea Cameră: „În consecință, deși Curtea nu are îndoieli cu privire la faptul că datele conexe referitoare la comunicații reprezintă un instrument esențial pentru serviciile de informații în combaterea terorismului și a infracțiunilor grave, aceasta nu consideră că autoritățile au găsit un echilibru just între interesele publice și cele private concurente prin aplicarea unei derogări integrale în ceea ce privește garanțiile aplicabile căutării și examinării conținutului. Deși Curtea nu sugerează că datele conexe referitoare la comunicații ar trebui să fie accesibile numai pentru a stabili dacă o persoană se află sau nu în Insulele Britanice, întrucât acest lucru ar

Într-adevăr, Codul de practică privind interceptarea comunicațiilor prezintă ca exemple de „date secundare” (atât „datele privind sistemele”, cum ar fi configurațiile de router, adresele de e-mail sau ID-ul utilizatorilor, dar și identificatorii alternativi de cont, cât și „datele de identificare”, cum ar fi locul de desfășurare a unei reuniuni pentru care există o programare în calendar, informații referitoare la fotografii, cum ar fi ora, data și locul în care au fost făcute). **Prin urmare, CEPD subliniază aprecierea consecventă în acest sens a CEDO și CJUE și reamintește preocupările exprimate în legătură cu datele secundare, care ar trebui să beneficieze de garanții specifice, având în vedere caracterul lor sensibil. Prin urmare, CEPD solicită Comisiei Europene să evalueze cu atenție dacă garanțiile prevăzute de legislația Regatului Unit pentru o astfel de categorie de date cu caracter personal asigură un nivel de protecție în esență echivalent cu cel garantat în UE.**

4.3.1.6. Prelucrarea automată a datelor referitoare la comunicații

178. CEPD ia act de faptul că autoritățile serviciilor de informații nu numai că utilizează selectori simpli sau complecși pentru a filtra datele obținute în masă, ci se pot baza și pe alte instrumente de prelucrare automată pentru a analiza „volume mari de informații, ceea ce permite agențiilor să identifice, de asemenea, legături, modele, asociații sau comportamente care ar putea demonstra o amenințare gravă ce trebuie investigată”, în conformitate cu raportul din 2015 al Comitetului pentru informații și securitate[112]. **CEPD cunoaște faptul că acest raport public se referă la practici din cadrul juridic anterior, care a fost înlocuit ulterior de IPA 2016. Cu toate acestea, CEPD consideră că este nevoie de o evaluare și o supraveghere independentă suplimentară a utilizării instrumentelor de prelucrare automată a datelor de către autoritățile de supraveghere competente din Regatul Unit și invită Comisia Europeană să evalueze în continuare acest aspect, precum și garanțiile care ar fi acordate și/sau care ar putea fi acordate persoanelor vizate din SEE în acest context**.

4.3.1.7. Riscuri de conformitate și practici neconforme ale autorităților competente ale serviciilor de informații

179. CEPD ia act de faptul că sunt disponibile rapoarte detaliate de supraveghere. Acestea oferă elemente valoroase cu privire la ceea ce se evaluează ca reprezentând practici pozitive în materie de conformitate, precum și cu privire la riscurile de conformitate și practicile neconforme identificate.

însemna să se impună aplicarea unor standarde mai stricte în cazul datelor conexe referitoare la comunicații decât cele aplicabile conținutului, ar trebui totuși să existe suficiente garanții pentru a se asigura că derogarea aplicată în cazul datelor conexe referitoare la comunicații de la cerințele articolului 16 din RIPA este limitată la măsura necesară pentru a stabili dacă o persoană se află, pentru moment, în Insulele Britanice.”

[111] A se vedea hotărârea CJUE, *Privacy International*, punctul 71: „Ingerința pe care o implică transmiterea datelor de transfer și a datelor de localizare pentru agențiile de securitate și de informații în dreptul consacrat la articolul 7 din cartă trebuie considerată deosebit de gravă, ținând seama în special de caracterul sensibil al informațiilor pe care le pot furniza aceste date și în special de posibilitatea de a stabili pe baza acestora profilul persoanelor în cauză, o asemenea informație fiind la fel de sensibilă ca și conținutul însuși al comunicațiilor. În plus, aceasta este susceptibilă să genereze în mintea persoanelor vizate sentimentul că viața lor privată face obiectul unei supravegheri constante (a se vedea prin analogie Hotărârea din 8 aprilie 2014, Digital Rights Ireland și alții, C-293/12 și C-594/12, EU:C:2014:238, punctele 27 și 37, precum și Hotărârea din 21 decembrie 2016, Tele2, C-203/15 și C-698/15, EU:C:2016:970, punctele 99 și 100).”

[112] Comitetul pentru informații și securitate al Parlamentului, „Privacy and Security: A modern and transparent legal framework (Confidențialitate și securitate: un cadru juridic modern și transparent), 2015, punctul 18, p. 13, https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf.

180. În această privință, potrivit raportului IPC pentru anul 2019, mai multe elemente referitoare la aplicarea cadrului juridic de către diferitele autorități competente au evidențiat unele (riscuri de) neconformități la nivelul autorităților competente.

