Avizul 28/2018

referitor la Proiectul de decizie de punere în aplicare al Comisiei Europene privind nivelul de protecție adecvat a datelor cu caracter personal în Japonia

Adoptat la 5 decembrie 2018

CUPRINS

Comitetul European pentru Protecția Datelor

Având în vedere articolul 70 alineatul (1) litera (s) din Regulamentul 2016/679/UE 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 SEE și, în special, anexa XI și Protocolul 37 la acesta, astfel cum au fost modificate prin Decizia nr. 154/2018 a Comitetului mixt al SEE din 6 iulie 2018,

Având în vedere articolul 12 și articolul 22 din Regulamentul său de Procedură din 25 mai 2018,

ADOPTĂ URMĂTORUL AVIZ:

1 REZUMAT

1. Comisia Europeană a aprobat proiectul de decizie de punere în aplicare privind nivelul de protecție adecvat a datelor cu caracter personal în Japonia în temeiul Regulamentului General privind Protecția Datelor, (denumit în continuare: RGPD)[1] la 5 septembrie 2018[2]. Pe această bază, Comisia Europeană a lansat procedura pentru adoptarea formală a acestei decizii.

2. La 25 septembrie 2018, Comisia Europeană a solicitat avizul Comitetului European pentru Protecția Datelor („CEPD”)[3]. Comisiei i s-a solicitat să pună la dispoziția CEPD toată documentația necesară cu privire la această țară, inclusiv corespondența relevantă purtată cu guvernul Japoniei.

3. În urma discuțiilor purtate cu CEPD, Comisia Europeană și-a modificat de două ori proiectul de decizie privind nivelul de protecție adecvat, și a transmis ultima sa versiune la 13 noiembrie 2018[4] . CEPD a formulat prezentul aviz pe baza celei mai recente versiuni a proiectului de decizie de punere în aplicare (denumit în continuare „proiectul de decizie privind nivelul de protecție adecvat”).

4. Evaluarea efectuată de CEPD a nivelului de protecție asigurat prin decizia Comisiei privind nivelul de protecție adecvat a fost realizată în baza examinării deciziei ca atare, precum și în baza analizării documentației puse la dispoziție[5]de Comisie[6].

[1] Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE.
[2] Vezi comunicatul de presă http://europa.eu/rapid/press-release_IP-18-5433_en.htm.
[3] În temeiul articolului 70 alineatul (1) litera (s) din RGPD.
[4] Vezi anexa I la avizul CEPD pentru versiunea actualizată a proiectului de decizie de punere în aplicare a Comisiei Europene.
[5] CEPD și-a întemeiat analiza pe traducerile furnizate de autoritățile japoneze verificate de Comisia Europeană

5. CEPD s-a axat atât pe evaluarea aspectelor comerciale din proiectul de decizie privind nivelul de protecție adecvat, cât și pe accesul guvernului la datele cu caracter personal transferate din UE în scopuri de aplicare a legii și de securitate națională, inclusiv căile de atac pe care le au la dispoziție persoanele fizice din UE. De asemenea, CEPD a evaluat în ce măsură garanțiile oferite pe baza cadrului legal japonez au fost puse în aplicare și funcționează.

6. CEPD a utilizat drept referință principală pentru acest demers criteriile de referință privind nivelul de protecție adecvat[7] adoptate în februarie 2018.

1.1 Arii de convergență

7. Obiectivul cheie al CEPD a fost să formuleze un aviz pentru Comisia Europeană privind nivelul de protecție oferit persoanelor fizice de cadrul japonez. Este important de recunoscut că CEPD nu se așteaptă la reproducerea legislației europene în domeniul protecției datelor de cadrul juridic japonez.

8. Cu toate acestea, CEPD reamintește că, pentru a considera că oferă un nivel de protecție adecvat, jurisprudența CJUE, precum și articolul 45 din RGPD, impun ca legislația țării terțe să fie aliniată la esența principiilor fundamentale prevăzute în RGPD. În domeniul protecției datelor, CEPD constată, de asemenea, că există domenii cheie ce necesită aliniere între cadrul legislativ al RGPD și cadrul legislativ japonez cu privire la anumite prevederi de bază cum ar fi exactitatea și reducerea la minimum a datelor, limitări legate de stocare, securitatea datelor, limitări legate de scop și o autoritate de supraveghere independentă, Comisia pentru protecția informațiilor cu caracter personal (CPP).

9. În plus față de cele de mai sus, CEPD salută eforturile Comisiei Europene și ale autorităților japoneze de a garanta că Japonia oferă un nivel de protecție adecvat în raport cu cel oferit de RGPD, în special prin acoperirea diferențelor dintre RGPD și cadrul de protecție a datelor din Japonia, prin adoptarea de norme suplimentare de către CPP, aplicabile exclusiv datelor cu caracter personal transferate din UE în Japonia, și anume normele suplimentare. De exemplu, CEPD ia act că CPP a fost de acord să considere și alte categorii de date drept date cu caracter special (conform legislației japoneze, datele cu caracter special nu includ orientarea sexuală, nici apartenența sindicală). În plus, normele suplimentare garantează că drepturile persoanelor vizate se vor aplica tuturor datelor cu caracter personal transferate din UE, indiferent de perioada de păstrare a acestor date (întrucât sistemul juridic japonez prevede că drepturile persoanelor vizate nu se aplică datelor cu caracter personal prevăzute a fi eliminate în termen de șase luni).

10. De asemenea, CEPD remarcă eforturile Comisiei Europene de a consolida decizia privind nivelul de protecție adecvat, ca răspuns la preocupările semnalate de CEPD.

1.2 Provocări de ordin general

11. Cu toate acestea, există în continuare probleme, iar CEPD propune următoarele domenii principale care trebuie consolidate și monitorizate îndeaproape în sistemul japonez.

12. Prima problemă se referă la monitorizarea acestei noi arhitecturi a nivelului de protecție adecvat, care combină un cadru legislativ existent cu norme suplimentare specifice pentru a

[6] Vezi anexa II la avizul CEPD pentru lista de documente pe care Comisia Europeană nu le-a pus la dispoziția CEPD.
[7] WP254, Criterii de referință privind nivelul de protecție adecvat, 6 februarie 2018.

asigura un sistem sustenabil și fiabil care nu va pune **probleme practice privind respectarea concretă și eficientă** de entitățile japoneze și implementarea de către CPP.

13. Pe de altă parte, CEPD ia act de angajamentele și reasigurările repetate ale Comisiei Europene și ale autorităților japoneze privind caracterul obligatoriu și executoriu al normelor suplimentare și invită Comisia Europeană **să monitorizeze în permanență caracterul obligatoriu și implementarea efectivă ale acestor norme în Japonia**, deoarece valoarea lor legislativă este un element absolut esențial al nivelului de protecție adecvat UE - Japonia. În ceea ce privește orientările CPP, CEPD ar dori să obțină clarificări cu privire la proiectul de decizie privind nivelul de protecție adecvat în legătură cu **caracterul obligatoriu al acestor orientări și solicită Comisiei să monitorizeze cu atenție acest aspect**[8]**.**

1.3 Aspecte specifice de natură comercială

14. În ceea ce privește aspectele comerciale ale proiectului de decizie privind nivelul de protecție adecvat UE-Japonia, CEPD are câteva motive de îngrijorare și ar dori să solicite clarificări asupra unor chestiuni importante.

1.3.1 Motive de îngrijorare ale CEPD cu privire la principiile-cheie de protecție a datelor

15. CEPD salută faptul că normele suplimentare exclud posibilitatea ca datele cu caracter personal transferate din UE să fie transferate mai departe către o țară terță în baza normelor de protecție a vieții private în cooperarea economică transfrontalieră din Asia-Pacific (ACE CBPR). În plus, CEPD recunoaște că, în noul său proiect de decizie privind nivelul de protecție adecvat, Comisia Europeană s-a angajat să suspende decizia privind nivelul de protecție adecvat dacă transferurile ulterioare nu mai asigură continuitatea protecției.

16. Conform legislației japoneze, una dintre bazele legale pentru transferurile ulterioare este recunoașterea unei țări terțe ca oferind un nivel de protecție adecvat precum cel al Japoniei. Cu toate acestea, evaluarea de către Japonia a unei țări terțe ca fiind adecvată nu pare să includă „normele suplimentare" specifice negociate între Comisia Europeană și CPP, care sunt aplicabile doar datelor cu caracter personal din UE pentru a oferi un nivel de protecție echivalent, în esență, cu cel al standardelor RGPD. Rezultă că datele cu caracter personal ale UE transferate din Japonia către o țară terță care nu este recunoscută ca având, în esență, un cadru legislativ de protecție a datelor echivalent cu cel prevăzut de RGPD în baza nivelului adecvat oferit de Japonia, nu mai beneficiază, neapărat, de o protecție adecvată a datelor cu caracter personal ale UE.

17. **Totuși, trebuie reținut că pot apărea transferuri ulterioare de date cu caracter personal către țări terțe, care pot deveni obiectul unei decizii ulterioare a Japoniei privind nivelul de protecție adecvat. Este posibil ca aceste țări terțe să nu fi făcut obiectul unei evaluări anterioare sau constatări a nivelului adecvat din partea UE. În această etapă, COM trebuie să-și preia rolul de monitorizare și să se asigure că nivelul de protecție a datelor UE este menținut sau să ia în considerație suspendarea acestei decizii privind nivelul de protecție adecvat.**

18. Mai mult, CEPD are rezerve legate de **obligațiile de consimțământ și transparență** ale operatorilor de date (operatori economici care gestionează informații cu caracter personal). CEPD a efectuat o verificare atentă a acestor elemente deoarece, spre deosebire de legislația europeană privind protecția datelor, utilizarea consimțământului ca temei pentru prelucrare și transferuri are un rol central în sistemul legislativ japonez. De exemplu, CEPD își exprimă

[8] Pentru mai multe informații, vezi secțiunea 1.3.4. din prezentul aviz.

îngrijorarea privind noțiunea de consimțământ, care nu este definită astfel încât să includă dreptul de retragere, un element esențial al legislației UE pentru a asigura controlul efectiv al persoanei vizate asupra datelor sale cu caracter personal. În ceea ce privește obligațiile de transparență ale operatorilor economici care gestionează informații cu caracter personal, există îndoieli cu privire la oferirea de informații proactive către persoanele vizate

19. CEPD este îngrijorat că **sistemul de recurs japonez** s-ar putea să nu fie ușor accesibil persoanelor fizice din UE care au nevoie de sprijin sau doresc să depună o plângere ținând cont că sprijinul oferit de CPP este disponibil doar prin intermediul liniei de asistență telefonică și doar în limba japoneză. Aceeași problemă există și în ceea ce privește serviciul de mediere oferit de CPP, deoarece sistemul nu este disponibil publicului pe baza versiunii în limba engleză a site-ului CPP și documente informative importante, cum ar fi întrebări frecvente despre Legea privind protecția datelor cu caracter personal, sunt disponibile doar în limba japoneză. În acest sens, CEPD ar aprecia dacă Comisia ar discuta cu CPP posibilitatea înființării unui serviciu online, cel puțin în limba engleză, în scopul furnizării de asistență și gestionării reclamațiilor persoanelor fizice din UE - similar celui prevăzut în anexa II la această decizie privind nivelul de protecție adecvat. De asemenea, Comisia Europeană trebuie să monitorizeze îndeaproape eficiența sancțiunilor și a măsurilor reparatorii relevante.

1.3.2 Necesitatea de clarificare

20. CEPD ar aprecia să primească asigurări privind anumite aspecte din proiectul de decizie privind nivelul de protecție adecvat care necesită încă clarificări suplimentare.

21. Acestea se referă, de exemplu, la câteva aspecte-cheie ale legislației japoneze. Mai precis, există o lipsă de claritate cu privire la **statutul așa-numitului „mandatar”** - un termen asemănător celui de operator de date conform RGPD, dar a cărui abilitate de a determina și modifica scopul și mijloacele de prelucrare a datelor cu caracter personal rămâne ambiguă.

22. De asemenea, din cauza lipsei de documente relevante, CEPD are nevoie de asigurări în ceea ce privește necesitatea și proporționalitatea **limitărilor cu privire la drepturile persoanelor fizice** (în special, drepturile de acces, rectificare și contestare) într-o societate democratică, precum și respectarea esenței drepturilor fundamentale.

23. CEPD se așteaptă, de asemenea, ca Comisia Europeană să monitorizeze îndeaproape protecția efectivă a **datelor cu caracter personal transferate din UE în Japonia, în baza proiectului de decizie privind nivelul de protecție adecvat, de-a lungul întregului „ciclu de viață” al acestora**, chiar dacă legislația japoneză impune obligația de a păstra cel mult trei ani înregistrările cu privire la proveniența datelor.

1.4 Referitor la accesul autorităților publice la datele transferate în Japonia

24. CEPD a analizat, de asemenea, cadrul legislativ aferent entităților guvernamentale japoneze referitor la accesarea datelor cu caracter personal transferat din UE în Japonia în scopuri de aplicare a legii sau de securitate națională. Deși recunoaște asigurările oferite de guvernul japonez, menționate la anexa II la proiectul de decizie privind nivelul de protecție adecvat, CEPD a identificat o serie de aspecte ce necesită clarificări și ridică anumite îndoieli, dintre care următoarele trebuie menționate.

25. În domeniul aplicării legii, CEPD constată că principiile juridice care se aplică accesării datelor par să fie deseori similare normelor aplicabile în UE, în măsura în care acestea sunt disponibile. Din cauza lipsei de traduceri disponibile pentru mai multe texte juridice și pentru jurisprudența relevantă, este dificil să se concluzioneze, totuși, că toate procedurile pentru

accesarea datelor sunt necesare și proporționale și că aplicarea acelor principii se efectuează într-un mod care este „echivalent, în esență," cu legislația UE.

26. În domeniul securității naționale, CEPD recunoaște că guvernul japonez a reafirmat că informațiile pot fi obținute doar din surse cu acces gratuit sau prin punerea voluntară la dispoziție de către societățile comerciale și că nu strânge informații despre publicul larg. Este, totuși, conștient de îngrijorările exprimate de experți și în mass-media, și ar aprecia obținerea de clarificări suplimentare cu privire la măsurile de supraveghere ale entităților guvernamentale japoneze.

27. În ceea ce privește căile de atac ale persoanelor fizice din UE, în domeniul aplicării legii cât și al securității naționale, CEPD salută negocierea, de către Comisia Europeană și guvernul japonez, a unui mecanism suplimentar pentru persoanele fizice din UE, în sensul oferirii unei căi suplimentare de atac, extinzând astfel competențele autorității japoneze pentru protecția datelor. Cu toate acestea, rămâne îngrijorarea că acest nou mecanism nu poate compensa în totalitate deficiențele în materie de supraveghere și căi de atac ale legislației japoneze. Prin urmare, CEPD dorește să obțină precizări suplimentare pentru a se asigura că acest nou mecanism compensează în totalitate deficiențe respective.

1.5 Concluzie

28. CEPD consideră că această decizie privind nivelul de protecție adecvat este extrem de importantă. Fiind prima decizie privind nivelul de protecție adecvat de la intrarea în vigoare a RGPD, aceasta va constitui **un precedent pentru viitoarele solicitări privind nivelul de protecție adecvat, precum și pentru revizuirea deciziilor privind nivelul adecvat pronunțate în temeiul Directivei 95/46[9].** De asemenea, este important de subliniat că persoanele fizice sunt din ce în ce mai conștiente de impactul globalizării asupra vieții lor private și apelează la autoritățile de supraveghere pentru a se asigura că există garanții adecvate atunci când datele lor cu caracter personal sunt transferate în străinătate. În lumina acestor implicații, CEPD consideră că Comisia Europeană trebuie să se asigure că nu există nicio deficiență în ceea ce privește protecția oferită prin nivelul adecvat UE-Japonia și că acest tip specific de adecvare este aliniat cerințelor prevăzute la articolul 45 din RGPD.

29. CEPD salută eforturile Comisiei Europene și ale CPP japoneze de a alinia, pe cât posibil, cadrul legislativ japonez la cel european. **Îmbunătățirile** aduse prin normele suplimentare în vederea remedierii unora dintre diferențele existente între cele două cadre legislative sunt foarte importante și bine primite.

30. Cu toate acestea, în urma unei analize atente a proiectului de decizie al Comisiei privind nivelul de protecție adecvat, precum și al cadrului japonez privind protecția datelor, CEPD remarcă că **există încă o serie de preocupări, precum și nevoia de precizări suplimentare**. Mai mult, acest tip specific de adecvare care combină un cadru național existent cu norme specifice suplimentare ridică întrebări și în ceea ce privește punerea sa în aplicare la nivel operațional. Prin prisma considerațiilor de mai sus, CEPD recomandă Comisiei Europene să răspundă preocupărilor și solicitărilor de clarificare exprimate de CEPD și să prezinte dovezi suplimentare și explicații cu privire la problemele ridicate. CEPD invită, de asemenea, Comisia Europeană să efectueze o reexaminare a acestei constatări a nivelului adecvat (cel puțin) o

[9] 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.

dată la doi ani și nu o dată la patru ani astfel cum sugerează proiectul de decizie actual privind nivelul de protecție adecvat.

2 INTRODUCERE

2.1 Cadrul japonez privind protecția datelor

31. Cadrul japonez privind protecția datelor a fost modernizat foarte recent, în 2017. Acest cadru cuprinde mai mulți piloni, în centrul cărora se află un act legislativ cu caracter general, legea privind protecția informațiilor cu caracter personal (APPI). Un alt act legislativ important este decretul ministerial de punere în aplicare a APPI („decret ministerial") care precizează anumite principii de bază ale APPI.

32. În baza unei decizii a guvernului, adoptată la 12 iunie 2018[10] și a articolului 6 din APPI, CPP i-a fost conferită competența de a *„lua măsurile necesare pentru a remedia diferențele la nivel de sisteme și de operațiuni dintre Japonia și țara terță vizată, în vederea asigurării unei gestiuni corespunzătoare a informațiilor cu caracter personal primite din fiecare țară"*[11]. De asemenea, decizia guvernului sugerează că normele adoptate de CPP care suplimentează sau depășesc sfera celor prevăzute de APPI ar avea caracter obligatoriu și ar produce efecte juridice asupra operatorilor economici japonezi[12].

33. În consecință, CPP a intrat în negocieri cu Comisia Europeană și , în iunie 2018, a adoptat norme mai stricte decât cele prevăzute în APPI și decretul ministerial privind datele transferate din UE. Acestea sunt normele suplimentare în temeiul legii privind protecția informațiilor cu caracter personal referitoare la gestionarea datelor cu caracter personal transferate din UE în baza unei decizii privind nivelul de protecție adecvat, denumite în continuare „norme suplimentare"[13]. Aceste norme suplimentare sunt, de asemenea, anexate proiectului de decizie de punere în aplicare al Comisiei publicat în iulie 2018.

34. Este important de remarcat că normele suplimentare sunt aplicabile doar datelor cu caracter personal transferate din Uniunea Europeană în Japonia în baza deciziei privind nivelul de protecție adecvat cu scopul de a îmbunătăți protecția aplicabilă acelor date. Ca atare, acestea nu se aplică datelor cu caracter personal ale persoanelor fizice din Japonia sau provenind din alte țări decât cele din SEE.

35. Mai mult, CEPD dorește să atragă atenția asupra faptului că APPI a intrat în vigoare în forma sa modificată la 30 mai 2017, iar CPP a fost instituită în forma sa actuală în 2016. În plus, normele suplimentare negociate de CPP cu Comisia Europeană nu au intrat încă în vigoare, aceasta depinzând de recunoașterea de către Comisia Europeană a Japoniei ca jurisdicție adecvată celei din UE.

2.2 Sfera de aplicare a evaluării CEPD

[10] CEPD remarcă faptul că, conform proiectului de decizie privind nivelul de protecție adecvat, această decizie a guvernului a fost adoptată la 12 iunie 2018. Cu toate acestea, CEPD i-a fost prezentată doar versiunea preliminară a deciziei guvernului, care datează din luna aprilie 2018.
[11] Decizia guvernului din 25 aprilie 2018.
[12] Vezi Secțiunea 1.3.4. de mai jos pentru mai multe informații.
[13] Normele suplimentare, anexa I la decizia de punere în aplicare a Comisiei din XXXX, în temeiul Regulamentului 2016/679 al Parlamentului și Consiliului European, privind nivelul de protecție adecvat a datelor cu caracter personal în Japonia, transmise către CEPD în septembrie 2018.-

36. Proiectul de decizie al Comisiei Europene privind nivelul de protecție adecvat este rezultatul unei evaluări a normelor de protecție a datelor din Japonia, urmată de negocieri cu autoritățile japoneze. Rezultatul acestor negocieri este reflectat, cu precădere, în cele două anexe atașate la proiectul de decizie privind nivelul de protecție adecvat: prima furnizează măsuri de protecție suplimentare pe care operatorii economici japonezi vor trebui să le aplice prelucrării datelor cu caracter personal transferate din EU, în timp ce a doua conține asigurări și angajamente ale guvernului japonez cu privire la accesul autorităților publice la date.

37. CEPD a examinat cadrul japonez de protecție a datelor, normele suplimentare negociate de Comisia Europeană și asigurările și angajamentele guvernului japonez. Se așteaptă ca CEPD să prezinte un aviz independent asupra constatărilor Comisiei Europene, să identifice, dacă există, insuficiențele din cadrul privind nivelul adecvat, și să depună eforturi în vederea propunerii de modificări sau amendamente în vederea rezolvării acestora.

38. Așa cum se precizează în criteriile de referință ale CEPD privind nivelul de protecție adecvat, „*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 din țara terță*”[14]*.*

39. Cu toate acestea, CEPD a primit majoritatea documentelor traduse în limba engleză, la care se face referință în proiectul de decizie privind nivelul de protecție adecvat și care sunt o parte esențială a sistemului legislativ japonez. Așadar, CEPD emite prezentul aviz pe baza analizei documentelor disponibile în limba engleză. CEPD a luat în considerare cadrul aplicabil protecției datelor în Uniunea Europeană, inclusiv articolul 8 din Convenția europeană a drepturilor omului (denumită în continuare: CEDR) care protejează dreptul la viața privată și de familie precum și articolele 7, 8 și 47 din Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare Carta), respectiv protejarea dreptului la viața privată și de familie, dreptul la protecția datelor cu caracter personal și dreptul la o cale de atac eficientă și la un proces echitabil. În plus față de prevederile de mai sus, CEPD a luat în considerare cerințele RGPD și a examinat jurisprudența relevantă.

40. Obiectivul acestui exercițiu este asigurarea unui cadru japonez de protecție a datelor echivalent, în esență, cu cel al Uniunii Europene. Conceptul de „nivel de protecție adecvat” care există deja în temeiul Directivei 95/46 a fost dezvoltat mai amplu de către CJUE. Este important să reamintim standardul stabilit de CJUE în cauza Schrems, și anume că - în timp ce „nivelul de protecție” în țara terță trebuie să fie „echivalent, în esență”, cu cel garantat în UE - „mijloacele la care recurge respectiva țară terță, în acest sens, în vederea oferirii unui nivel de protecție similar pot diferi de cele utilizate în cadrul [UE]”[15]. Așadar, obiectivul nu este acela de a reflecta legislația europeană punct cu punct, ci de a stabili cerințele esențiale, de bază, ale legislației care face obiectul examinării. Adecvarea poate fi obținută prin combinarea drepturilor persoanelor vizate cu obligațiile celor care prelucrează datele sau care exercită control asupra unor astfel de prelucrări și supravegherea de către organisme independente. Cu toate acestea, normele de protecție a datelor își produc efectele doar dacă sunt aplicabile din punct de vedere juridic și respectate în practică. Este așadar necesară luarea în considerare nu numai a conținutului normelor aplicabile datelor cu caracter personal transferate într-o țară terță sau unei organizații internaționale, ci și sistemul

[14] WP254, p.3.

[15] Cauza C-362/14, Maximillian Schrems / comisarul pentru protecția datelor, din 6 octombrie 2015 (§§ 73, 74).

implementat pentru a asigura eficacitatea unor astfel de norme. Existența unor mecanisme eficiente de punere în aplicare este de o importanță capitală pentru asigurarea eficacității normelor de protecție a datelor[16].

2.3 Comentarii și preocupări de ordin general

2.3.1 Particularități ale acestui tip de decizie privind nivelul de protecție adecvat

41. Nivelul adecvat UE-Japonia este primul care trebuie examinat în noul context legal oferit de RGPD. Acest aspect face ca activitatea CEPD să fie cu atât mai importantă prin prisma efectelor acestui proiect de decizie privind nivelul de protecție adecvat asupra viitoarelor puneri în aplicare privind nivelul adecvat.

42. De asemenea, nivelul adecvat UE-Japonia ar fi prima adecvare reciprocă. Atunci când și dacă UE va recunoaște Japonia ca oferind un nivel de protecție echivalent, în esență, cu cel prevăzut de RGPD, Japonia va emite la rândul său propria sa decizie privind nivelul adecvat, în temeiul articolului 24 din APPI, recunoscând UE ca oferind un nivel de protecție adecvat conform cadrului japonez de protecție a datelor. Astfel, adecvarea preconizată a Japoniei cu UE este de o natură specifică pe care CEPD a luat-o în considerare în evaluarea sa. Astfel cum se precizează mai sus, CPP japoneză a negociat cu Comisia Europeană norme specifice, mai stricte, aplicabile doar datelor transferate din UE. Aceste norme mai stricte au caracter obligatoriu și executoriu conform deciziei cabinetului și trebuie respectate de toți operatorii economici care gestionează informații cu caracter personal (denumiți în continuare PIHBO) în Japonia atunci când prelucrează date cu caracter personal care provin din UE, în baza acestui proiect de decizie privind nivelul de protecție adecvat.

43. Așadar, Comisia Europeană și-a bazat constatarea privind nivelul de protecție adecvat nu numai pe cadrul existent general privind protecția datelor din Japonia, ci și pe aceste norme specifice. Necesitatea elaborării de norme suplimentare în vederea completării APPI indică faptul că Comisia Europeană recunoaște, per se, lipsa de echivalență, în esență, între legislația japoneză în materie de protecție a datelor și RGPD.

44. **Prin prisma aspectelor menționate mai sus, CEPD invită Comisia Europeană să se asigure că această nouă arhitectură a adecvării, prima ce urmează a fi adoptată în conformitate cu RGPD, pe baza normelor suplimentare, va fi un sistem sustenabil și fiabil care nu va pune probleme de ordin practic în ceea ce privește respectarea sa concretă și eficientă de entitățile japoneze și punerea în aplicare de CPP.**

2.3.2 Exactitatea traducerilor

45. La fel ca și Comisia Europeană, CEPD a lucrat pe baza traducerilor în limba engleză furnizate de autoritățile japoneze[17]. CEPD invită Comisia Europeană să precizeze dacă și-a întemeiat proiectul de decizie privind nivelul de protecție adecvat pe traducerile în limba engleză primite și să verifice regulat calitatea și exactitatea acestor traduceri.

2.3.3 Nivelul adecvat la nivel sectorial

46. Constatarea nivelului adecvat al acestui proiect de decizie privind nivelul de protecție adecvat este limitată la protejarea informațiilor cu caracter personal de către operatorii economici care gestionează informații cu caracter personal, în sensul APPI. Aceasta înseamnă că adecvarea are caracter sectorial deoarece se aplică exclusiv sectorului privat, datele cu

[16] WP254, p.2.
[17] Comisia Europeană a verificat aceste traduceri.

caracter personal transferate între autoritățile și organismele din sectorul public ieșind din sfera de aplicare a acesteia. În prezent, Comisia Europeană precizează pe scurt această caracteristică a domeniului de aplicare privind adecvarea în considerentul 10 din proiectul de decizie privind nivelul de protecție adecvat.

47. **CEPD invită Comisia Europeană să expliciteze natura sectorială a acestei constatări a nivelului adecvat în titlul deciziei de punere în aplicare precum și în articolul 1 din aceasta, în conformitate cu articolul 45 alineatul (3) din RGPD.**

2.3.4 Caracterul obligatoriu al normelor suplimentare și al orientărilor CPP

48. Articolul 6 din APPI menționează că „guvernul va... lua inițiativele legislative și de altă natură necesare astfel încât să poată acționa în mod discret în vederea protejării informațiilor cu caracter personal ceea ce necesită, cu precădere, asigurarea unei stricte implementări a gestionării acestora în cadrul eforturilor de a asigura o mai bună protecție a drepturilor și intereselor persoanelor fizice, și va lua măsurile necesare în colaborarea cu guvernele din alte țări în vederea construirii unui sistem conform la nivel internațional în ceea ce privește informațiile cu caracter personal prin promovarea cooperării cu o organizație internaționale și un alt cadru internațional". Cu toate că acest articol al APPI prevede în mod clar că are competența de a lua o astfel de inițiativă legală, acesta nu se referă în mod direct la CPP ca organism competent să adopte norme specifice[18]. Din cauza constrângerilor de timp, CEPD nu a reușit să colecteze, să revizuiască și să analizeze dovezile existente referitoare la acest aspect.

49. **Având în vedere importanță acestui aspect, CEPD ia notă de repetatele angajamente și asigurări oferite de Comisia Europeană și autoritățile japoneze cu privire la caracterul obligatoriu și executoriu al normelor suplimentare. CEPD invită Comisia Europeană să monitorizeze în continuu caracterul obligatoriu și punerea în aplicare efectivă a acestora în Japonia, deoarece valoarea lor legislativă este un element esențial în cadrul adecvării dintre UE și Japonia.**

50. Mai mult, Comisia Europeană face referire în mai multe secțiuni ale proiectului său de decizie privind nivelul adecvat la orientările CPP (orientările).

51. Cu toate că la considerentul 16 din proiectului său de decizie privind nivelul de protecție adecvat Comisia Europeană precizează că orientările furnizează o interpretare cu valoare de autoritate a APPI, în cadrul aceluiași considerent se face referire la caracterul obligatoriu al acestor orientări: „Potrivit informațiilor primite de la CPP, acele orientări sunt considerate ca norme obligatorii care sunt parte integrală a cadrului juridic și trebuie citite împreună cu textul APPI, decretul ministerial, normele CPP și o serie de întrebări și răspunsuri pregătite de CPP."[19]

52. Cu toate acestea, în accepțiunea CEPD în baza acelorași informații furnizate de CPP, orientările nu au caracter obligatoriu din punct de vedere juridic. Mai degrabă, acestea furnizează o „interpretare cu caracter de autoritate" a legii. CPP afirmă că orientările sunt

[18] Conform unui articol publicat în iulie 2018, dată la care normele suplimentare existau sub formă de proiect, era de așteptat ca obligativitatea juridică a acestor norme să facă obiectul unei dezbateri interne la nivel de țară. Vezi Fujiwara S., „Comparison between the EU and Japan's Data Protection Legal Frameworks", Jurist, vol. 1521 (iulie 2018): p. 19.

[19] Decizia de punere în aplicare a Comisiei din XXXX, în temeiul Regulamentului 2016/679 al Parlamentului European și al Consiliului privind nivelul de protecție adecvat a datelor cu caracter personal în Japonia, astfel cum a fost transmisă către CEPD la 13 noiembrie 2018, considerentul 16.

respectate în practică de operatorii care gestionează informații cu caracter personal, sunt folosite de CPP pentru aplicarea legii în contradictoriu cu operatorii care gestionează informații cu caracter personal și sunt folosite de instanțe în pronunțarea hotărârilor. Totuși, aceste elemente nu constituie dovezi suficiente că orientările sunt norme cu caracter obligatoriu din punct de vedere juridic.

53. **CEPD dorește să obțină clarificări în decizia privind nivelul de protecție adecvat în ceea ce privește natura obligatorie a orientărilor CPP și solicită Comisiei Europene să monitorizeze cu atenție acest aspect.**

54. Potrivit CPP, orientările sunt totuși respectate în practică, conform cutumei locale. CPP menționează că instanțele japoneze folosesc orientările CPP în pronunțarea hotărârilor la aplicarea normelor APPI. Comisia Europeană face referire la o hotărâre judecătorească[20] din 2006 de a furniza dovezi că instanțele din Japonia se bazează pe orientări în constatările lor. În pofida faptului că această hotărâre judecătorească nu i-a fost prezentată CEPD, acesta ar aprecia dacă Comisia Europeană ar furniza o hotărâre judecătorească mai recentă, fie din domeniul protecției datelor, fie dintr-un alt sector în care instanțele japoneze au utilizat orientările CPP sau alte orientări asemănătoare pentru a-și întemeia decizia.

2.3.5 Revizuirea periodică a constatării privind nivelul adecvat

55. Articolul 45 alineatul (3) din RGPD precizează că o revizuire periodică trebuie efectuată cel puțin o dată la patru ani. Potrivit criteriilor de referință ale CEPD privind nivelul de protecție adecvat[21], acesta este un cadru temporal general care trebuie adecvat la fiecare țară terță sau organizație internațională cu o decizie privind nivelul de protecție adecvat. În funcție de circumstanțele specifice în discuție, se poate garanta un ciclu mai scurt de revizuire. De asemenea, incidentele sau alte informații sau modificări privind cadrul juridic din țara terță sau organizația internațională în cauză ar putea declanșa nevoia efectuării unei revizuiri înainte de termen. De asemenea, pare oportun să se efectueze destul de rapid o primă revizuire a unei decizii complet noi privind nivelul de protecție adecvat și să se adapteze treptat ciclul de revizuire, în funcție de rezultate.