181. În primul rând, CEPD a observat că criteriile de clasificare a unui set de date ca date cu caracter personal care fac obiectul unei interceptări în masă sau ca date care fac obiectul unei interceptări specifice nu par să fie întotdeauna clare chiar pentru MI5 și SIS, în special pentru MI5, ceea ce poate duce la absența unor garanții adecvate aplicate datelor[113]. În raportul său din 2019, IPC a sugerat că „această chestiune ar trebui soluționată cu prioritate”[114]. De asemenea, în ceea ce privește seturile de date cu caracter personal care fac obiectul unei interceptări în masă, CEPD remarcă faptul că, pentru GCHQ, deși clasificarea seturilor de date cu caracter personal care fac obiectul unei interceptări în masă pare să fie satisfăcătoare (dar încă nu a fost auditată de către IPC), în martie 2019, evaluarea internă a conformității mandatelor de către echipa alocată în acest sens a generat preocupări serioase, 50 % din justificările pentru mandatele de obținere de date în masă care au fost examinate de echipa de verificare a conformității GCHQ neîndeplinind standardul necesar. Potrivit IPC, echipa de verificare a conformității și-a început activitatea de investigare a acestei chestiuni și a demarat activități de recalificare a personalului în vederea îmbunătățirii acestui standard. Formarea actualizată cu privire la dispozițiile IPA 2016 și formarea suplimentară oferită de rețelele de politici și de conformitate (denumite în continuare „PCN”) au îmbunătățit conformitatea GCHQ în acest domeniu. IPC nu se așteaptă la o scădere a acestui standard în cadrul verificărilor viitoare, însă va continua să examineze îndeaproape aceste aspecte[115]. **Prin urmare, CEPD împărtășește opinia potrivit căreia este necesară o revizuire și o monitorizare suplimentară a elementelor menționate de către Comisia Europeană în cadrul evaluării nivelului de protecție pentru a asigura îmbunătățirea acestui standard, astfel cum se subliniază în raportul IPC, și reamintește că punerea în aplicare și aplicarea concretă a cadrului juridic trebuie, de asemenea, să fie luate în considerare, astfel cum se prevede la articolul 45 din RGPD, atunci când se evaluează echivalența în esență a unei țări terțe.**

182. În sens mai larg, CEPD subliniază punctele de interes împărtășite de IPC în ceea ce privește „căutările bazate pe sarcini” desfășurate de agenții MI5 – care permit unui anchetator să efectueze

[113] A se vedea „Annual Report of the Investigatory Powers Commissioner 2019” (Raportul anual al comisarului pentru utilizarea competențelor de investigare – 2019), 15 decembrie 2020, punctul 8.39, https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf: „Am observat evoluția pozitivă a [Comisiei de supraveghere a interceptării în masă a datelor (BOP)] și am luat act de impactul acesteia asupra gestionării conformității interne. Avem în continuare nevoie de clarificări suplimentare în ceea ce privește procesul utilizat de MI5 pentru a efectua examinări inițiale ale seturilor noi de date pentru a înțelege mai bine deciziile de clasificare a unui set de date ca date care fac obiectul unei interceptări în masă sau, de exemplu, ca date care fac obiectul unei interceptări specifice. Ne exprimăm îngrijorarea în legătură cu o acțiune nesoluționată din procesul-verbal al BOP în ceea ce privește soluționarea discrepanțelor de alocare a datelor care fac obiectul unei interceptări în masă la nivelul MI5 și SIS. Este posibil ca, din cauza utilizărilor diferite ale datelor și a eliminărilor diferite operate asupra datelor deținute, ambele agenții să dețină același set de date sau versiuni ale acestuia și ca acesta să fie clasificat în mod legal ca făcând obiectul unei interceptări în masă de către una dintre agenții și ca făcând obiectul unei interceptări specifice de către cealaltă. În cazul în care una dintre agenții a clasificat în mod incorect deținerile de date ca făcând obiectul unei interceptări specifice, există riscul ca acestea să fie deținute fără un mandat corespunzător și să nu fie vizate de garanții adecvate.”

[114] A se vedea „Annual Report of the Investigatory Powers Commissioner 2019” (Raportul anual al comisarului pentru utilizarea competențelor de investigare – 2019), punctul 8.39.

[115] A se vedea „Annual Report of the Investigatory Powers Commissioner 2019” (Raportul anual al comisarului pentru utilizarea competențelor de investigare – 2019), punctul 10.48.

mai multe căutări în seturile disponibile de date cu caracter personal care fac obiectul unei interceptări în masă, precum și „riscurile grave de conformitate asociate cu anumite medii tehnologice utilizate de MI5", cu privire la locul în care au fost stocate datele în mediul respectiv, persoanele care au avut acces la acestea, măsura în care acestea au fost copiate sau partajate, procesele de ștergere care li s-au aplicat, precum și perioadele de păstrare. Deși IPC indică faptul că au fost luate măsuri și că au fost introduse garanții, unele dintre acestea continuă să se desfășoare manual și individual, cu implicarea resurselor umane, subliniind că este esențial ca „MI5 să continue să mențină aceste noi procese și să furnizeze suficiente resurse pentru ca ele să funcționeze în mod eficace. În cazul în care MI5 identifică o creștere a comportamentelor neconforme"[116], IPC preconizează că acestea i se vor aduce la cunoștință cât mai curând posibil. **Prin urmare, CEPD solicită Comisiei Europene să monitorizeze îndeaproape aceste aspecte în viitor**.