56. Luând în considerare o serie de factori, inclusiv faptul că APPI a intrat în vigoare în 2017, că CPP a fost înființată în 2016 și că deocamdată nu există informații sau dovezi cu privire la aplicarea practică a normelor suplimentare, **CEPD invită Comisia Europeană să efectueze o revizuire a acestei constatări privind nivelul adecvat (cel puțin) o dată la doi ani și nu o dată la patru ani.**

2.3.6 Angajamentele internaționale asumate de Japonia

57. Potrivit articolului 45 alineatul (2) litera (c) din RGPD și criteriilor de referință privind nivelul de protecție adecvat[22], atunci când evaluează nivelul de protecție adecvat dintr-o țară terță, Comisia Europeană ia în considerare, printre altele, angajamentele internaționale la care a aderat țara terță sau alte obligații care decurg din participarea țării terțe la sisteme multilaterale sau regionale, mai ales în domeniul protecției datelor cu caracter personal, precum și punerea în aplicare a acestor obligații. Mai mult, trebuie luate în considerare

[20] Decizia de punere în aplicare a Comisiei din XXXX, în temeiul Regulamentului 2016/679 al Parlamentului și Consiliului European privind nivelul de protecție adecvat a datelor cu caracter personal în Japonia, astfel cum a fost transmisă la CEPD la 13 noiembrie 2018, pagina 5, nota de subsol 16, „Tribunalul Regional din Osaka, decizia din 19 mai 2006, Hanrei Jiho, vol. 1948, p. 122.
[21] WP254, p.3.
[22] WP254, p.2.

aderarea țării terțe la Convenția Consiliului Europei din 28 ianuarie 1981 pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal („Convenția 108+”)[23] precum și protocolul adițional la aceasta.

58. **În acest sens, CEPD remarcă faptul că Japonia deține calitatea de observator al Comitetului Consultativ al Convenției 108+.**

2.3.7 Competențele autorității pentru protecția datelor (APD)[24] de a introduce acțiuni în instanță în ceea ce privește valabilitatea unei decizii privind nivelul de protecție adecvat

59. CEPD subliniază faptul că, deși considerentul 179 din proiectul de decizie privind nivelul de protecție adecvat menționează doar cazurile în care APD a primit o plângere care pune sub semnul întrebării compatibilitatea unei decizii privind nivelul de protecție adecvat cu drepturile fundamentale ale persoanelor în ceea ce privește protecția vieții private și a datelor, această declarație trebuie înțeleasă ca un exemplu de situație în care APD poate sesiza o instanță națională, lucru care poate fi posibil și în absența unei plângeri, mai degrabă decât sub forma unei restricționări a competențelor conferite în acest sens ADP-urilor în temeiul RGPD și a legislației naționale a statelor membre. Într-adevăr, prevederile RGPD includ atât competența de a suspenda transferurile de date chiar și atunci când acestea se bazează pe o decizie privind nivelul de protecție adecvat, cât și de a introduce o acțiune privind valabilitatea unei decizii privind nivelul de protecție adecvat, nu sunt limitate la cazurile în care s-a primit o plângere dacă, prin legislația națională, le-a fost conferită competența de a acționa în acest sens la nivel mai larg și indiferent de existența unei plângeri, în conformitate cu prevederile relevante din RGPD.

60. **CEPD invită Comisia Europeană să specifice clar în proiectul său de decizie privind nivelul de protecție adecvat dacă competența autorităților de supraveghere de a introduce o acțiune împotriva valabilității unei decizii privind nivelul de protecție adecvat în urma unei plângeri este doar o ilustrare a competențelor mai largi ale APD-urilor ce decurg din RGPD, inclusiv competența de a suspenda transferurile și de a introduce o acțiune cu privire la validitatea deciziei privind nivelul de protecție adecvat în absența unei plângeri, în situația în care legislația națională permite acest lucru.**

3 ASPECTE COMERCIALE

3.1 Principii privind conținutul

61. Capitolul 3 din criteriile de referință privind nivelul de protecție adecvat tratează „Principii referitoare la conținut”. Sistemul unei țări terțe sau organizații internaționale trebuie să le includă pentru ca nivelul de protecție conferit să fie echivalent, în esență, cu cel garantat prin legislația UE. CEPD recunoaște faptul că sistemul juridic japonez are o abordare diferită față de cea prevăzută de RGPD în scopul aplicării efective a dreptului la viața privată. Cu toate că dreptul la viața privată nu este prevăzut în constituția japoneză per se, acesta a fost

[23] Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, Convenția 108+, 18 mai 2018.
[24] Cauza C-362/14, Maximillian Schrems/ Comisarul pentru protecția datelor, 6 octombrie 2015.

recunoscut ca drept constituțional prin jurisprudență, astfel cum se menționează și în decizia Comisiei Europene[25].

62. În special deoarece abordarea japoneză diferă semnificativ de cea europeană, trebuie analizat cu atenție dacă întregul sistem oferă un nivel de protecție „echivalent în esență", nu doar aspecte izolate. Aceasta înseamnă că, posibilele „deficiențe" ale unui singur principiu privind conținutul ar putea fi compensate de alte aspecte care să asigure mecanisme de control și echilibrare.

3.1.1 Concepte

63. Pe baza criteriilor de referință privind nivelul de protecție adecvat, cadrul juridic al țării terțe trebuie să includă concepte și/sau principii de bază de protecție a datelor. Chiar dacă acestea nu trebuie să corespundă terminologiei RGPD, ele trebuie să reflecte conceptele consacrate în legislația europeană privind protecția datelor și să fie în concordanță cu acestea. De exemplu, RGPD include următoarele concepte importante: „date cu caracter personal", „prelucrarea datelor cu caracter personal", „operator de date", „persoană împuternicită de operator ", „destinatar" și „date cu caracter special"[26].

64. APPI mai include și o serie de definiții cum ar fi, printre altele, cele privind „informațiile cu caracter personal", „date cu caracter personal", „operator economic care gestionează informații cu caracter personal". **Cu toate acestea, se pare că APPI nu include o definiție a termenului „gestionarea datelor cu caracter personal" care este similar cu termenul „prelucrarea datelor cu caracter personal".**

65. În ceea ce privește definiția termenului „gestionarea datelor cu caracter personal", CPP a furnizat răspunsuri scrise întrebării CEPD cu privire la această definiție. Comisia Europeană a citat acest răspuns în proiectul de decizie al Comisiei *„Deoarece APPI nu folosește termenul de „prelucrare", aceasta se bazează pe conceptul echivalent de „gestionare" care, potrivit informațiilor primite de la CPP, acoperă „orice operațiune efectuată asupra datelor cu caracter personal" inclusiv achiziționarea, introducerea, acumularea, organizarea, stocarea, editarea/prelucrarea, reînnoirea, eliberarea, reasigurarea, producerea, utilizarea, sau furnizarea de informații cu caracter personal*." [27]

66. Cu toate acestea, deoarece textul de referință pentru această definiție nu a fost pus la dispoziție, CEPD invită **Comisia Europeană să monitorizeze îndeaproape respectarea efectivă, în practică, a definiției conceptului menționat mai sus, conform precizărilor CPP**.

3.1.1.1 Conceptul de persoană împuternicită de operator și obligațiile „mandatarului"

67. Așa cum s-a menționat mai sus, conform criteriilor de referință privind nivelul de protecție adecvat, cadrul legislativ al țării terțe trebuie să prevadă conceptele și/sau principiile de bază privind protecția datelor.

[25] Traducerea în limba engleză a acestei decizii a instanței nu a fost prezentată CEPD. Vezi Decizia de punere în aplicare a Comisiei din XXXX, în temeiul Regulamentului 2016/679 al Parlamentului European și al Consiliului privind nivelul de protecție adecvat a datelor cu caracter personal în Japonia, astfel cum a fost transmisă către CEPD la 13 noiembrie 2018, nota de subsol 9.
[26] WP254, p.4.
[27] Decizia de punere în aplicare a Comisiei din XXXX, în temeiul Regulamentului 2016/679 al Parlamentului European și al Consiliului privind nivelul de protecție adecvat a datelor cu caracter personal în Japonia, astfel cum a fost transmisă la CEPD la 13 noiembrie 2018, considerentul 17.

68. APPI include o definiție a „operatorului economic care gestionează informații cu caracter personal” care, potrivit Comisiei Europene, include atât termenul de „operator de date” cât și cel de „persoană împuternicită de operator”, astfel cum sunt prevăzuți în RGPD și nu face distincție între cei doi[28]. Cu toate acestea, APPI include la articolul 22 și termenul de „mandatar”, care este asemănător, în anumite aspecte, termenului de „persoană împuternicită de operator” în sensul RGPD.

69. După cum a explicat CPP în răspunsurile sale adresate CEPD, incluse și în proiectul de decizie al Comisiei Europene privind nivelul de protecție adecvat, un mandatar este considerat echivalentul operatorului de date în temeiul RGPD - fiindu-i încredințată gestionarea datelor cu caracter personal de către operatorii economici care gestionează informații cu caracter personal. Mandatarul are aceleași obligații și drepturi ca orice operator economic care gestionează informații cu caracter personal, inclusiv cele precizate în normele suplimentare privind datele cu caracter personal transferate din UE. Operatorul economic care gestionează informații cu caracter personal care încredințează gestionarea acestor date unui mandatar este obligat să „efectueze acțiuni de supraveghere adecvate și necesare”[29] asupra mandatarului.

70. **CEPD invită Comisia Europeană să explice statutul și obligațiile mandatarului atunci când mandatarul modifică scopurile și mijloacele prelucrării și să clarifice dacă consimțământului persoanei vizate rămâne o condiție necesară pentru o astfel de modificare a scopului sau stabilire a mijloacelor[30].**

3.1.1.2 Conceptul de date cu caracter personal stocate

71. APPI menționează conceptul de „date cu caracter personal stocate”, care sunt considerate o subcategorie a datelor cu caracter personal. Potrivit APPI, prevederile cu privire la drepturile persoanelor vizate[31] se aplică exclusiv datelor cu caracter personal stocate. Definiția datelor cu caracter personal stocate este inclusă în articolul 2 alineatul (7) din APPI.

72. Datele cu caracter personal stocate sunt date cu caracter personal, altele decât cele (i) prevăzute a fi eliminate într-un termen de maximum 6 luni[32] sau care (ii) intră sub incidența excepțiilor prevăzute la articolul 4 din decretul ministerial și care pot aduce atingere intereselor publice sau de altă natură dacă prezența sau absența lor devine cunoscută.

73. Norma suplimentară (2) precizează că „*datele cu caracter personal primite din UE pe baza deciziei privind nivelul adecvat trebuie gestionate ca date cu caracter personal stocate, indiferent de termenul de eliminare prevăzut în acest scop*”.

74. Cu toate acestea, pentru datele cu caracter personal care intră sub incidența excepțiilor prevăzute la articolul 4 din decretul ministerial nu va fi necesară gestionarea acestora ca date cu caracter personal stocate și drepturile persoanelor vizate nu se vor aplica.

---

[28] Decizia de punere în aplicare a Comisiei din XXXX, în temeiul Regulamentului 2016/679 al Parlamentului European și al Consiliului privind nivelul de protecție adecvat a datelor cu caracter personal în Japonia, astfel cum a fost transmisă la CEPD la 13 noiembrie 2018, considerentul 35.

[29] Articolul 22 din Legea modificată privind protecția informațiilor cu caracter personal (APPI), intrată în vigoare la 30 mai 2017.

[30] Articolul 23 alineatul (5) litera (i) din APPI. Vezi și secțiunea de mai jos privind principiul transparenței.

[31] Articolele 27-30 din APPI.

[32] Amendament la decretul ministerial de punere în aplicare a Legii privind protecția informațiilor cu caracter personal (decret ministerial), intrat în vigoare la 30 mai 2017, articolul 5.

75. Articolul 23 din RGPD prevede, asemenea articolului 4 din decretul ministerial, că legislația Uniunii sau a statului membru sub incidența căruia se află operatorul/persoana împuternicită de operator, poate restricționa domeniul de aplicare al obligațiilor aplicabile acestuia și drepturile disponibile pentru persoana vizată. Acest lucru este posibil printr-o măsură legislativă. Aceste restrângeri trebuie să respecte esența drepturilor și libertăților fundamentale și reprezintă o măsură necesară și proporțională într-o societate democratică.

76. În ceea ce privește conținutul excepțiilor prevăzute la articolul 4 din decretul ministerial, CEPD nu i-a fost prezentată o documentație suficientă privind limitările sau elementele suplimentare pentru clarificarea domeniului de aplicare ale acestor prevederi[33]. CEPD nu este în măsură să evalueze dacă limitările drepturilor persoanelor vizate sunt limitate la ceea ce s-ar considera strict necesar și proporțional în temeiul legislației UE, fiind astfel echivalent, în esență, cu drepturile conferite persoanelor vizate din UE.

77. **Datorită lipsei unor documente relevante, CEPD dorește primirea unor asigurări de la Comisia Europeană în legătură cu faptul că limitările cu privire la drepturile persoanelor fizice (în special, drepturile de acces, rectificare și opoziție) sunt necesare și proporționale într-o societate democratică și respectă esența drepturilor fundamentale.**

78. O cerință esențială a RGPD este protejarea datelor cu caracter personal de-a lungul întregului „ciclu de viață" al acestora.

79. Luând în considerare faptul că normele suplimentare se aplică exclusiv datelor cu caracter personal transferate din UE, CEPD ar aprecia să primească informații suplimentare cu privire la punerea în practică a acestor norme de către operatorii economici care gestionează informații cu caracter personal, în special atunci când aceste date sunt comunicate mai departe unui alt operator economic care gestionează informații cu caracter personal după prima lor transmitere în Japonia.

80. Comisia Europeană a clarificat în considerentul 15 din proiectul său de decizie privind nivelul de protecție adecvat că operatorii economici care gestionează informații cu caracter personal care primesc și/sau prelucrează ulterior date cu caracter personal din UE vor avea obligația juridică de a respecta normele suplimentare și, în acest scop, va fi necesar să se asigure că pot identifica astfel de date cu caracter personal de-a lungul întregului lor „ciclu de viață".

81. În răspunsurile sale, CPP[34]a explicat că această identificare va fi efectuată prin metode tehnice (etichetare) sau metode organizaționale (stocarea datelor provenind din UE într-o bază de date dedicată).

82. În nota de subsol 14 a proiectului său de decizie privind nivelul de protecție adecvat, Comisia Europeană explică faptul că operatorii economici care gestionează informații cu caracter personal trebuie să înregistreze informațiile privind originea datelor provenind din UE pentru atât timp cât este necesar în vederea îndeplinirii obligației de respectare a normelor suplimentare. Acest aspect este consacrat prin articolul 26 alineatele (1), (3) și (4) din APPI, care precizează că un operator economic care gestionează informații cu caracter personal are obligația de a confirma și a înregistra sursa acestor date și toate circumstanțele privind dobândirea acestor date.

[33] CEPD nu i-au fost prezentate deciziile Curții Supreme la care se face referire la considerentul 53 din proiectul de decizie privind caracterul adecvat al nivelului de protecție.
[34] Anexa III la prezentul aviz.

83. Cu toate acestea, CEPD remarcă faptul că articolul 18 din normele CPP[35] specifică că obligațiile operatorilor economici care gestionează informații cu caracter personal cu privire la păstrarea înregistrărilor sunt limitate la un termen de maximum trei ani în situațiile care nu intră în domeniul de aplicare a metodelor specifice de păstrare a înregistrărilor descrise la articolul 16 din normele CPP (utilizarea unui document scris, a unei înregistrări electromagnetice sau a unui microfilm). Acest aspect este, de asemenea, menționat de Comisia Europeană la considerentul 71 din proiectului său de decizie privind nivelul de protecție adecvat: *„Așa cum este specificat la articolul 18 din normele CPP, acele înregistrări trebuie păstrate pentru o perioadă de unul până la trei ani, în funcție de circumstanțe”*.

84. Chiar dacă, conform precizărilor Comisiei Europene din nota de subsol 14 din proiectul său de decizie privind nivelul de protecție adecvat, nu există interdicția ca operatorii economici care gestionează informații cu caracter personal să păstreze înregistrări cu privire la proveniența datelor mai mult de trei ani pentru a putea să-și îndeplinească obligațiile în baza normelor suplimentare (2), acest aspect nu este reflectat în mod clar nici în legislația japoneză, nici în normele suplimentare. CEPD consideră că există riscul ca operatorii economici care gestionează informații cu caracter personal să respecte, de fapt, prevederile articolului 18 din normele CPP chiar și la prelucrarea datelor provenite din UE. Aceasta se datorează, în principal, faptului că, în accepțiunea CEPD și conform documentelor disponibile, nu există în schimb nicio prevedere care să impună unui operator economic care gestionează informații cu caracter personal o astfel de obligație de respectare a normelor suplimentare. Aceasta ar avea drept consecință privarea datelor transferate din UE de protecția conferită prin protecțiile suplimentare incluse în normele suplimentare.

85. **CEPD invită Comisia Europeană să monitorizeze îndeaproape protejarea efectivă a datelor cu caracter personal transferate din UE către Japonia, în baza proiectului de decizie privind nivelul de protecție adecvat, de-a lungul întregului „ciclu de viață” al acestora, chiar dacă legislația japoneză impune obligația de păstrare a înregistrărilor cu privire la proveniența datelor pentru cel mult trei ani.**

3.1.2 Motive care justifică prelucrarea legală și echitabilă în scopuri legitime

86. Potrivit criteriilor de referință privind nivelul de protecție adecvat, în conformitate cu RGPD, datele trebuie prelucrate în mod legal, corect și legitim[36]. Temeiul juridic în baza căruia datele cu caracter personal pot fi prelucrate în mod legal, corect și legitim trebuie precizat într-un mod suficient de clar. Cadrul european recunoaște mai multe astfel de temeiuri legitime, inclusiv, de exemplu, dispozițiile din legislația națională, consimțământul persoanei vizate, executarea unui contract sau un interes legitim al operatorului de date sau al unui terț care nu prevalează asupra intereselor persoanei.

87. Conform APPI, consimțământul joacă un rol central în sistemul legislativ japonez de protecție a datelor. Consimțământul este temeiul juridic central pentru prelucrarea datelor cu caracter personal în Japonia și, de asemenea, unul dintre principalele temeiuri juridice pentru transferul datelor cu caracter personal din Japonia către o țară terță. Mai mult, consimțământul este necesar pentru modificarea scopului prelucrării.

88. Potrivit normelor suplimentare (3), temeiul juridic pentru prelucrarea datelor cu caracter personal transferate din UE în Japonia va fi temeiul juridic în baza căruia datele sunt

[35] Normele de punere în aplicare a legii privind protecția informațiilor cu caracter personal (Normele CPP), intrată în vigoare la 30 mai 2017, Articolul 16.
[36] WP254, p.4.

transferate în Japonia. Dacă operatorul economic care gestionează informații cu caracter personal dorește să prelucreze ulterior aceste date într-un scop diferit, acesta trebuie să obțină în prealabil consimțământul persoanei vizate.

89. CEPD consideră că, în special datorită rolului său central în cadrul legislativ japonez, calitatea consimțământului trebuie să respecte cerințele fundamentale ale noțiunii de consimțământ, de exemplu, potrivit legislației UE, o „*manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate* ...". Persoana vizată poate să-și retragă consimțământul ca garanție esențială a faptului că voința liberă a persoanei vizate este garantată în tot acest interval[37]. Dreptul de retragere, ca element obligatoriu al consimțământului, pare să lipsească din cadrul juridic japonez. Într-adevăr, potrivit orientărilor CPP[38], posibilitatea de retragere este doar „dezirabilă" și condiționată de „caracteristicile, dimensiunea și statutul activităților economice".

3.1.3 Principiul transparenței

90. În temeiul articolului 5 din RGPD, transparența este un principiu fundamental al sistemului de protecție a datelor din UE[39]. Conform criteriilor de referință privind nivelul de protecție adecvat, „transparența" este unul dintre principiile privind conținutul care trebuie luat în considerare la evaluarea nivelului de protecție echivalent în esență, asigurat de o terță țară. Principiul transparenței și echității urmărește să garanteze că persoana vizată deține controlul asupra datelor sale și că, în acest scop, îi vor fi furnizate, de regulă, informații în mod proactiv. În cazul Scutului de Confidențialitate, Grupul de Lucru „Articolul 29"[40], în avizul 1/2016, a făcut referire la anexa II, II 1 b din acordul privind Scutul de Confidențialitate (notificare către persoana fizică), precizând că, dacă datele nu sunt colectate în mod direct, o organizație trebuie să notifice persoana vizată, iar momentul notificării ar trebui să fie punctul la care datele sunt înregistrate de organizația parte la Scutul de Confidențialitate" (secțiunea 2.2.1.a). Punerea la dispoziția publicului a politicii privind confidențialitatea este un criteriu suplimentar (vezi secțiunea 2.2.1.b). Prin urmare, s-a considerat necesară informarea în mod direct a persoanei vizate deja în temeiul Directivei 95/46/CE.

91. Un prim motiv de îngrijorare constă în modul în care se furnizează informații persoanei vizate, în temeiul APPI. Potrivit articolului 27 alineatul (1) din APPI, un operator economic care gestionează informații cu caracter personal este obligat să furnizeze informațiile descrise la articolul 27 alineatul 1 din APPI prezentându-le sub o formă „astfel încât mandantul să-și dea seama". Cu toate acestea, formularea nu clarifică măsura în care operatorul economic care gestionează informații cu caracter personal trebuie să ia măsuri pozitive în vederea unei informări efective a persoanei vizate.

---

[37] RGPD, articolul 4 alineatul (11). Pentru informații suplimentare, vezi și orientările relevante ale CEPD privind consimțământul, WP259, 10 aprilie 2018.

[38] Consorțiul pentru cercetarea și analiza protecției datelor din punct de vedere juridic și tehnic (CPD), O evaluare a nivelului de protecție a datelor cu caracter personal asigurat de legislația japoneză, p. 46: „Mai mult, din punct de vedere al protecției drepturilor și intereselor unui mandant, cum ar fi consumatorul, este dezirabil, în cazul primirii unei solicitări de păstrare a datelor cu caracter personal din partea unui mandant, să se răspundă ulterior solicitării mandantului printr-o modalitate ca, de exemplu, oprirea etc. transmiterii de corespondență în mod direct sau încheierea în mod voluntar a unei întreruperi a utilizării etc., luând în considerare caracteristicile, dimensiunea și statutul activităților economice".

[39] WP 254, capitolul 3, punctul 7, p. 5; vezi și considerentul (39) din RGPD.

[40] Acest grup de lucru a fost instituit în temeiul articolului 29 din Directiva 95/46/CE. A fost un organism consultativ european independent pentru protecția datelor și a vieții private. Sarcinile sale sunt descrise la articolul 30 din Directiva 95/46/CE și la articolul 15 din Directiva 2002/58/CE. GL29 a devenit între timp CEPD.

92. **CEPD invită Comisia să clarifice înțelesul termenului „poate să-și dea seama” și dacă APPI asigură, de regulă, obligația de informare efectivă a persoanei vizate.**

93. Mai mult, potrivit criteriilor de referință privind nivelul de protecție adecvat, pot exista restricții privind informațiile ce urmează a fi furnizate persoanei vizate, asemănător prevederilor articolului 23 din RGPD. Mergând pe o linie similară, articolul 14 alineatul (5) din RGPD prevede o excepție de la dreptul de a fi informat dacă informațiile sunt susceptibile să facă imposibilă sau să afecteze în mod grav realizarea prelucrării respective. Cu toate acestea, chiar și în acest caz, operatorul va furniza un anumit tip de informații, de exemplu, prin punerea la dispoziția publicului a unor informații „generalizate”. Mai mult, atunci când riscul încetează să mai existe, persoana vizată va fi notificată[41]. Aceste aspecte sunt importate în vederea asigurării principiului fundamental al echității.

94. În temeiul articolului 23 din APPI, un operator economic care gestionează informații cu caracter personal trebuie să furnizeze în general, în prealabil, informații persoanei vizate cu privire la furnizarea datelor sale către un terț fie în mod implicit prin obținerea consimțământului acestuia/acesteia, fie în mod explicit printr-o notificare de neparticipare voluntară. CEPD înțelege că nu există notificări transmise persoanei vizate pentru a o informa că datele sale nu sunt date cu caracter personal păstrate în temeiul APPI, deoarece acestea se află sub incidența excepțiilor de la articolul 4 din decretul ministerial. Drept urmare, aceste persoane nu vor putea beneficia pe deplin de drepturile lor. Persoanele vizate nu sunt informate nici în cazurile prevăzute la articolul 18 alineatul (4) din APPI.

95. **CEPD recunoaște faptul că este posibil ca drepturile să fie restricționate din cauza unor obiective legitime urmărite de operatorul economic care gestionează informații cu caracter personal și autoritățile de stat. În același timp, CEPD consideră că ar trebui să existe cel puțin o informare generală prealabilă referitoare la posibilitatea de restricționare a drepturilor din cauza unor obiective la care se face referire prin lege și că persoana vizată trebuie să fie notificată atunci când riscurile din cauza cărora informațiile sunt restricționate încetează să mai existe.**

96. În cele din urmă, alte aspecte privind transparența sunt dezvoltate în continuare. Acestea se referă la riscurile pe care le implică transferul către o țară terță[42] și informațiile asupra raționamentului prelucrării în contextul unei practici decizionale automatizate, inclusiv crearea de profiluri.[43]

3.1.4 Restricții privind transferurile ulterioare

97. CEPD salută eforturile autorităților japoneze și Comisiei Europene de întărire a nivelului de protecție în ceea ce privește transferurile ulterioare prin normele suplimentare (4), prin care se exclude posibilitatea de transfer ulterior a datelor cu caracter personal din UE către o țară terță în baza APEC (Organizația de Cooperare Economică Asia-Pacific) - CBPR (norme transfrontaliere privind confidențialitatea). În plus, CEPD recunoaște faptul că în considerentele 177 și 184 din noul său proiect de decizie privind nivelul adecvat, Comisia Europeană s-a angajat să suspende decizia privind nivelul adecvat atunci când transferurile ulterioare nu mai asigură continuitatea protecției. Cu toate acestea, CEPD dorește să atragă

[41] Tele2, cauzele reunite C 203/15 și C 698/15, hotărârea Curții, 21 decembrie 2016, rec. 121 și Drepturile digitale Irlanda, Cauzele reunite C-293/12 și C-594/12, hotărârea Curții, 8 aprilie 2014, rec. 54-62.
[42] Vezi secțiunea 2.1.4.
[43] Vezi secțiunea 2.1.6.

atenția asupra a două aspecte în ceea ce privește transferurile datelor cu caracter personal UE din Japonia către țări terțe.

98. **Utilizarea consimțământului ca temei pentru transferurile de date din Japonia către o țară terță în cadrul sistemului legislativ japonez dă naștere unor motive de îngrijorare datorită faptului că CEPD consideră că informațiile oferite persoanelor vizate din UE în prealabil acordării consimțământului nu par să fie cuprinzătoare.**

99. Articolul 24 din APPI interzice transferul datelor cu caracter personal către o terță parte în afara teritoriului Japoniei fără consimțământul acordat în prealabil al persoanei fizice vizate. Norma suplimentată (4) stipulează că persoanelor vizate din UE trebuie să li se ofere informații cu privire la circumstanțele privind transferul, acestea fiind necesare pentru a decide dacă să-și dea sau nu consimțământul.

100. În proiectul său de decizie privind nivelul de protecție adecvat, Comisia Europeană concluzionează că norma suplimentară (4) garantează persoanelor vizate din UE posibilitatea de a-și da consimțământul în cunoștință de cauză[44] deoarece acestea vor fi informate că datele urmează să fie transferate în străinătate și din țara respectivă de destinație. Acest lucru ar permite persoanei vizate să evalueze riscul asupra confidențialității pe care îl implică transferul.

101. În baza principiului transparenței din criteriile de referință privind nivelul de protecție adecvat, persoanele fizice vor fi informate asigurându-se un anumit grad de echitate. În contextul realizării unor transferuri ulterioare pe baza consimțământului, CEPD consideră că, pentru a garanta persoanelor vizate un grad adecvat de echitate, acestea trebuie informate în mod explicit cu privire la riscurile posibile asociate respectivelor transferuri ce decurg din absența unei protecții adecvate în țara terță și din absența unor garanții adecvate înainte ca persoanele vizate să-și dea consimțământul. Această notificare trebuie să includă, de exemplu, informații cu privire la posibilitatea ca, în țara terță, să nu existe o autoritate de supraveghere și/sau principii de prelucrare a datelor și/sau drepturile persoanelor vizate ar putea să nu fie garantate în țara terță[45]. Pentru CEPD, furnizarea acestor informații este esențială pentru a permite persoanelor vizate să-și dea acordul în deplină cunoștință a acestor elemente specifice transferului[46].

102. Consimțământul exprimat în cunoștință de cauză este, de asemenea, important în ceea ce privește excluderile sectoriale. Decizia privind nivelul de protecție adecvat nu acoperă anumite tipuri de prelucrare de către anumite organisme, cum sunt universitățile, în vederea prelucrării datelor cu caracter personal în scopuri academice. Motivul de îngrijorare al CEPD, în acest caz, se referă la scenariul specific în care datele transferate din UE în baza deciziei privind nivelul adecvat - de exemplu, datele (legate de resursele umane) studenților Erasmus în Japonia - sunt folosite într-un scop diferit care nu intră sub incidența deciziei privind nivelul de protecție adecvat (de exemplu, scopuri de cercetare), în baza consimțământului

[44] Decizia de punere în aplicare a Comisiei din XXXX, în temeiul Regulamentului 2016/679 al Parlamentului și European și al Consiliului privind nivelul de protecție adecvat a datelor cu caracter personal în Japonia, astfel cum a fost transmisă la CEPD la 13 noiembrie, considerentul 76.

[45] Orientările CEPD 2/2018 privind derogărilor de la articolul 49 în conformitate cu Regulamentul 2016/679, 25 mai 2018, p.8.

[46] Orientările CEPD 2/2018 privind derogărilor de la articolul 49 în conformitate cu Regulamentul 2016/679, 25 mai 2018, p.7.

persoanei vizate - și, așadar, nu mai sunt acoperite de protecția suplimentară oferită de normele suplimentare.

103. Comisia Europeană declară în considerentul 38 din proiectul său de decizie privind nivelul de protecție adecvat, că un astfel de scenariu se află sub incidența transferurilor ulterioare și că, atunci când acest lucru se va întâmpla, operatorul economic care gestionează informații cu caracter personal trebuie să furnizeze persoanei vizate toate informațiile necesare înainte de a obține consimțământul său, inclusiv faptul că informațiile cu caracter personal nu vor beneficia de protecția asigurată prin normele APPI.

104. Norma suplimentară (4) impune operatorului economic care gestionează informații cu caracter personal obținerea consimțământului persoanei doar după ce i s-au furnizat acesteia informații cu privire la circumstanțele privind transferul, necesare mandantului să decidă cu privire la acordarea consimțământului.

105. **CEPD invită Comisia Europeană să se asigure că informațiile care trebuie furnizate persoanei vizate „asupra circumstanțelor privind transferul" vor include informații despre riscurile posibile asociate transferurilor ce decurg din absența unei protecții adecvate în țara terță și din absența unor garanții adecvate sau, în cazul excluderilor sectoriale, din absența protecției asigurate de normele suplimentare și APPI.**

106. **Transferurile ulterioare de date cu caracter personal pot surveni către țări terțe care pot deveni obiectul unei decizii ulterioare a Japoniei privind caracterul adecvat.**

107. Fără a aduce atingere derogărilor prevăzute în articolul 23 paragraful 1 din APPI, datele transferate inițial din UE către Japonia pot fi apoi transferate din Japonia către o țară terță fără obținerea consimțământului în două cazuri:

- Dacă operatorul economic care gestionează informații cu caracter personal și terțul destinatar au implementat împreună măsuri în vederea asigurării unui nivel de protecție echivalent cu cel asigurat de APPI împreună cu normele suplimentare prin intermediul unui contract sau alte forme de acorduri cu caracter obligatoriu sau acorduri cu caracter obligatoriu în cadrul unui grup corporatist[47].
- Dacă țara terță a fost recunoscută de către CPP în temeiul articolului 24 din APPI și al articolului 11 din normele CPP[48] ca asigurând un nivel de protecție echivalent cu cel garantat în Japonia.

108. CEPD evaluează articolul 24 din APPI drept o normă mai specifică, care conține o derogare de la norma cu caracter general în temeiul articolului 23 din APPI. Prin urmare, CEPD nu împărtășește evaluarea Comisiei Europene în ultima propoziție nouă din considerentul 78 al proiectului de decizie privind nivelul adecvat, precizând că inclusiv în acele cazuri, transferul către terț va intra sub incidența obligației de obținere a consimțământului în temeiul articolului 23 alineat (1) din APPI.