183. În ceea ce privește GCHQ, CEPD înțelege, de asemenea, din raportul IPC că, pentru operațiunile desfășurate în temeiul mandatelor de interceptare în masă, „calitatea cererilor de aprobare internă a fost variabilă și s-a observat că pot fi aduse îmbunătățiri în ceea ce privește modul în care au fost realizate astfel de cereri"[117], precum și că, în ceea ce privește intervențiile specifice asupra echipamentelor, explicațiile pentru utilizarea descriptorilor generali sunt uneori prea generale și imprecise[118]. CEPD a observat, de asemenea, că, în contextul intervențiilor în masă asupra echipamentelor, IPC recomandă ca „astfel de cereri să înregistreze în mod consecvent și explicit legătura dintre aspectul vizat, scopul statutar și cerințele în materie de informații"[119] și ca „toate cererile să abordeze în mod clar potențialul de intruziune colaterală și măsurile de atenuare relevante atunci când se evaluează proporționalitatea"[120], precum și că IPC a subliniat că, în pofida progreselor înregistrate, „se mai pot aduce îmbunătățiri"[121], fiind necesar să se acorde atenție în continuare acestor aspecte și în viitor.

184. În ceea ce privește regimul aplicabil interceptării în masă în temeiul Legii privind reglementarea competențelor de investigare din 2000 (denumită în continuare „RIPA 2000"), care a fost înlocuit între timp de dispoziții ale IPA 2016, CEPD reamintește că supravegherea insuficientă, atât a selecției purtătorilor de internet pentru interceptare, cât și a filtrării, a căutării și a selectării comunicațiilor interceptate în vederea examinării, a fost unul dintre aspectele esențiale pe care CEDO le-a considerat neconforme cu articolul 8 din Convenția europeană a drepturilor omului în ceea ce privește legislația anterioară privind competențele de investigare ale autorităților din Regatul Unit în contextul cauzei *Big Brother Watch*, în prezent în curs de examinare de Marea Cameră. **CEPD invită Comisia Europeană să verifice stadiul procedurilor, să țină seama de aceste**

[116] A se vedea „Annual Report of the Investigatory Powers Commissioner 2019" (Raportul anual al comisarului pentru utilizarea competențelor de investigare – 2019), punctul 8.52.
[117] A se vedea „Annual Report of the Investigatory Powers Commissioner 2019" (Raportul anual al comisarului pentru utilizarea competențelor de investigare – 2019), punctul 10.2.
[118] A se vedea „Annual Report of the Investigatory Powers Commissioner 2019" (Raportul anual al comisarului pentru utilizarea competențelor de investigare – 2019), punctele 10.16 și 10.17.
[119] A se vedea „Annual Report of the Investigatory Powers Commissioner 2019" (Raportul anual al comisarului pentru utilizarea competențelor de investigare – 2019), punctul 10.23.
[120] A se vedea „Annual Report of the Investigatory Powers Commissioner 2019" (Raportul anual al comisarului pentru utilizarea competențelor de investigare – 2019), punctul 10.23.
[121] A se vedea „Annual Report of the Investigatory Powers Commissioner 2019" (Raportul anual al comisarului pentru utilizarea competențelor de investigare – 2019), punctul 10.23.

elemente și să le specifice în decizia privind caracterul adecvat al nivelului de protecție, în cazul în care Comisia Europeană va adopta o astfel de decizie.

185. În acest caz, CEDO: „nu a fost convinsă că garanțiile care reglementează selecția purtătorilor pentru interceptare și selectarea materialului interceptat pentru examinare sunt suficient de solide pentru a oferi garanții adecvate împotriva abuzurilor. Cel mai semnificativ motiv de îngrijorare îl reprezintă însă absența unei supravegheri independente solide a selectorilor și a criteriilor de căutare utilizate pentru filtrarea comunicațiilor interceptate."[122] Astfel cum subliniază IPC, „această constatare se regăsește într-o recomandare similară din raportul Comitetului pentru securitate și informații intitulat „Privacy and Security: A modern and transparent legal framework 2015"[123] (Confidențialitate și securitate: un cadru juridic modern și transparent – 2015). **CEPD salută faptul că, în consecință, IPC a efectuat o revizuire a abordării sale privind verificarea practicilor de interceptare în masă în 2019, „care a inclus o revizuire atentă a modalităților complexe din punct de vedere tehnic de punere efectivă în aplicare a interceptării în masă"[124] și s-a angajat să includă „o examinare detaliată a selectorilor și a criteriilor de căutare menționate de CEDO și la care se face referire în cele de mai sus"[125] în verificările practicilor de interceptare în masă începând cu 2020. Având în vedere importanța acestui aspect, CEPD își exprimă îngrijorarea cu privire la faptul că IPC nu a efectuat încă o examinare detaliată a selectorilor și a criteriilor de căutare și invită Comisia Europeană să monitorizeze îndeaproape evoluțiile în acest sens, în special având în vedere că formatul concret al unei astfel de supravegheri nu a fost clarificat încă[126].**