109. În temeiul articolului 11 alineatul (1) din normele CPP, decizia CPP privind nivelul de protecție adecvat necesită standarde materiale echivalente celor prevăzute în APPI, a căror implementare să fie asigurată în țara terță și care să fie supravegheate efectiv de o autoritate

[47] Norma suplimentară (4) (ii).

[48] Normele de punere în aplicare pentru Legea privind protecția informațiilor cu caracter personal, 30 mai 2017. O traducere în limba engleză a noului articol 11 a fost transmisă de către Comisia UE către CEPD, dar acest articol nu a fost publicat încă.

independentă de aplicare a legii. Mai mult, CPP poate impune condițiile necesare în vederea protejării drepturilor și intereselor persoanelor fizice din Japonia, în conformitate cu articolul 11 alineatul (2) din normele CPP.

110. Norma suplimentară (4) prevede că datele cu caracter personal din UE pot fi transferate către o țară terță care face obiectului unei decizii privind nivelul adecvat din Japonia fără alte restricții. Dar articolul 44 din RGPD precizează că orice transfer de date cu caracter personal către o țară terță trebuie să îndeplinească condițiile prevăzute la capitolul V din RGPD, inclusiv transferurile ulterioare dintr-o țară terță către o altă țară terță. Nivelul de protecție al persoanelor fizice ale căror date sunt transferate nu trebuie să fie subminat de transferul ulterior[49]. Cu toate că această interpretare este, în principiu, împărtășită și de Comisia Europeană în proiectul său de decizie privind nivelul adecvat[50], se pare că aceasta nu este respectată întocmai. Comisia Europeană a negociat interzicerea faptului ca datele provenind din UE să fie transferate către o țară terță în cadrul Organizației de Cooperare Economică Asia-Pacific (APEC) - Norme transfrontaliere privind confidențialitatea (CBPR). Prin prisma instrumentului comparativ dezvoltat în 2014 în cadrul Directivei UE între regulile corporatiste obligatorii (BCR) și CBPR care arată cerințele ambelor sisteme, punctele de convergență și diferențele dintre acestea (Avizul WP29 02/2014), CEPD are suspiciuni cu privire la utilizarea CBPR drept instrument de transfer ulterior pentru datele cu caracter personal transferate din UE către țări din afara Japoniei.

111. În schimb, transferurile ulterioare de date cu caracter personal transferate din UE către Japonia în baza deciziei privind nivelul adecvat al Japoniei, pare să fie acceptată de către Comisia Europeană, fără a-i lăsa CPP posibilitatea de a impune normele suplimentare drept condiții în vederea protejării drepturilor și intereselor persoanelor fizice din UE, dacă este cazul. CEPD deduce din articolul 44 din RGPD că protecția sporită a datelor transferate din UE în Japonia prevăzută în normele suplimentare trebuie extinsă întotdeauna atunci când datele cu caracter personal transferate din UE în Japonia sunt transferate ulterior către o țară terță, în cazul în care cadrul de protecție a datelor din țara respectivă nu este recunoscut ca fiind echivalent, în esență, celui prevăzut de RGPD.

112. **Prin urmare, CEPD invită Comisia Europeană să își preia rolul de monitorizare și să se asigure că nivelul de protecție al datelor UE este menținut sau să ia în considerare suspendarea acestei decizii privind nivelul adecvat dacă datele cu caracter personal transferate din UE în Japonia sunt transferate ulterior către țări terțe care pot face obiectul unei decizii ulterioare a Japoniei privind nivelul adecvat dacă aceste țări terțe nu au făcut obiectul unei evaluări sau constatări a nivelului adecvat de către UE în prealabil.**

3.1.5 Marketingul direct

113. Potrivit normei suplimentare (3), unui operator economic care gestionează informații cu caracter personal i se interzice prelucrarea datelor cu caracter personal în scopuri de marketing direct dacă acestea au fost transferate din Uniunea Europeană în alt scop și dacă persoana vizată din UE nu și-a dat consimțământul în vederea modificării scopului de utilizare.

[49] WP 254, p.5.

[50] Decizia de punere în aplicare a Comisiei din XXXX, în temeiul Regulamentului 2016/679 al Parlamentului și Consiliului European privind nivelul de protecție adecvat a datelor cu caracter personal în Japonia, transmisă către CEPD la 13 noiembrie, considerentul 75.

114. Potrivit criteriilor de referință privind nivelul de protecție adecvat, dacă datele sunt prelucrate în scopuri de marketing direct, persoana vizată trebuie să aibă posibilitatea, în orice moment și fără percepere de taxe, de a se opune prelucrării datelor sale în astfel de scopuri. Potrivit articolului 16 din APPI, un operator economic care gestionează informații cu caracter personal poate prelucra informații cu caracter personal doar cu consimțământul persoanei vizate. Retragerea consimțământului ar putea conduce la același rezultat precum dreptul privilegiat de a se opune marketingului direct.

115. Cadrul japonez privind protecția datelor nu prevede un drept privilegiat de contestare și, conform celor explicate mai sus în secțiunea privind consimțământul, retragerea consimțământului în baza Orientărilor CPP este numai dezirabilă și condițională și, așadar, nu poate fi considerată ca echivalând cu dreptul de contestare în orice moment conform celor prevăzute în Criteriile de referință privind nivelul adecvat. **CEPD invită Comisia Europeană să ofere noi asigurări cu privire la dreptul de retragere a consimțământului și să monitorizeze cazurile care implică marketingul direct.**

3.1.6 Procesul decizional automatizat și crearea de profiluri

116. Potrivit criteriilor de referință privind nivelul de protecție adecvat, deciziile care se bazează exclusiv pe prelucrarea automatizată (procesul decizional individual automatizat), inclusiv crearea de profiluri, care produc efecte juridice sau afectează în mod semnificativ persoana vizată, pot fi luate doar în anumite condiții stabilite prin cadrul juridic din țara terță. Așadar, de fiecare dată când un proces decizional individual automatizat și o creare de profiluri sunt efectuate în cadrul circumstanțelor menționate mai sus, acestea trebuie să se bazeze pe un temei legal.

117. În cadrul juridic european, condițiile aferente procesului decizional automatizat includ, de exemplu, necesitatea obținerii consimțământului explicit[51] al persoanelor vizate sau necesitatea unei astfel de decizii în vederea încheierii unui contract. Dacă decizia nu respectă condițiile stipulate în cadrul juridic al țării terțe, persoana vizată trebuie să aibă dreptul de a nu face obiectul acestuia. Mai mult, în orice caz, legislația țării terțe trebuie să asigure garanțiile necesare, inclusiv dreptul de a fi informat cu privire la motivele specifice care stau la baza deciziei și raționamentul folosit pentru a rectifica informațiile inexacte sau incomplete și a contesta decizia atunci când aceasta a fost adoptată pe baza unor elemente factuale incorecte.

118. Decizia Comisiei se referă exclusiv la sectorul bancar atunci când se aplică regulile sectoriale[52] în ceea ce privește deciziile automatizate. Orientările cuprinzătoare privind Supravegherea marilor bănci din considerentul 93 al proiectului de decizie privind nivelul de protecție adecvat indică faptul că persoanei respective trebuie să i se ofere explicații specifice cu privire la motivele respingerii solicitării de încheiere a unui contract de creditare.

119. Argumentația Comisiei Europene cu privire la proiectul de decizie privind nivelul de protecție adecvat (considerentul 94), potrivit căreia absența unor reguli specifice cu privire la procesul decizional automatizat din APPI este puțin susceptibilă să afecteze nivelul de protecție, pare (de exemplu) să nu ia în considerare situația în care datele cu caracter personal transferate

[51] Pentru observații critice referitoare la conceptul de consimțământ în cadrul juridic japonez privind protecția datelor, vezi: 2.1. Considerente generale și 2.2.8. Marketingul direct.

[52] Aceste norme sectoriale nu au fost prezentate CEPD.

din UE sunt prelucrate ulterior de către un alt operator de date japonez (diferit de importatorul japonez inițial al datelor).

120. Se pare, așadar, că nu există norme generale aplicabile la nivel sectorial în Japonia care să guverneze procesul decizional automatizat și de creare de profiluri.

121. **CEPD invită Comisia Europeană să monitorizeze cazurile referitoare la procesul decizional automatizat și de creare de profiluri.**

3.2 Mecanisme procedurale și de punere în aplicare

122. În baza criteriilor prevăzute în criteriile de referință privind nivelul de protecție adecvat, CEPD a analizat următoarele aspecte din cadrul juridic japonez privind protecția datelor așa cum este reglementat în proiectul de decizie privind nivelul de protecție adecvat: existența și funcționarea efectivă a unei autorități independente de supraveghere; existența unui sistem care să asigure un nivel de respectare adecvat și un sistem de acces la mecanismele de recurs adecvate care să asigure persoanelor fizice din UE mijloacele de exercitare a drepturilor și căi de atac fără obstacole dificile în mecanismele de recurs juridice și administrative.

123. Plecând de la parametrii stabiliți de CJUE în cauza Schrems[53] și de la cei evidențiați în considerentul 104 și la articolul 45 din RGPD, CEPD constată că, deși în Japonia există un sistem compatibil cu cel european, acest sistem poate fi dificil de accesat în practică de persoanele fizice din UE ale căror date vor fi transferate în temeiul acestei decizii privind nivelul de protecție adecvat, prin prisma existenței unor bariere lingvistice și instituționale.

124. Secțiunile de mai jos vor examina aspectele cadrului japonez menționate anterior, înainte de a propune recomandări Comisiei.

3.2.1 Autoritatea de supraveghere independentă competentă

125. CPP a fost constituită la 1 ianuarie 2016 ca urmare a amendamentelor aduse la APPI din 2015, înlocuind comisia precedentă - Comisia pentru protecția informațiilor cu caracter personal specifice (constituită în 2013 în temeiul documentului „My Number Act"). Chiar dacă este o organizație tânără, de la constituirea sa, CPP a depus eforturi considerabile în vederea construirii infrastructurii necesare punerii în aplicare a APPI modificate. Dintre acestea, sunt de remarcat normele CPP, orientările CPP al căror scop este îndrumarea operatorului economic care gestionează informații cu caracter personal în interpretarea APPI, publicarea unui document de tipul întrebări și răspunsuri[54] despre CPP și înființarea unei linii de asistență telefonică pentru a-i consilia pe operatorii economici și pe cetățeni cu privire la prevederile în domeniul protecției datelor, precum și înființarea unui serviciu de mediere pentru gestionarea reclamațiilor.

126. Constituirea și funcționarea CPP este reglementată în capitolul V din APPI. Cu toate că CPP cade sub jurisdicția Primului Ministru, articolul 62 autorizează funcționarea CPP în mod independent. CEPD salută clarificarea efectuată de către Comisia Europeană în proiectul modificat de decizie a nivelului adecvat prezentat la 13 noiembrie 2018 în sensul unei descrieri mai ample a măsurii în care CPP rămâne independentă de influențe interne sau externe.

[53] Cauza 362/14 (2015) Maximillian Schems/Comisarul pentru protecția datelor, (punctele 73 și 74).
[54] Acest document nu a fost prezentat de către Comisia Europeană către CEPD în limba engleză.

3.2.2 Sistemul de protecție a datelor trebuie să asigure un nivel adecvat de respectare

127. Proiectul de decizie privind nivelul adecvat procedează la o examinare cuprinzătoare a competențelor de care dispune CPP în temeiul articolelor 40, 41 și 42 din APPI în vederea asigurării monitorizării și punerii în aplicare a legislației. Articolul 40 abilitează CPP să solicite operatorului economic care gestionează informații cu caracter personal să depună rapoarte și documentație cu privire la operațiunile de prelucrare, precum și să efectueze inspecții la fața locului. În temeiul articolului 42, CPP are competența - atunci când se recunoaște necesitatea protejării drepturilor individuale sau când este constatată o încălcare a prevederilor legii - de a emite recomandări, iar dacă acestea eșuează, să emită ordine către operatorii economici care gestionează informații cu caracter personal, în vederea suspendării acțiunii de încălcare sau să ia măsurile necesare pentru a rectifica încălcarea respectivă.

128. În octombrie 2018, CPP a inițiat una dintre primele sale acțiuni în temeiul articolului 41 din APPI modificată și a emis „orientări" destinate unui operator economic care gestionează informații cu caracter personal, recomandând companiei să-și întărească măsurile de securitate și să supravegheze efectiv furnizorii aplicațiilor, oferind explicații clare și ușor de înțeles utilizatorilor despre modul în care sunt utilizate informațiile lor cu caracter personal, recomandându-i, de asemenea, să obțină consimțământul în prealabil atunci când informațiile sunt împărtășite cu un terț și să răspundă prompt solicitării utilizatorilor de ștergere a informațiilor acestora. În răspunsurile oferite către CEPD[55], funcționarii CPP au făcut cunoscut acordul companiei de a coopera în acest sens și au declarat că, în caz contrar, îi vor face o „recomandare" în temeiul articolului 42 alineatul (1) din APPI.

129. Investigația derulată de CPP asupra operatorului economic care gestionează informații cu caracter personal menționat mai sus este un indicator pozitiv al eforturilor autorității de supraveghere japoneze de a asigura un bun nivel de conformitate la nivelul țării.

130. Cu toate că există îmbunătățiri în ceea ce privește cadrul existent comparativ cu perioada anterioară amendamentelor din 2015, CEPD remarcă faptul că CPP deține mai puține competențe comparativ cu o APD europeană în temeiul RGPD, în special în ceea ce privește **punerea în aplicare**. De exemplu[56], amenzile administrative sunt destul de blânde. Decizia Comisiei Europene subliniază în recitalul 108 faptul că, în situații de nerespectare sau în anumite cazuri de încălcare a APPI, vor fi impuse sancțiuni penale și că CPP poate redirecționa cazurile către procuratură. Cu toate acestea, decizia Comisiei Europene nu ia în considerare faptul că în Japonia, urmărirea în justiție are caracter discreționar și uneori, poate constitui obiectul unor procese îndelungate de revizuire[57]. Mai mult, pedeapsa cu închisoare (cu sau fără muncă) asociată cu încălcări ale APPI în temeiul prevederilor capitolului VII poate fi dificil de executat deoarece vizează persoane fizice și, în orice caz, nu sancționează operatorul economic care gestionează informații cu caracter personal în calitate de entitate juridică care nu își exercită obligațiile privind responsabilitatea.

[55] Anexa III.

[56] Acestea sunt stipulate în capitolul VII din APPI. Pedeapsa maximă prevăzută de art. 83 (furnizarea sau utilizarea în secret a unei baze de date ce conține informații cu caracter personal pentru profitul ilegal propriu sau al unui terț) și este echivalentă fie cu un an de închisoare cu muncă, fie cu o amendă care nu depășește 500.000 yeni (aproximativ 3900 EUR). Potrivit explicațiilor furnizate de către Comisie, amenzile sunt cumulative per încălcare. Deși acest lucru poate fi valabil, CEPD remarcă că, chiar dacă sunt aplicate amenzi cumulative, suma totală poate rămâne considerabil mai scăzută față de standardele europene.

[57] Oda H., Japanese Law, Oxford University Press (ediția a III-a), 2009: 439 – 440.

131. **Având în vedere cele de mai sus, CEPD invită Comisia Europeană să monitorizeze îndeaproape eficacitatea sancțiunilor și măsurilor reparatorii relevante din sistemul japonez de protecție a datelor.**

3.2.3 Sistemul de protecție a datelor trebuie să furnizeze sprijin și să ajute persoanele vizate persoane fizice în exercitarea drepturilor acestora și a mecanismelor reparatorii adecvate

132. CPP oferă indicații și orientări detaliate pe site-ul său în vederea sensibilizării operatorilor economici care gestionează informații cu caracter personal cu privire la obligațiile și responsabilitățile care le revin conform cadrului privind protecția datelor precum și o linie de asistență telefonică pentru oferirea de informații și sprijin cetățenilor japonezi cu privire la drepturile lor ca persoane fizice, conform APPI. Site-ul are și o secțiune, denumită „Camera copiilor", dedicată în mod explicit publicului format din copii și tineri. CEPD remarcă faptul că aceste informații - împreună cu sprijinul oferit prin linia de asistență telefonică, orientările și documentația de tipul întrebări și răspunsuri - sunt disponibile în limba japoneză[58]. Așadar, CEPD crede cu tărie că ar fi benefic dacă CPP ar putea pune la dispoziție o pagină dedicată pe baza versiunii în limba engleză a site-ului destinată furnizării de informații despre drepturile persoanelor fizice conform cadrului japonez privind protecția datelor și normelor suplimentare pentru persoanele fizice din UE ale căror date vor fi transferate în temeiul deciziei Comisiei Europene privind nivelul adecvat .

133. CEPD salută clarificarea făcută de Comisia Europeană în considerentul 104 din proiectul modificat de decizie privind nivelul adecvat prezentat la 13 noiembrie 2018 cu privire la serviciul de mediere gestionat de către CPP în temeiul articolului 61 alineatul (ii) din APPI. Cu toate acestea, CEPD dorește să atragă atenția asupra a două aspecte în acest sens. În primul rând, serviciul de mediere nu este disponibil publicului în versiunea în limba engleză a site-ului CPP. În al doilea rând, serviciul este accesibil doar telefonic și disponibil în limba japoneză. În cele din urmă, medierea este un proces de facilitare care nu conduce la un acord cu caracter obligatoriu între părți și care are implicații asupra eficacității opțiunilor de soluționare puse la dispoziția persoanelor vizate[59].

134. În cele din urmă, CEPD remarcă faptul că proiectul de decizie privind nivelul adecvat pune accentul pe căile de atac disponibile prin acțiuni de drept civil precum și procedurile penale, dar nu recunoaște existența unor **bariere instituționale în soluționarea litigiilor** în Japonia cum ar fi cheltuielile judecătorești (taxele de judecată sunt împărțite în mod egal între reclamant și pârât, indiferent de partea care câștigă în cadrul procedurilor[60]), lipsa avocaților din țară[61], faptul că avocaților străini nu li se permite practicarea dreptului intern, precum și cerința privind sarcina probei în temeiul Legii răspunderii civile delictuale. CEPD îi este teamă că acești factori ar putea - în practică - împiedica accesul persoanelor fizice la justiție și periclita dreptul acestora de a apela la căi juridice de atac în mod rapid și fără suportarea unor costuri prohibitive.

---

[58] https://www.ppc.go.jp/en/contactus/piinquiry/.

[59] Kojima T., *Civil Procedure and ADR in Japan*, Chuo University Press, 2004; și Menkel-Meadow C., *Dispute Processing and Conflict Resolution: Theory, Practice and Policy*, Ashgate (2003) (ed.).

[60] Wagatsuma (2012), 'Recent Issues of Cost and Fee Allocation in Japanese Civil Procedure' in Reimann (ed.), Cost and Fee Allocation in Civil Procedure – Ius Gentium; comparative Perspectives on Law and Justice Vol. 11, pp. 195 – 200.

[61] Potrivit celor mai recente date, numărul avocaților din Japonia este de 38.980 (aproximativ 290 de avocați pentru un milion de persoane [Japan Federation of Bar Association] (2017), White Paper on Attorneys: p. 8 – 9.

135. Având în vedere cele de mai sus, CEPD **este îngrijorată de faptul că există un risc ca persoanele fizice din UE să aibă dificultăți în accesarea căilor de atac administrative și judiciare** și, așadar, dorește ca Comisia Europeană să discute cu CPP posibilitatea de înființare a unui serviciu online, disponibil cel puțin în limba engleză, **dedicat furnizării de sprijin și gestionării reclamațiilor[62] persoanelor fizice din UE.** În plus, CEPD dorește ca APD UE să aibă posibilitatea de a acționa în calitate de intermediar pentru plângerile persoanelor vizate din UE pe lângă organizațiile care operează în Japonia și CPP.

4 REFERITOR LA ACCESUL AUTORITĂȚILOR PUBLICE LA DATELE TRANSFERATE ÎN JAPONIA

136. Intenția COM este de a recunoaște, prin decizia privind nivelul adecvat, faptul că „Japonia asigură un nivel adecvat de protecție datelor cu caracter personal transferate din UE operatorilor economici din Japonia care gestionează informații cu caracter personal", conform celor stipulate în articolul 1 al proiectului de decizie privind nivelul adecvat. În conformitate cu articolul 45 alineatul (2) din RGPD, COM a analizat, de asemenea, limitările și garanțiile în ceea ce privește accesul autorităților publice la datele cu caracter personal. Acest capitol se axează pe evaluarea accesului autorităților de aplicare a legii și a altor entități guvernamentale la datele cu caracter personal în scopuri de securitate națională. Analiza CEPD se bazează pe proiectul de decizie privind nivelul de protecție adecvat, anexa II, în care guvernul japonez oferă o privire de ansamblu a cadrului juridic relevant, și textele legislative japoneze, în măsura în care acestea au fost furnizate de COM. Așadar, în contextul specific al acestei evaluări, CEPD a luat în considerare elemente cu privire la legislația japoneză care nu au fost incluse în constatările Comisiei Europene, dar care sunt relevante în vederea evaluării condițiilor și garanțiilor în temeiul cărora autoritățile publice japoneze pot accesa datele cu caracter personal transferate din UE.

4.1 Accesul la date în vederea aplicării legii

4.1.1 Procedurile pentru accesarea datelor din domeniul dreptului penal

137. Proiectul de decizie privind nivelul adecvat prezintă trei modalități prevăzute de legislația japoneză pentru ca autoritățile de aplicare a legii să aibă acces la date în Japonia:

4.1.1.1 Solicitările de acces cu mandat judecătoresc

138. Proiectul de decizie privind nivelul adecvat precizează că pentru ca guvernul să aibă acces la date în Japonia, și în special pentru ca autoritățile de aplicare a legii penale să solicite acces la probele electronice în contextul cercetărilor penale, acestea vor avea întotdeauna nevoie de un mandat, cu excepția situației în care recurg la procedura de prezentare voluntară a informațiilor - vezi mai jos.

4.1.1.1.1 Cerința „cauzei adecvate", necesității și proporționalității mandatelor

139. CEPD recunoaște faptul că în temeiul constituției japoneze, orice colectare a datelor cu caracter personal prin intermediul unor mijloace obligatorii trebuie să se bazeze pe mandat judecătoresc. Mai precis, proiectul de decizie privind nivelul adecvat indică faptul că în toate cazurile de „percheziție și sechestru", trebuie emise mandate judecătorești pentru „cauza adecvată", acestea fiind considerate de Curtea Supremă ca existând doar atunci când

[62] Într-un mod similar celui prevăzut în anexa II a acestei decizii privind caracterul adecvat pentru reclamațiile provenite de la rezidenți UE cu privire la accesul autorităților publice japoneze la datele acestora.

persoana fizică în cauză (suspectul sau acuzatul) este considerată a fi săvârșit o infracțiune, iar percheziția și sechestrul sunt necesare pentru derularea cercetării penale. În cazul de față COM face trimitere la hotărârea Curții Supreme din 18 martie 1969, cauza N. 100 (1968(Shi)).). CEPD reamintește că, în temeiul jurisprudenței CJUE[63], doar o instanță judecătorească, și nu procurorii unei instanțe judecătorești, pot autoriza colectarea de date de trafic și localizare, cu precădere.

140. Tot prin prisma jurisprudenței CJUE, potrivit căreia accesul la date poate face obiectul unui mandat, precum în Tele2, CEPD regretă faptul că nu au fost furnizate informații suplimentare în vederea evaluării modului în care criteriile pentru evaluarea necesității unui mandat - gravitatea infracțiunii și modalitatea de comitere a acesteia; valoarea și importanța materialelor confiscate ca probe; probabilitatea ca materialele confiscate să fie ascunse sau distruse; măsura dezavantajelor cauzate prin sechetru; alte condiții aferente - și conceptul „cauzei adecvate" care derivă din Constituție sunt aplicate în practică. Așadar, CEPD invită Comisia să monitorizeze dacă emiterea de mandate îndeplinește criteriile stabilite de CJUE în practică.

4.1.1.1.2 Tipuri de infracțiuni pentru care pot fi emise mandate

141. Aplicarea procedurii mandatului este limitată doar cazurilor în care este efectuată o „anchetă obligatorie". În principiu, aceste mandate pot fi emise doar în cazurile în care s-a produs o încălcare a legii. În această privință, CEPD notează adoptarea recentă a „Legii privind pedepsirea crimei organizate și controlul procedurilor penale" din 15 iunie 2017 în contextul aderării Japoniei la Convenția Națiunilor Unite împotriva Criminalității transfrontaliere (UNTOC)[64]. În absența unei versiuni disponibile în limba engleză a acestei legislații, și având în vedere cerința legislației UE ca unele date să fie colectate exclusiv în contextul cercetării, detectării sau urmăririi unor infracțiuni grave[65], și având în vedere îngrijorarea exprimată de mai mulți comentatori, inclusiv raportorul special al ONU Joseph Cannataci[66], în ceea ce privește domeniul mare de aplicare, și care se bazează pe o definiție a „grupului criminal organizat" raportată ca fiind prea vagă și prea generală, CEPD nu este în măsură să concluzioneze dacă accesul la probele electronice conform legislației japoneze relevante este limitat la pragurile prevăzute de legislația UE.

142. Trebuie remarcat, de asemenea, faptul că pentru anumite tipuri de infracțiuni, Poliția Prefecturii deține competență și că aceștia au propriile lor ordonanțe specifice poliției. Regulile interne aplicabile Poliției prefecturii nu au fost puse la dispoziția CEPD.

143. Potrivit proiectului de decizie privind nivelul adecvat, colectarea de informații în format electronic în domeniul aplicării legii penale cade sub incidența responsabilităților Poliției prefecturii.

4.1.1.2 Mandate pentru ascultarea liniilor telefonice

144. Anexa II la proiectul de decizie privind nivelul adecvat indică faptul că Legea privind ascultarea liniilor telefonice în scopul cercetărilor penale prevede condițiile specifice pentru interceptarea comunicațiilor. Această legislație a fost furnizată foarte târziu fapt ce nu a permis o interpretare în profunzime. Prin urmare, chiar dacă acest cadru juridic pare să

[63] Vezi cauzele 203/15 și C 293/12 și C 594/12 ale CJUE.
[64] Vezi: https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html.
[65] Vezi cauzele reunite C 293/12 și C 594/12 și cazul C 203/15.
[66] Raportorul special al ONU cu privire la dreptul la viața privată precum și Graham Greenleaf, Cercetător la Facultatea de Drept UNSW.

prevadă multe garanții, CEPD nu este în măsură să evalueze dacă condițiile prevăzute în acest act legislativ sunt sprijinite de garanții echivalente în mod substanțial celor prevăzute în UE atât prin Cartă, astfel cum sunt interpretate de CJUE, și prin CEDO, astfel cum sunt interpretate de Curtea de la Strasbourg.

4.1.1.3 Procedura de „prezentare voluntară a informațiilor" în baza unui formular de investigație

145. Această formă neobligatorie de cooperare permite autorităților publice să solicite operatorilor (cu excepția operatorilor de comunicații) să le furnizeze datele pe care le dețin. Nerespectarea solicitării nu este opozabilă. Rămâne neclar modul în care autoritățile pot utiliza acest tip de procedură, dar aceasta pare să fie limitată celor care anchetează infracțiuni.

4.1.1.3.1 Condiții de emitere a „formularelor de investigație"

146. CEPD recunoaște faptul că Curtea Supremă japoneză, prin referire la Constituție, a încadrat limitările la utilizarea „prezentării voluntare de informații".[67] În baza proiectului de decizie privind nivelul adecvat rezultă că, în mod concret, o „prezentare voluntară de informații" poate fi solicitată de autoritățile competente prin emiterea unui „formular de investigare". Se menționează că trimiterea unui astfel de „formular de investigare" este permisă doar ca parte a unei cercetări penale și, așadar, presupune întotdeauna o suspiciune concretă de infracțiune deja comisă. Astfel de anchete sunt desfășurate, în general, de către Poliția prefecturii, atunci când limitările ce decurg din articolul 2 alineatul (2) al Legii poliției se aplică, ceea ce înseamnă că ar trebuie să aibă relevanță pentru activitățile Poliției. Cu toate acestea, CEPD dorește să obțină clarificări suplimentare în ceea ce privește reprezentările concrete ale criteriilor care permit emiterea unui formular de investigație (cum ar fi jurisprudența care ilustrează aplicarea acestor criterii) și relația dintre procedura de prezentare voluntară de informații și confiscarea datelor în baza unui mandat. Într-adevăr, se pare că chiar și atunci când datele nu pot fi obținute prin intermediul unei proceduri voluntare, acestea pot totuși fi obținute în baza unui mandat, dacă acest lucru este indispensabil pentru autoritățile de investigare[68].

4.1.1.3.2 Jurisprudența disponibilă cu privire la limitările utilizării prezentării voluntare de informații

147. Cazurile citate în proiectul de decizie privind nivelul adecvat[69] în vederea ilustrării limitărilor utilizării procedurilor de prezentare voluntară de informații se referă la cazuri în care acuzatul(a) era fie fotografiat(ă) sau filmat(ă) în spațiul public de către poliție în mod direct, și așadar oferă indicații limitate cu privire la situațiile în care autoritățile competente pot solicita unui operator să divulge date, în special în ceea ce privește criteriile enumerate la anexa II cu privire la „caracterul adecvat al metodelor", ceea ce pare să aibă legătură cu evaluarea caracterului „adecvat" sau rezonabil investigației voluntare, în vederea atingerii scopului anchetei. Același lucru se poate spune despre criteriile generale conform cărora evaluarea legalității anchetelor voluntare poate fi „considerată rezonabilă în conformitate cu convențiile acceptate de societate". Mai mult, Agenția Națională de Poliție, care este autoritatea federală responsabilă pentru tot ceea ce ține de poliția judiciară, a emis instrucțiuni pentru Poliția prefecturii cu privire la „utilizarea corectă în cazul folosirii formularelor de investigare în chestiuni de cercetare". Printre altele, investigatorul principal

[67] Vezi anexa II pagina 8.
[68] Vezi anexa II pagina 7.
[69] Vezi anexa II pagina 8 - două decizii ale Curții Supreme din 24 decembrie 1969 (1965 (A) Nr. 1187) și 15 aprilie 2008 (2007 (A) Nr. 839).

trebuie să primească aprobare internă de la un funcționar superior. CEPD nu deține informații cu privire la faptul că aceste instrucțiuni sunt obligatorii. Cu toate acestea, CEPD declară că utilizarea acestei proceduri trebuie să fie proporțională sau necesară.

4.1.1.3.3 Drepturile și obligațiile operatorilor în contextul prezentării voluntare de informații

148. În plus, acordarea consimțământului de furnizare a datelor depinde de operatori (dar se pare că nu există nicio obligație din partea acestora să obțină consimțământul persoanelor vizate sau să le informeze), atunci când aceste solicitări nu contravin altor obligații legale (cum ar fi obligațiile de confidențialitate). Raportul furnizat de către Comisie pare să indice că după o rată ridicată de cazuri de respectare, operatorii au început să ia în considerare protecția datelor clienților lor și au început, așadar, să răspundă mai rar acestor solicitări.

149. De asemenea, rămâne neclar dacă operatorii sunt stimulați în vreun mod pentru a da curs solicitărilor (de exemplu, dacă obțin vreun avantaj dacă tratează solicitările sau dacă nu mai sunt urmăriți penal etc.). În special, nu este menționat niciun principiu cum ar fi „principiul necontribuirii la propria incriminare”.

150. CEPD dorește să obțină informații suplimentare, dacă există, cifre cu privire la numărul și tipurile de solicitări, precum și în ceea ce privește răspunsurile oferite de operatorii solicitați. În absența unei jurisprudențe și a cifrelor, CEPD invită Comisia să monitorizeze eficacitatea și aplicarea concretă a acestei proceduri în practică.

151. Cu toate acestea, CEPD duce lipsă de jurisprudență și cifre cu privire la această procedură pentru a stabili aceste elemente. În consecință, CEPD nu este în măsură să furnizeze o evaluare privind eficacitatea și aplicarea concretă a acestei proceduri fără elemente suplimentare cu privire la practică.

4.1.1.4 Concluzie asupra procedurile pentru accesarea datelor în scopuri de aplicare a legii

152. În concluzie, CEPD recunoaște faptul că principiul potrivit căruia datele cu caracter personal pot fi accesate în mod obligatoriu de autoritățile competente doar atunci când acest lucru este necesar și proporțional scopului, și în baza unui mandat, corespunde garanțiilor esențiale conferite prin legislația UE și CEDO. Drept urmare a constatărilor de mai sus, CEPD solicită Comisiei să monitorizeze domeniul de aplicare a acestor măsuri, domeniul de aplicare a procedurii prezentării voluntare de informații și aplicarea acestor principii de către Poliția prefecturii și de către Instanțe în jurisprudența relevantă și, de asemenea, monitorizarea cadrului legislativ japonez cu privire la asigurarea garanțiilor esențiale stabilite de către CJUE în baza Cartei și de către CEDO în baza Convenției.