4.3.2. Utilizarea ulterioară a informațiilor colectate în scopuri de securitate națională și divulgările în străinătate

186. În ceea ce privește utilizarea ulterioară a informațiilor colectate în scopuri de securitate națională, Comisia Europeană face trimitere, în evaluarea sa, la articolul 87 alineatul (1) din DPA 2018, care prevede într-adevăr că „datele cu caracter personal astfel colectate nu trebuie prelucrate într-un mod incompatibil cu scopul pentru care sunt colectate". Cu toate acestea, CEPD subliniază că dispoziția respectivă poate face obiectul unor derogări în materie de securitate națională, în conformitate cu articolul 110 din DPA 2018. În plus, CEPD observă că, indiferent dacă este vorba de interceptarea și examinarea unor date specifice, obținerea și păstrarea unor date specifice referitoare la comunicații, intervențiile specifice asupra echipamentelor sau interceptarea în masă și intervențiile în masă asupra echipamentelor, legislația prevede posibilitatea „divulgării în străinătate" a datelor.

4.3.2.1. Utilizare ulterioară, divulgare în străinătate și cadrul juridic aplicabil în Regatul Unit

187. Comisia Europeană a identificat partea 4 din DPA 2018 și, în special, articolul 109 drept dispozițiile relevante care stabilesc cerințe specifice pentru utilizarea ulterioară a informațiilor colectate și, în

[122] A se vedea hotărârea CEDO *Big Brother Watch*, punctul 347.
[123] A se vedea „Annual Report of the Investigatory Powers Commissioner 2019" (Raportul anual al comisarului pentru utilizarea competențelor de investigare – 2019), punctul 10.28.
[124] A se vedea „Annual Report of the Investigatory Powers Commissioner 2019" (Raportul anual al comisarului pentru utilizarea competențelor de investigare – 2019), punctul 10.28.
[125] A se vedea „Annual Report of the Investigatory Powers Commissioner 2019" (Raportul anual al comisarului pentru utilizarea competențelor de investigare – 2019), punctul 10.28.
[126] A se vedea „Annual Report of the Investigatory Powers Commissioner 2019" (Raportul anual al comisarului pentru utilizarea competențelor de investigare – 2019), punctul 10.28: „formatul exact al acestei verificări nu a fost convenit încă".

special, pentru transferul internațional de date cu caracter personal de către serviciile de informații către țări terțe sau organizații internaționale. Cu toate acestea, CEPD observă că articolul 110 din DPA 2018 prevede o derogare în materie de securitate națională, specificând că anumite dispoziții ale DPA 2018 nu se aplică în cazul în care derogarea de la aceste dispoziții este necesară în scopul protejării securității naționale. Dispozițiile în cauză care pot să nu se aplice includ capitolul 2 din partea 4 din DPA 2018 în legătură cu principiile de protecție a datelor, inclusiv limitarea scopului, precum și capitolul 3 din partea 4 din DPA 2018 în ceea ce privește drepturile persoanelor vizate. Articolul 109 din DPA 2018, coroborat cu articolul 110 din DPA 2018 și condițiile sale de aplicare, poate conduce la situații în care serviciile de informații efectuează un transfer internațional de date cu caracter personal către țări terțe, fără a aplica dispoziții referitoare la principiile de protecție a datelor și la drepturile persoanelor vizate.

188. Astfel, potrivit celor identificate de Comisia Europeană, această derogare trebuie să fie evaluată de la caz la caz și poate fi invocată numai în măsura în care aplicarea unei anumite dispoziții ar avea consecințe negative pentru securitatea națională. Într-adevăr, eliberarea unui certificat național pentru serviciile de informații din Regatul Unit are ca scop certificarea faptului că este necesară o derogare în ceea ce privește anumite date cu caracter personal care sunt prelucrate în scopul protejării securității naționale. Cu toate acestea, CEPD observă că, în orientările sale privind certificatul de securitate națională în temeiul DPA 2018, Ministerul de Interne al Regatului Unit clarifică faptul că „[e]ste important să se remarce de la început că nu este necesar un certificat pentru a se invoca derogarea în materie de securitate națională; de fapt, în majoritatea cazurilor, operatorii vor stabili singuri dacă este aplicabilă derogarea în materie de securitate națională.” [127] În plus, orientările Ministerului de Interne al Regatului Unit precizează că „aceste certificate de securitate națională se pot aplica datelor cu caracter personal care pot fi identificate în mod specific sau care acoperă o categorie mai largă de date cu caracter personal. Ele pot fi emise atât în avans, cât și retroactiv.” [128] Prin urmare, se poate aplica o derogare în materie de securitate națională în legătură cu un transfer internațional de date cu caracter personal realizat de către serviciile de informații către țări terțe în absența unui certificat de securitate națională.