4.1.2 Supravegherea în domeniul dreptului penal

153. Proiectul de decizie privind nivelul de protecție adecvat, precum și anexa II prezintă patru tipuri de supraveghere efectuate asupra poliției, ministerelor și agențiilor publice.

4.1.2.1 Supraveghere judiciară

4.1.2.1.1 În cazurile în care informații în format electronic sunt colectate prin mijloace obligatorii (percheziție și sechetru)

154. Potrivit proiectului de decizie privind nivelul adecvat, în toate cazurile în care informațiile în format electronic sunt colectate prin mijloace obligatorii (percheziția și sechestrul), poliția trebuie să obțină, în prealabil, un mandat judecătoresc. Cu toate acestea, există o excepție la această regulă.[70] Într-adevăr, articolul 220 alineatul (1) din Codul procedurii penale permite

[70] Vezi anexa II.

unui procuror public, asistentului său sau unui funcționar al poliției judiciare, atunci când aceștia arestează un suspect, să recurgă la percheziționarea sau confiscarea de informații în format electronic la locul arestării. În această situație, există posibilitatea ca aceste informații să fie excluse ca probe de către un judecător.

155. CEPD este conștientă de faptul că legislația UE include, la rândul său, excepții asemănătoare. Aceasta remarcă faptul că controlul judiciar nu este întotdeauna exercitat în cazurile în care informațiile în format electronic sunt colectate prin mijloace de constrângere, astfel cum este stipulat în proiectul de decizie privind nivelul adecvat. În acest context, CEPD reamintește jurisprudența CEDO cu privință la practica judiciară în baza verificărilor a posteriori.[71]

4.1.2.1.2 În cazul solicitărilor de prezentare voluntară de informații

156. Potrivit proiectului de decizie privind nivelul adecvat, în cazul cererilor de prezentare voluntară de informații, judecătorii nu exercită niciun control ex ante. Într-un astfel de caz, Poliția prefecturii operează sub supravegherea procurorului public. Proiectul de decizie privind nivelul adecvat menționează articolele 192 alineatul (1) și 246 asupra cooperării reciproce și coordinării procurorilor, Comisiei prefecturii privind siguranța publică și Funcționarilor poliției judiciare și schimbul de informații dintre aceștia. Acesta se mai referă și la articolul 193 alineatul (1) potrivit căruia procurorul public poate oferi instrucțiunile necesare poliției judiciare și stabili standarde pentru o anchetă echitabilă. În cele din urmă, acesta menționează articolul 194 cu privire la acțiunile disciplinare ce pot fi întreprinse împotriva poliției judiciare pentru nerespectarea procurorilor publici de către Comisia prefecturii sau națională pentru siguranța publică.

157. CEPD recunoaște stabilirea măsurilor și supravegherii anterioare efectuată de către Comisia națională și prefecturală pentru siguranța publică.

4.1.2.2 Supravegherea poliției de către Comisiile pentru siguranța publică

158. Potrivit Anexei II la proiectul de decizie privind nivelul adecvat, există două tipuri de comisie care supraveghează poliția. Ambele au drept scop garantarea gestionării democratice și neutralitatea politică a administrației din cadrul poliției.

4.1.2.2.1 Supravegherea exercitată de Comisia națională pentru siguranța publică

159. Anexa II la proiectul de decizie privind nivelul adecvat a menționat supravegherea exercitată de Comisia națională pentru siguranța publică asupra APN. Legea poliției prevede o listă a sarcinilor Comisiei din care rezultă competențele sale de supraveghere (vezi articolul 5).

160. Potrivit articolului 4 din Legea poliției, Comisia națională pentru siguranța publică se înființează sub jurisdicția Primului-ministru și este compusă dintr-un președinte și cinci membri. Articolul 7 stabilește anumite limitări în ceea ce privește numirea membrilor Comisiei. Mandatul membrilor Comisiei este de cinci ani și poate fi reînnoit o singură dată, după cum prevede articolul 8. Mai mult, Dieta pare să dispună de o înaltă competență asupra numirii și revocării membrilor Comisiei, ceea ce asigură caracterul independent al Comisiei naționale pentru siguranță publică.

161. Astfel de prevederi legale cresc neutralitatea politică a Comisiei naționale pentru siguranță publică.

[71] CEDO, Modestou împotriva Greciei Nr. 51693/13.

4.1.2.2.2 Supravegherea exercitată de Comisiile prefecturii pentru siguranță publică

162. Poliția prefecturii constituie obiectul supravegherii exercitate de către Comisiile prefecturii pentru siguranță publică care există în cadrul fiecărei prefecturi. Potrivit articolelor 2 și 36 alineatul (2) din Legea poliției, Comisiile prefecturilor pentru siguranță publică sunt responsabile pentru „protecția drepturilor și libertăților persoanelor fizice". Articolul 38, precum și articolul 42 din Legea poliției enumeră îndatoririle Comisiilor prefecturilor pentru siguranță publică. Scopul acestor Comisii este, de asemenea, garantarea gestionării democratice și neutralitatea politică a administrației din cadrul poliției după cum se menționează în articolul 43 alineatul (2) prin emiterea către Poliția prefecturii a unor cazuri individuale atunci când acestea consideră acest lucru necesar în contextul unei verificări a activităților Poliției prefecturii sau abateri ale personalului acesteia din urmă.

163. Cu toate acestea, este neclar dacă aceste Comisii au și alte competențe decât cele de a verifica conduita poliției. CEPD se întreabă dacă termenul de „abatere disciplinară" include accesul ilegal la date și, într-un astfel de caz, dacă aceste Comisii au competența de a dispune sau nu ștergerea datelor.

164. În ceea ce privește neutralitatea și independența acestor Comisii, după cum se menționează în proiectul de decizie privind nivelul adecvat[72], Comisiile prefecturilor pentru siguranță publică se înființează sub jurisdicția guvernatorului prefecturii, care trebuie să numească membrii Comisiei cu acordul adunării prefecturii. Membrii Comisiei prefecturii pentru siguranță publică au un mandat de trei ani și pot fi realeși de cel mult două ori. Articolul 39 din Legea poliției prevede limitări în ceea ce privește numirea membrilor. Proiectul de decizie privind nivelul adecvat menționează, de asemenea, supravegherea Poliției prefecturii de către adunarea locală prin trimitere la articolul 100 din Legea privind autonomia locală. Cu toate acestea, această lege nu a fost prezentată CEPD.[73]

165. Mai mult, potrivit articolului 42 alineatul (2) și alineatul (3) din Legea poliției, „niciun membru al Comisiei nu va deveni concomitent membru al adunării sau al personalului ca angajat ce prestează o activitate cu normă întreagă pentru entități publice locale sau o activitate cu normă redusă conform prevederii din paragraful 1, articolul 28 alineatul (5) din Legea serviciului public local.

166. Potrivit elementelor mai sus menționate și având în vedere colaborarea dintre Comisiile prefecturilor pentru siguranță publică și Comisia națională pentru siguranță publică, CEPD este de acord cu proiectul de decizie privind nivelul de protecție adecvat și salută neutralitatea și independența membrilor Comisiilor prefecturilor pentru siguranță publică. CEPD înțelege că Comisiile prefecturilor pentru siguranță dețin doar competența de a investiga conduita poliției și nu dețin alte competențe supraveghetorii, inclusiv ștergerea datelor colectate de către poliția prefecturii. Așadar, se pare că sunt necesare clarificări suplimentare cu privire la probabilitatea ca supravegherea exercitată de comisiile prefecturilor pentru siguranță publică să fie suficientă potrivit standardelor prevăzute în legislația UE.

4.1.2.2.3 Supravegherea exercitată de Dietă

167. Proiectul de decizie privind nivelul de protecție adecvat [74] și anexa II[75] furnizează anumite informații cu privire la supravegherea exercitată de Dietă în ceea ce privește guvernul,

[72] Vezi proiectul de decizie privind nivelul de protecție adecvat p. 31.
[73] Vezi proiectul de decizie privind nivelul de protecție adecvat p. 33.
[74] Vezi proiectul de decizie privind nivelul de protecție adecvat p. 30.

inclusiv referitor la legalitatea colectării de informații și de date de către poliție. Într-adevăr, ambele menționează articolul 62 din Constituție potrivit căruia Dieta poate solicita prezentarea de documente și depoziția martorilor. De asemenea, ambele menționează prevederile juridice din Legea Dietei, în special articolul 104 cu privire la competențele Dietei, precum și articolul 74 cu privire la depunerea cererilor de informații formulate în scris, cărora Cabinetul trebuie să le răspundă în scris în termen de șapte zile așa cum este prevăzut la articolul 75. Proiectul de decizie privind nivelul de protecție adecvat mai adaugă și faptul că „Rolul Dietei în supravegherea executivului este întărit de obligațiile de raportare, de exemplu în temeiul articolului 29 din Legea privind ascultarea liniilor telefonice".

168. CEPD recunoaște implicarea Dietei în supravegherea guvernului și a poliției în ceea ce privește legalitatea colectării de date.

4.1.2.2.4 Supravegherea exercitată de către executiv

169. Potrivit Anexei II la proiectul privind nivelul adecvat, pe de o parte, Ministrul sau Responsabilul fiecărui minister sau agenție dispune de autoritatea de supraveghere și punere în aplicare în temeiul Legii privind protecția informațiilor personale deținute de către organele administrative (APPIHAO)[76]. Pe de altă parte, Ministrul Afacerilor Interne și Comunicărilor (MIC) are competența de investigare cu privire la aplicarea APPIHAO de către toate celelalte ministere, inclusiv Ministerul de Justiție pentru Poliție așa cum se menționează în proiectul de decizie privind nivelul de protecție adecvat[77].

170. Ministerul poate solicita responsabilului unui organ administrativ să prezinte materiale și explicații referitoare la gestionarea informațiilor cu caracter personal de către organul administrativ vizat în temeiul articolului 50 din APPIHAO. Acesta poate solicita o revizuire a măsurilor când se suspectează survenirea unei încălcări sau utilizări inadecvate a Legii, precum și emiterea de avize referitoare la gestionarea informațiilor cu caracter personal de către organul administrativ vizat potrivit articolelor 50 și 51 din APPIHAO.

171. Proiectul de decizie privind nivelul de protecție adecvat și anexa II menționează, de asemenea, înființarea a 51 de centre de informare cu caracter cuprinzător care „asigură buna implementare a acestei Legi" potrivit articolului 47 din APPIHAO. CEPD remarcă faptul că APPIHAO nu explicitează mai mult rolul și competențele acelor centre de informare, dar că proiectul de decizie privind nivelul de protecție adecvat oferă anumite precizări.

172. Așadar, CEPD salută faptul că există o supraveghere la nivel executiv de către MIC a ministerelor și organelor administrative în ceea ce privește APPIHAO.

173. În concluzie, legislația UE și CEDO, în cadrul jurisprudenței Instanțelor aferente fiecăreia, stabilesc standarde și garanții potrivit cărora supravegherea trebuie să fie completă, neutră și independentă. CEPD remarcă faptul că CPP nu dispune de competențe de supraveghere în chestiuni legate de aplicarea legii. Mai mult, dacă supravegherea exercitată de către Dietă, Comisia națională și prefecturală pentru siguranță publică pare să fie neutră și independentă, sunt necesare mai multe clarificări cu privire la competențele de supraveghere ale Comisiilor prefecturilor pentru siguranță publică.

---

[75] Vezi anexa II pagina 12.
[76] Vezi anexa II pagina 10.
[77] Vezi anexa II pagina 11.

4.1.3 Supravegherea în domeniul dreptului penal

174. Proiectul de decizie privind nivelul de protecție adecvat, completat de anexa II, prezintă mai multe căi prin care persoanele își pot depune reclamațiile, atât la autoritățile independente, cât și la judecători.

175. În continuare, sunt prezentate căile și elementele esențiale ale procedurilor ce derivă din documentația disponibilă, după o scurtă trecere în revistă a drepturilor disponibile pentru a clarifica la ce se pot aștepta persoanele vizate de la autoritățile publice în contextul prelucrării datelor în domeniul procedurilor penale.

4.1.3.1 Drepturi disponibile pentru persoanele vizate în contextul procedurilor penale

176. Pentru a obține reparații, persoanele vizate trebuie să aibă drepturi în virtutea legii pentru a putea pretinde că acestea nu au fost respectate. Așadar, CEPD a evaluat și drepturile disponibile în contextul procedurilor penale prezentate în proiectul de decizie privind nivelul de protecție adecvat.

4.1.3.1.1 Limitări generale ale drepturilor persoanelor vizate în temeiul APPIHAO

177. În proiectul său de decizie privind nivelul de protecție adecvat, COM face referire la și se bazează pe principiile generale privind protecția datelor pe care autoritățile publice trebuie să le respecte după colectarea de date cu caracter personal. Aceste principii sunt, de asemenea, prezentate mai amplu în anexa II, astfel încât CEPD a decis să formuleze observații și asupra acestora.

178. În ceea ce privește drepturile disponibile, CEPD remarcă faptul că, potrivit anexei II la proiectul de decizie privind nivelul de protecție adecvat, unele dintre drepturile cu caracter general oferite persoanelor vizate în contextul prelucrării datelor de organele administrative rămân disponibile și în contextul cercetărilor penale. Cu toate acesta, limitările suplimentare cu privire la colectarea și gestionarea ulterioară a informațiilor cu caracter personal în acest context decurg și din APPIHAO ca atare.

179. Aceste limitări, care par să se aplice atât în contextul datelor colectate în baza unui mandat, cât și în baza unui formular de investigare în contextul prezentării voluntare de informații, ridică semne de întrebare cu privire la mai multe aspecte.

180. În ceea ce privește principiul limitării legate de scop, chiar dacă, în principiu, se solicită organelor administrative să specifice scopul pentru care păstrează date cu caracter personal fără a avea dreptul de a le păstra în afara scopului necesar în vederea atingerii obiectivului de utilizare specificat, acestea pot modifica scopul dacă datele reprezintă „ceea ce poate fi considerat în mod rezonabil ca fiind relevant pentru scopul original”.

181. APPIHAO prevede și principiul neprezentării de informații, potrivit căruia un angajat nu va dezvălui informațiile cu caracter personal dobândite unei alte persoane fără un motiv justificat sau nu va utiliza astfel de informații într-un scop ilicit. Cu toate acestea, nu au fost furnizate informații suplimentare cu privire la interpretarea a ceea ce „motiv justificat” sau „scop ilicit” pot însemna și, așadar, mai multe clarificări sunt necesare în vederea evaluării.

182. Articolul 8 alineatul (1) din APPIHAO prevede, de asemenea, interzicerea utilizării sau prezentării de date „cu excepția cazurilor prevăzute de legislație și reglementări”. Cu toate acestea, chiar dacă această prevedere nu contravine, în principiu, nivelului de protecție conferit în temeiul legislației UE, CEPD îi lipsesc elemente suplimentare cu privire la măsura în care orice supraveghere sau verificare este exercitată atunci când prezentarea de date

este obligatorie în temeiul legislației sau reglementărilor. În plus, în temeiul articolului 8 alineatul (2), excepțiile suplimentare se aplică acestei reguli atunci când „astfel de cazuri excepționale de prezentare de date nu sunt susceptibile de a prejudicia pe nedrept drepturile și interesele persoanei vizate sau unui terț". Fără elemente suplimentare referitoare la acest aspect, excepția de față, care se bazează pe noțiunea neclară a prejudiciului „nedrept", necesită clarificări suplimentare cu privire la faptul dacă este suficient de restrictivă.

183. În sfârșit, articolul 9 din APPIHAO prevede restricții suplimentare asupra scopului sau metodei de utilizare sau oricăror alte restricții impuse de șeful unui organism reprezentativ, atunci când informațiile cu caracter personal păstrate sunt furnizate unei alte persoane. Deoarece noțiunile de „orice alte restricții necesare" și „furnizate unei alte persoane" sunt foarte largi, aceste restricții suplimentare cu privire la drepturile persoanelor vizate constituie motive de îngrijorare în lipsa unor clarificări suplimentare cu privire la domeniul de aplicare al acestei prevederi.

184. Cu toate că CEPD este pe deplin conștient că drepturile de acces și alte principii privind protecția datelor sunt limitate și în procedurile penale din legislația UE, garanții suplimentare sunt asigurate când astfel de limitări sunt prevăzute, inclusiv în ceea ce privește supervizarea, supravegherea și căile de atac. În lipsa unei jurisprudențe suficiente asupra acestor limitări sau elemente suplimentare în vederea clarificării domeniului de aplicare a acestor prevederi, CEPD nu este în măsură să evalueze dacă limitările drepturilor persoanelor vizate sunt restrânse la ceea ce s-ar considera strict necesar și proporțional în temeiul legislației UE, și ar fi astfel echivalent, în esență, cu drepturile conferite persoanelor vizate UE.