189. De asemenea, CEPD constată că, de exemplu, certificatul național de securitate DPA/S27/Security Service[129] prevede că, până la 24 iulie 2024, datele cu caracter personal prelucrate „pentru, în numele, la cererea sau cu ajutorul sau asistența Serviciului de Securitate sau” și „în cazul în care o astfel de prelucrare este necesară pentru a facilita îndeplinirea corespunzătoare a funcțiilor Serviciului de Securitate descrise în articolul 1 din Legea privind serviciile de securitate din 1989” fac obiectul unei derogări de la dispozițiile din legislația Regatului Unit care corespund capitolului V din RGPD în ceea ce privește transferurile de date cu caracter personal către țări terțe sau organizații internaționale. Deși celelalte certificate naționale de securitate disponibile publicului nu prevăd o derogare de la dispozițiile articolului 109 din DPA 2018, trebuie reamintit faptul că o parte din sau întregul text al unui certificat de securitate național poate fi confidențial, în cazul în care

[127] A se vedea Ministerul de Interne, „The Data Protection Act 2018 – National Security Certificates Guidance” (Legea privind protecția datelor din 2018 – Orientări cu privire la certificatele de securitate națională), august 2020, punctul 3, p. 3.
[128] A se vedea Ministerul de Interne, „The Data Protection Act 2018 – National Security Certificates Guidance” (Legea privind protecția datelor din 2018 – Orientări cu privire la certificatele de securitate națională), august 2020, punctul 5, p. 4.
[129] A se vedea DPA/S27/Security Service, articolul 27 din DPA 2018, Certificat al Secretarului de Stat, 24 iulie 2019, https://ico.org.uk/media/about-the-ico/documents/nscs/2615660/nsc-part-2-mi5-201908.pdf.

publicarea acestuia ar fi contrară intereselor securității naționale și interesului public sau ar putea pune în pericol siguranța oricărei persoane.

190. În general, în cadrul evaluării proiectului de decizie în raport cu aceste dispoziții, CEPD a observat că garanțiile pentru aceste divulgări includ doar condiția ca destinatarul datelor să respecte cerințele privind securitatea datelor, limitarea divulgării la ceea ce este necesar, păstrarea datelor și restricționarea accesului la date la un număr limitat de persoane. Astfel, **CEPD subliniază că, în ceea ce privește divulgările în străinătate, aplicarea derogării în materie de securitate națională prevăzută de legislația Regatului Unit poate conduce la situații în care garanțiile în legătură cu principiile limitării scopului, necesității și proporționalității, precum și în legătură cu drepturile persoanelor fizice, supravegherea și căile de atac nu ar fi pe deplin furnizate sau respectate în țara terță de destinație. Prin urmare, CEPD recomandă Comisiei Europene să examineze în continuare garanțiile generale prevăzute de legislația Regatului Unit în ceea ce privește divulgarea de informații în străinătate, în special având în vedere aplicarea derogărilor în materie de securitate națională.**

4.3.2.2. Divulgarea în străinătate și schimbul de informații în contextul cooperării internaționale

191. CEPD observă, de asemenea, că, în cadrul evaluării caracterului adecvat al nivelului de protecție, Comisia Europeană nu a luat în considerare acordurile internaționale existente încheiate între Regatul Unit și 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.

192. În plus, CEPD subliniază că evaluarea Comisiei Europene se bazează în principal pe evaluarea părții 4 din DPA 2018 și este preocupat în special de faptul că IPA 2016 se axează pe „cereri" de schimb de informații cu parteneri străini, dar nu abordează alte forme de schimb de informații. În acest sens, CEPD observă că proiectul de decizie al Comisiei Europene nu face referire și nici nu evaluează legătura dintre cadrul legislativ al Regatului Unit și „Acordul privind serviciile de informații în domeniul comunicațiilor dintre Regatul Unit și SUA" (denumit în continuare „Acordul privind serviciile de informații dintre Regatul Unit și SUA"). Într-o declarație recentă care marchează cea de a 75-a aniversare a acestui acord, Agenția Națională de Securitate a SUA (denumită în continuare „NSA") a menționat că acest parteneriat permite „schimbul de informații dintre cele două agenții în măsura maximă posibilă, cu restricții minime" și că „acest document inovator a creat politici și proceduri pentru profesioniștii din domeniul serviciilor de informații din Regatul Unit și SUA în ceea ce privește schimbul de informații referitoare la comunicații, traduceri, analize și descifrarea codurilor"[130]. În plus, acest acord a devenit fundamentul altor parteneriate în domeniul serviciilor de informații cu Australia, Canada și Noua Zeelandă.

193. Caracterul secret al acestui acord și al dispozițiilor sale specifice reprezintă o provocare semnificativă din perspectiva clarității și a previzibilității legii în ceea ce privește utilizarea ulterioară și divulgarea în străinătate a informațiilor colectate de autoritățile din Regatul Unit în scopuri de securitate națională. În acest context, CEPD reamintește că, în ceea ce privește nivelul de protecție garantat în UE, CJUE a subliniat că legislația care implică o ingerință în dreptul fundamental la protecția datelor cu caracter personal trebuie „să prevadă norme clare și precise care să reglementeze conținutul și aplicarea unei măsuri și care să impună o serie de cerințe minime, astfel încât persoanele ale căror date cu caracter personal sunt vizate să dispună de garanții suficiente

[130] A se vedea comunicatul de presă al NSA, „GCHQ and NSA Celebrate 75 Years of Partnership" (NSA și GCHQ aniversează 75 de ani de parteneriat), 5 februarie 2021, https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2494453/gchq-and-nsa-celebrate-75-years-of-partnership/.

care să permită protejarea în mod eficient a datelor lor împotriva riscurilor de abuz, precum și împotriva oricărei accesări și a oricărei utilizări ilicite a acestor date. Necesitatea de a dispune de asemenea garanții este cu atât mai importantă în cazul în care datele cu caracter personal sunt supuse unei prelucrări automate și există un risc important de acces ilicit la aceste date”[131]. Prin urmare, CEPD consideră că, în cadrul evaluării caracterului adecvat al nivelului de protecție, Comisia Europeană ar trebui să ia în considerare impactul Acordului privind serviciile de informații dintre Regatul Unit și SUA.

194. În hotărârea secției I a CEDO din 13 septembrie 2018 în cauza *Big Brother Watch*, Curtea a evaluat regimul aplicabil schimbului de informații din Regatul Unit și, în special, Acordul privind serviciile de informații dintre Regatul Unit și SUA. Într-adevăr, CEDO a apreciat că „respectivul cadru legal care permite serviciilor de informații din Regatul Unit să solicite materiale interceptate de la serviciile de informații străine nu este cuprins în RIPA. Acordul dintre Regatul Unit și SUA privind serviciile de informații din 5 martie 1946 permite în mod specific schimbul de materiale între Statele Unite și Regatul Unit”*[132]*, considerând că există „un temei juridic pentru solicitarea de informații de la serviciile de informații străine și că această lege este suficient de accesibilă”[133]. Deși CEDO a concluzionat că articolul 8[134] din Convenția europeană a drepturilor omului nu a fost încălcat în ceea ce privește regimul aplicabil schimbului de informații, CEPD observă că această hotărâre a fost deferită spre examinare Marii Camere, a cărei decizie este încă pendinte. CEPD observă, de asemenea, că, într-o opinie parțial contrară și parțial concordantă cu această hotărâre, judecătorul Koskelo, căruia i s-a alăturat judecătorul Turković[135], a concluzionat că există o încălcare a articolului 8 din Convenția europeană a drepturilor omului în ceea ce privește regimul aplicabil schimbului de informații, afirmând că „este ușor de acceptat principiul conform căruia orice acord în temeiul căruia informațiile provenite din comunicațiile interceptate sunt obținute prin intermediul serviciilor de informații străine, fie pe baza unor cereri de efectuare a unei astfel de interceptări, fie pe baza unor cereri de transmitere a rezultatelor acesteia, nu ar trebui să permită o implicație de eludare a garanțiilor ce trebuie să fie instituite pentru orice măsură de supraveghere a autorităților naționale (a se vedea punctele 216, 423 și 447). Orice altă abordare ar fi într-adevăr neplauzibilă.”

195. Astfel cum s-a subliniat în mai multe rapoarte ale mass-mediei și ale organizațiilor neguvernamentale[136][137], cea mai recentă versiune a Acordului privind serviciile de informații dintre Regatul Unit și SUA care a fost făcută publică datează din 1956, însă, de atunci, tehnologia comunicațiilor și natura informațiilor pe baza semnalelor electromagnetice s-au schimbat în mod semnificativ. Relatările din mass-media au arătat, de exemplu, că datele transmise prin intermediul

[131] A se vedea hotărârea *Schrems I*, punctul 91.
[132] A se vedea hotărârea CEDO *Big Brother Watch*, punctul 425.
[133] A se vedea hotărârea CEDO *Big Brother Watch*, punctul 427.
[134] A se vedea hotărârea CEDO *Big Brother Watch*, punctul 448.
[135] A se vedea opinia parțial contrară și parțial concordantă cu hotărârea CEDO *Big Brother Watch* a judecătorului Koskelo și a judecătorului Turković.
[136] A se vedea BBC, „Diary reveals birth of secret UK-US spy pact that grew into Five Eyes” [Un jurnal dezvăluie cum a luat naștere o înțelegere secretă de spionaj care s-a dezvoltat într-un acord Five Eyes (Cinci ochi)], 5 martie 2021, https://www.bbc.com/news/uk-56284453.
[137] A se vedea raportul Privacy International intitulat „Policy Briefing – UK Intelligence Sharing Arrangements (Informare privind politicile – acordurile Regatului Unit privind schimbul de informații), aprilie 2018, https://privacyinternational.org/sites/default/files/2018-04/Privacy%20International%20Briefing%20-%20Intelligence%20Sharing%20%28UK%29%20FINAL.pdf.

cablurilor submarine care ajung pe teritoriul Regatului Unit sunt interceptate de GCHQ și puse la dispoziția NSA[138].

196. Pentru CEPD, o întrebare esențială în ceea ce privește schimbul de informații este dacă articolul 109 din DPA 2018 și dispozițiile IPA 2016 continuă să se aplice atunci când serviciile de informații din Regatul Unit acționează în conformitate cu Acordul privind serviciile de informații dintre Regatul Unit și SUA. Un alt aspect esențial care trebuie evaluat este dacă dispozițiile sau aplicarea efectivă a acestui acord au un impact asupra nivelului de protecție a datelor cu caracter personal aflate în tranzit dinspre SEE către Regatul Unit sau permit accesul direct și obținerea de date cu caracter personal de către serviciile de informații ale altor țări terțe.

197. În consecință, în plus față de rezervele exprimate cu privire la „divulgările în străinătate" în temeiul părții 4 din DPA 2018 și derogarea aferentă în materie de securitate națională, precum și la cererile formulate în temeiul IPA 2016, **CEPD este preocupat de alte forme de schimb de informații și divulgări, pe baza altor instrumente, în special pe baza diferitelor acorduri internaționale încheiate de Regatul Unit cu alte țări terțe, în special în cazul în care aceste instrumente rămân inaccesibile publicului, cum ar fi Acordul privind serviciile de informații dintre Regatul Unit și SUA. Efectul unui astfel de acord ar putea duce la o eludare a garanțiilor identificate în ceea ce privește accesul la datele cu caracter personal și utilizarea acestora în scopuri de securitate națională.**

198. Într-adevăr, CEPD împărtășește punctul de vedere exprimat de raportorul special al Organizației Națiunilor Unite, Joe Cannatacci, potrivit căruia „schimbul de informații nu trebuie să reprezinte o modalitate ascunsă de a obține sau de a facilita pentru alte părți obținerea de informații fără a ține seama de garanțiile interne și nici o oportunitate pentru guvernele străine cu standarde mai scăzute privind protecția vieții private (sau a altor drepturi ale omului) de a obține informații de la serviciile secrete din Regatul Unit care ar putea duce la încălcări ale drepturilor omului"[139].

199. În plus, **CEPD consideră că încheierea de acorduri bilaterale sau multilaterale cu țări terțe în scopul cooperării în domeniul serviciilor de informații, prin care se asigură un temei juridic pentru interceptarea și obținerea directă de date cu caracter personal sau pentru transferul de date cu caracter personal către aceste țări, poate afecta, de asemenea, în mod semnificativ condițiile de utilizare ulterioară a informațiilor colectate, întrucât astfel de acorduri pot afecta cadrul juridic privind protecția datelor din Regatul Unit, astfel cum a fost acesta evaluat.**

4.3.3. Supraveghere

200. CEPD subliniază importanța unei supravegheri cuprinzătoare de către autorități de supraveghere independente în vederea asigurării 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

[138] A se vedea The Guardian, „GCHQ taps fibre-optic cables for secret access to world's communications" (GCHQ se conectează la cablurile de fibră optică pentru a accesa în secret comunicațiile din întreaga lume), 21 iunie 2013, https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

[139] A se vedea declarația de sfârșit de mandat a Raportorului special privind dreptul la viață privată la încheierea misiunii sale în Regatul Unit al Marii Britanii și Irlandei de Nord, Londra, 29 iunie 2018, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E#:~:text=Intelligence%20sharing%20must%20not%20result,UK%20intelligence%20that%20could%20give.

respectării dispozițiilor în domeniul protecției persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.

201. Atunci când datele cu caracter personal sunt accesate și utilizate în scopuri de securitate națională, funcția de supraveghere este îndeplinită în principal de IPC și de comisarii judiciari (denumiți în continuare „comisarii judiciari").

202. **CEPD recunoaște, în general, că introducerea comisarilor judiciari în IPA 2016 reprezintă o îmbunătățire semnificativă.** În conformitate cu o solicitare formulată în cele de mai sus, Comisia Europeană este invitată să evalueze mai detaliat independența **comisarilor judiciari și, în special, în ce măsură este garantată din punct de vedere juridic independența IPC și a biroului IPC (denumit în continuare „IPCO"), deoarece acest aspect nu se regăsește în IPA 2016.** Acest lucru este cu atât mai important cu cât IPC decide cu privire la căile de atac introduse de guvern, în cazul în care o cerere de instituire a unei **măsuri** de supraveghere a fost respinsă **de** un comisar judiciar.

203. IPC are funcții de supraveghere *ex ante*, precum și *ex post*. În ceea ce privește supravegherea *ex ante*, CEPD înțelege că funcția comisarilor judiciari este de a aproba, în cazuri individuale, diferite măsuri de supraveghere, inclusiv interceptarea specifică și obținerea în masă a datelor referitoare la comunicații. CEPD observă, de asemenea, că aprobarea prealabilă a măsurilor de supraveghere nu poate fi dedusă din jurisprudența CJUE ca o cerință absolută în legătură cu proporționalitatea măsurilor de supraveghere[140].

204. Cu toate acestea, pentru a evalua eficacitatea acestui nivel de supraveghere, CEPD consideră că este necesar să se clarifice în continuare scenariile pentru care este posibilă o interceptare legală fără aprobarea prealabilă a comisarilor judiciari.

205. În proiectul său de decizie, Comisia Europeană menționează în notele de subsol 201 și 266 „cazurile specifice limitate" prevăzute de IPA 2016 la articolele 44-52 cu privire la interceptările specifice. CEPD observă că articolele 45-51 din IPA 2016 prevăd derogări despre care se afirmă că nu sunt utilizate în mod regulat de serviciile de informații. În plus, **CEPD înțelege** că, în **cazurile în care se aplică derogările respective** (de exemplu, în legătură cu furnizorii de servicii de telecomunicații și servicii poștale), comisarii judiciari parcurg procedura de aprobare prealabilă în cazul în care autoritățile de aplicare a legii sau serviciile de informații **solicită** accesul la aceste date **și invită Comisia Europeană să confirme în decizia sa corectitudinea acestei afirmații**.

206. CEPD recunoaște că articolul 44 alineatul (2) din IPA 2016 permite interceptarea comunicațiilor în cazul în care una dintre părți (expeditorul sau destinatarul) și-a dat acordul în acest sens și există o autorizație în temeiul RIPA 2000 sau al Legii privind reglementarea competențelor de investigare din 2000 (din Scoția) (2000 asp 11), și anume fosta situație juridică anterioară înființării instituției comisarilor judiciari. CEPD **invită** Comisia Europeană să clarifice dacă acest lucru înseamnă că, în cazurile în care există acordul unilateral respectiv, procedura de aprobare prealabilă nu se aplică deloc.

[140] Cu toate acestea, Comitetul observă, de asemenea, că, atunci când a invalidat Scutul de confidențialitate în hotărârea *Schrems II*, CJUE a luat act de faptul că, în temeiul legislației SUA, așa-numita instanță FISA „nu autorizează măsuri individuale de supraveghere; dimpotrivă, acesta autorizează programe de supraveghere (precum PRISM, UPSTREAM) pe baza unor certificări anuale" (punctul 179).

207. În ceea ce privește supravegherea *ex post*, este, de asemenea, important să se verifice dacă se asigură o supraveghere independentă eficientă fără lacune, în special în cazul în care aceasta nu este prevăzută *ex ante*.

208. CEPD observă că, în legătură cu cele prevăzute la articolele 48-52 din IPA 2016, comisarii judiciari efectuează o examinare *ex post* și **invită Comisia Europeană să clarifice în baza căror cerințe și la inițiativa cui urmează să se efectueze o astfel de examinare *ex post***.

209. În conformitate cu articolul 229 alineatul (4) din IPA 2016, IPC nu monitorizează exercitarea anumitor funcții. În acest sens, CEPD invită Comisia Europeană să clarifice dispozițiile articolului 229 alineatul (4) literele (d) și (e) din IPA 2016 în ceea ce privește impactul său practic asupra competenței de control a IPC. **CEPD înțelege că ICO este autoritatea de supraveghere competentă în cazul în care se aplică derogările de la articolul 229 alineatul (4) din IPA 2016 și invită Comisia Europeană să confirme în decizia sa corectitudinea acestei afirmații.**

210. **Se pare că, în cadrul** supravegherii *ex post***,** rolul IPC se **limitează** la formularea de recomandări în caz de neconformitate și la notificarea persoanei vizate, dacă eroarea este gravă și este în interesul public ca persoana respectivă să fie informată. **CEPD invită Comisia Europeană să clarifice modul în care IPCO poate asigura în mod eficace respectarea legislației.**

211. **În cele din urmă, CEPD înțelege că persoanele afectate nu se pot adresa direct IPCO, ci trebuie să depună o plângere la ICO, care are totuși competențe limitate în domeniul securității naționale. Prin urmare, CEPD invită Comisia Europeană să clarifice suplimentar modul în care se asigură din punct de vedere juridic gestionarea plângerilor în aceste cazuri de către IPCO.**

4.3.4. Căi de atac

212. Având în vedere hotărârile *Schrems I* și *Schrems II* ale CJUE, este clar că protecția jurisdicțională efectivă în sensul articolului 47 din Carta drepturilor fundamentale a Uniunii Europene este de o importanță fundamentală pentru prezumția caracterului adecvat al legislației unei țări terțe. Hotărârile în cauză au arătat, de asemenea, că, în această privință, trebuie să se acorde o atenție deosebită protecției jurisdicționale efective în ceea ce privește accesul la datele cu caracter personal în scopuri de securitate națională.

213. **CEPD recunoaște instituirea IPT de către Regatul Unit. IPT are competența nu numai de a audia cauze privind utilizarea competențelor de investigare de către autoritățile de aplicare a legii, ci și cauze care vizează utilizarea acestora de către serviciile de informații. CEPD înțelege că IPT funcționează ca instanță adecvată în sensul articolului 47 din Carta drepturilor fundamentale a Uniunii Europene. În ceea ce privește competențele sale, Comisia Europeană este invitată să confirme că IPT dispune de toate competențele menționate în considerentul 262 din proiectul de decizie, indiferent de temeiul juridic în baza căruia este introdusă plângerea.**

214. Supravegherea discretă de către serviciile de informații va însemna adesea că obiectul supravegherii, persoana vizată, nu este și nu va fi la curent cu supravegherea. În acest context, în cadrul analizelor sale asupra legislației SUA, CEPD și-a exprimat de nenumărate ori îngrijorarea cu privire la cerința „calității procesuale active”, astfel cum este interpretată în legislația SUA, în cazurile de supraveghere. În acest context, CEPD observă că plângerea depusă la IPT impune doar necesitatea unui test de „convingere”, conform căruia reclamantul trebuie să demonstreze că este potențial expus riscului de a fi supus unei măsuri.

215. În cadrul analizei sale asupra IPT, CEPD a acordat, de asemenea, o atenție deosebită faptului că s-a constatat în mod repetat că funcționarea IPT este în conformitate cu Convenția europeană a drepturilor omului, astfel cum a fost interpretată de CEDO.