4.1.3.1.2 Limitări suplimentare ale drepturilor din APPIHAO ce decurg din Codul de procedură penală și ordonanțele Poliției prefecturii

185. CEPD remarcă faptul că, chiar dacă APPIHAO pare să se aplice tuturor prelucrărilor efectuate de organele administrative din Japonia, anumite limitări importante ale drepturilor persoanelor vizate derivă din legi specifice. În special, articolul 53 alineatul (2) din Codul de procedură penală[78] stipulează că „informațiile cu caracter personal înregistrate în documente referitoare la procese și articole confiscate" sunt excluse din domeniul de aplicare al drepturilor persoanelor fizice prevăzute la capitolul IV din APPIHAO. În mod concret, CEPD înțelege că, în contextul procedurilor penale, persoanele vizate nu beneficiază de drepturile la informare, acces, rectificare sau ștergere a datelor cu caracter personal înregistrate în documente referitoare la procese sau articole confiscate.

186. În ceea ce privește aceste limitări, CEPD înțelege că acestea se aplică în contextul colectării de date pe bază de mandat, precum și în contextul datelor colectate în baza prezentării voluntare de informații prin intermediul formularelor de investigare (vezi mai jos). Într-adevăr, dat fiind că temeiul juridic al acestor două proceduri de accesare a datelor (prin mandat și prin formularul de investigare) este stipulat în codul de procedură penală, articolul 53-2 din acest cod pare să aibă aplicabilitate ambelor tipuri de colectare. Cu toate acestea, deoarece articolul 53-2 se referă la articolele „confiscate", se poate clarifica dacă limitările la drepturile prevăzute prin această stipulare se aplică și în contextul prezentării voluntare de informații.

[78] Disponibil aici http://www.japaneselawtranslation.go.jp/law/detail/?printID=&id=2283&re=02&vm=02 și citat în anexa II la proiectul de decizie privind nivelul de protecție adecvat, nota de subsol 25.

187. CEPD regretă că nu i-au fost prezentate ordonanțele Poliției prefecturii, despre care se spune că protejează informațiile cu caracter personal, drepturile și obligațiile într-un mod echivalent APPIHAO. Date fiind neclaritățile cu privire la interpretarea APPIHAO și lipsa de disponibilitate a ordonanțelor Poliției prefecturii, CEPD se întreabă dacă drepturile conferite persoanelor fizice în acest context și supravegherea suplimentară și/sau mecanismele de recurs sunt suficiente pentru a compensa lipsa drepturilor.

4.1.3.2 Calea de atac prin recurs la autorități independente

4.1.3.2.1 Recursul administrativ

188. CEPD remarcă că organele administrative care colectează datele, cum ar fi Poliția prefecturii, au competența de a soluționa solicitările persoanelor fizice în ceea ce privește drepturile - limitate - ale acestora cu privire la datele colectate în cadrul cercetărilor penale (vezi mai sus cu privire la drepturile disponibile), care par să includă atât colectarea de date în baza unui mandat, cât și formularele de investigare. În mod concret, aceste drepturi par să fie limitate la principii cu caracter general, cum ar fi necesitatea reținerii datelor, în legătură cu scopul (vezi articolul 3.1 APPIHAO), principiul limitării scopului (articolul 4) sau exactitatea datelor (articolul 5), în timp ce drepturile persoanelor fizice cum ar fi dreptul la informare, acces, rectificare sau ștergere sunt excluse pentru datele cu caracter personal înregistrate în documentele referitoare la procese sau articole confiscate[79]. Cu toate că aceste organe nu pot fi considerate ca fiind independente și așadar ca oferind căi de atac și de supraveghere independente, CEPD apreciază această posibilitate. Totuși, acesta subliniază că reclamațiile depuse în acest context rămân limitate la foarte puține drepturi ale persoanelor vizate având în vedere limitările drepturilor prevăzute în APPIHAO.

189. Mai mult, dat fiind că „informațiile cu caracter personal înregistrate în documente referitoare la procese și articole confiscate" sunt excluse din domeniul de aplicare a drepturilor persoanelor fizice prevăzute la capitolul IV din APPIHAO în temeiul articolelor 53-2 din Codul de procedură penală, posibilitățile de solicitare a accesului la informațiile cu caracter personal sunt și ele limitate la procedurile prevăzute prin celelalte prevederi ale acestui Cod de procedură penală. Se pare că doar victimele, persoanele suspectate sau acuzate pot acționa în acest context, acest lucru fiind posibil în funcție de etapa din cadrul procedurii penale. Așadar, CEPD este îngrijorat de faptul că niciun drept cu caracter general de accesare și/sau rectificare sau ștergere a informațiilor nu este disponibil persoanelor vizate în temeiul legislației japoneze în contextul procedurii penale, iar toate căile de atac disponibile implică fie statutul de victimă (în acest caz, persoana ar ști probabil că datele sale au fost colectate) sau persoană suspectată sau acuzată, fie demonstrarea unui prejudiciu, în timp ce persoanele vizate trebuie, la rândul lor, să beneficieze de drept de acces la datele lor și posibilitatea de rectificare sau ștergere a datelor atunci când nu au suferit niciun prejudiciu (probabil) și/sau când nu au nici statut de victimă, persoană suspectată sau acuzată, ci sunt martori, de exemplu.

4.1.3.2.2 Recursul administrativ prin comisiile prefecturilor pentru siguranță publică

190. În plus, comisiile prefecturilor pentru siguranță publică par să fie competente în soluționarea plângerilor. În temeiul articolului 79 din Legea poliției la care se face referire în proiectul de decizie privind nivelul de protecție adecvat, persoanele fizice pot depune o plângere

[79] Vezi mai sus în ceea ce privește limitările aduse APPIHAO și, în special, vezi articolul 53-2 din Codul de procedură penală (acesta nu este prezentat ci doar citat în anexa II la proiectul de decizie privind nivelul de protecție adecvat, nota de subsol 25).

împotriva unui comportament ilegal sau incorect al unui agent în exercitarea îndatoririlor acestuia.

191. CEPD dorește să se clarifice dacă orice prelucrare „ilegală” a datelor cu caracter personal se încadrează în „conduită ilegală sau incorectă a unui agent” și solicită clarificări privind demonstrarea dezavantajului care se pare că este solicitată persoanei vizate. Într-adevăr, notificarea emisă de ANP către Poliție și Comisiile prefecturilor pentru siguranță publică asupra gestionării corecte a plângerilor în ceea ce privește executarea îndatoririlor de ofițerii de poliție limitează plângerile la reclamații concrete referitoare la „corectarea unui dezavantaj specific care a fost cauzat de o conduită ilegală sau incorectă, neinițierea acțiunii necesare, de un ofițer de poliție în executarea îndatoririi sale” și posibilitatea de a „depune o plângere/reclamație de nemulțumire cu privire la modul incorect de executare a îndatoririlor de un ofițer de poliție”. Se clarifică în mod expres că „plângerile cu privire la nerespectarea de către un ofițer de poliție a oricărei chestiuni care nu este considerată ca intrând sub incidența îndatoririlor ofițerului de poliție, precum și cele exprimând o opinie generală sau o propunere, care nu afectează partea reclamantă în mod direct, vor fi excluse.”

192. În ceea ce privește cerințele de procedură în vederea depunerii unei plângeri, cu toate că acestea trebuie depuse în scris, CEPD ia notă că, în acest context, în temeiul legislației japoneze, se asigură asistență pentru redactarea plângerii, inclusiv străinilor. În plus, guvernul japonez pare să fi încredințat CPP și sarcina de a asigura asistență persoanelor vizate din UE în vederea gestionării și soluționării plângerilor din acest domeniu, inițiativă apreciată de CEPD. CEPD subliniază faptul că, în interpretarea sa, în acest context, CPP va acționa doar în calitate de punct de contact între persoanele vizate din UE și autoritățile competente din Japonia.

193. Rezultatele Comisie prefecturii pentru siguranță publică în urma unei plângeri nu vor fi notificate în cazurile enumerate la articolul 79-2 din Legea poliției, care include cazul în care „rezidentul plângerii este necunoscut”. CEPD recunoaște faptul că trimiterea la rezident nu înseamnă că, în toate cazurile, persoanele vizate din UE vor fi, așadar, excluse de la notificarea rezultatelor plângerilor lor pe motiv că nu sunt rezidente în Japonia.

4.1.3.2.3 Mecanism ad hoc implicând CPP

194. Având în vedere constatările descrise mai sus, CEPD apreciază faptul că guvernul japonez și Comisia UE au convenit asupra unui mecanism suplimentar de recurs care le oferă persoanelor fizice din UE o cale suplimentară de atac în Japonia, prin intermediul căreia persoanele fizice pot beneficia de căi de atac împotriva investigațiilor ilegale sau incorecte ale autorităților publice. CEPD mai remarcă, de asemenea, și salută faptul că plângerile pot fi depuse prin intermediul CPP mai degrabă decât printr-un alt funcționar al guvernului, extinzând așadar domeniul de aplicare al competenței CPP la cel al aplicării legii și securității naționale.

195. Principala preocupare a CEPD, în analizarea noului mecanism, a fost înțelegerea competențelor CPP în acest context.

196. Chiar dacă limbajul nu este pe deplin clar, CEPD înțelege că mecanismul suplimentar de recurs nu necesită „prezentarea” în sensul că solicitantul nu trebuie să demonstreze că este posibil ca datele sale cu caracter personal să fi constituit obiectul supravegherii de o autoritate japoneză. CEPD dorește, totuși, să obțină confirmarea Comisiei.

197. În conformitate cu evaluarea sa asupra mecanismului Omdusmanului, creat în temeiul Scutului de Confidențialitate, CEPD subliniază nevoia de competențe efective ale destinatarului solicitării, în acest caz CPP, pentru a considera mecanismul de recurs ca fiind echivalent, în esență, cu o cale efectivă de atac în sensul articolului 47 din Carta Drepturilor Fundamentale.

198. În explicarea mecanismului de recurs, guvernul japonez face referire la articolele 6, 61 punctul (ii) și 80 din APPI și prezintă aceste competențe în anexa II. Conform interpretării CEPD, procedura, astfel cum este descrisă în anexa II, specifică sau extinde competențele CPP, deoarece formularea articolelor 6, 61 punctul (ii) și 80 din APPI este mai degrabă vagă și generală. În măsura în care anexa II specifică sau extinde competențele CPP, CEPD dorește să obțină clarificări privind obligativitatea celorlalte agenții ale guvernului japonez de a le respecta.

199. În baza procedurii din anexa II, CEPD constată că autorităților publice competente din Japonia li se cere să coopereze cu CPP, „inclusiv prin furnizarea de informații necesare și materiale relevante, astfel încât CPP să poată evalua dacă colectarea sau utilizarea ulterioară a informațiilor cu caracter personal s-a efectuat cu respectarea regulilor aplicabile". În vederea evaluării eficacității sistemului, este important să se facă din nou referire la competențele pe care le dețin autoritățile competente cu care cooperează CPP. În accepțiunea CEPD, acele competențe nu ar fi extinse prin reasigurările prevăzute în anexa II.

200. CEPD mai remarcă faptul că, dacă este identificată o încălcare, „cooperarea autorităților publice în cauză cu CPP include obligația de remediere a încălcării", care include în mod expres ștergerea datelor colectate prin încălcarea normelor aplicabile. CEPD înțelege că obligațiile autorității competente derivă din „cooperarea cu CPP" mai degrabă decât dintr-o decizie a CPP.

201. În cele din urmă, CPP va informa solicitantul cu privire la „rezultatele evaluării, inclusiv orice acțiune corectivă inițiată acolo unde este cazul". În plus, CPP va informa solicitantul cu privire la „posibilitatea de a solicita o confirmare a rezultatelor de la autoritatea publică competentă și despre autoritatea către care va fi înaintată o astfel de cerere de confirmare".

202. În plus, CPP s-a angajat să acorde asistență solicitantului în a acționa în continuare în temeiul legislației japoneze, dacă solicitantul este nemulțumit de rezultatele procedurii.

203. Prin prisma necesității de a avea un mecanism de recurs eficient și echivalent, în esență, cu standardele UE, CEPD se întreabă, totuși, dacă CPP deține vreo competență specifică în afară de cea de a evalua dacă colectarea sau utilizarea ulterioară a informațiilor cu caracter personal s-a derulat în conformitate cu normele aplicabile și de a face apel la autoritățile competente pentru a face uz de competențele lor și de a soluționa plângerile înaintate de CPP. În cazul în care CPP acționează doar ca punct de contact pentru persoanele fizice din UE, CEPD ar considera aceasta drept insuficient în vederea asigurării unui mecanism de recurs eficient și echivalent, în esență, celui din standardele UE. Așadar, CEPD face apel la Comisie pentru a furniza clarificări asupra aspectelor menționate în acest subcapitol, în special dacă și în ce mod mecanismul extinde obligațiile autorităților competente, modul în care sunt obligate să îl respecte, și modul în care CPP poate asigura în mod eficient respectarea și nu doar acționarea în calitate de punct de contact pentru persoanele fizice din UE.

4.1.3.3 Căi de atac judiciare

4.1.3.3.1 Mecanism de cvasi-plângere

204. Așa numita procedură de „cvasi-plângere” permite acționarea împotriva colectării obligatorii de informații în baza unui mandat în vederea abrogării sau modificării sechestrului.

205. Această cale implică faptul ca persoana fizică să fie conștientă că datele sale sunt confiscate. Cu toate acestea, CEPD înțelege că procedura pentru colectarea datelor în baza unui mandat nu este notificată persoanei vizate. De asemenea, înțelege că prezentarea voluntară de informații nu implică obligația companiilor de a aduce la cunoștința persoanelor vizate solicitările primite și cărora li s-au conformat. Așadar, cu toate că în anexa II se subliniază că „o astfel de provocare poate fi inițiată fără ca persoana să trebuiască să aștepte încheierea cazului”, în practică, exceptând mandatele care autorizează ascultarea liniilor telefonice, pentru care se stipulează că legea prevede cerința de notificare[80], această cale pare să fie disponibilă, efectiv, doar odată ce persoana vizată devine conștientă de colectarea datelor printr-o acțiune deschisă împotriva sa.

4.1.3.3.2 Măsuri reparatorii

206. În plus, în vederea obținerii ștergerii datelor colectate printr-o procedură penală (așa-numita „măsură reparatorie”), sau obținerii de compensări pentru daune, persoanele fizice pot intenta acțiuni civile în justiție.

207. În ceea ce privește compensarea, CEPD remarcă că procedura pare să se limiteze la situațiile în care un funcționar public a provocat daune persoanei fizice în cauză în cursul îndeplinirii îndatoririlor sale, în mod ilegal și din culpă (în mod intenționat sau prin neglijență). În accepțiunea CEPD, dauna pare să includă daunele morale. Nu este, totuși, prevăzut în detaliu ceea ce trebuie să demonstreze persoana fizică care a suferit un prejudiciu. CEPD nu este în măsură să evalueze jurisprudența referitoare la acordarea de despăgubiri, și nu poate, așadar, evalua dacă această acțiune reprezintă o cale de atac eficientă în caz de prejudicii.

208. În ceea ce privește „măsurile reparatorii”, CEPD remarcă, de asemenea, că pentru a depune o solicitare, persoana fizică trebuie să fie mai întâi conștientă că datele sale au fost colectate și că acestea fac încă obiectul păstrării. Așadar, luând în considerare drepturile limitate de informare și de acces al persoanelor fizice în contextul cercetării și procedurilor penale, eficiența procedurii pare să fie, la rândul său, destul de limitată.

4.1.3.4 Evaluarea globală a căilor de atac

209. În urma evaluării tuturor căilor de atac disponibile persoanelor fizice în temeiul legislației japoneze, precum și persoanelor vizate din UE pe lângă CPP, CEPD apreciază mecanismul de soluționare ad hoc a litigiilor care implică CPP. Acesta are o valoare adăugată pentru persoanele vizate din UE, în special deoarece le permite să înțeleagă căile care le sunt disponibile pentru a obține reparații și/sau compensări, precum și pentru a-și prezenta solicitările în conformitate cu cerințele de procedură aplicabile în temeiul legislației japoneze. Cu toate acestea, sunt necesare clarificări suplimentare, în special cu privire la posibilitatea ca mecanismul să extindă obligațiile autorităților competente și modul de realizare a acestuia, modul în care autoritățile competente sunt obligate să-l respecte, precum și modul în care CPP poate asigura în mod eficient conformitatea, pentru a garanta că acest nou mecanism asigură o cale de atac eficientă.

[80] Articolul 23 din Legea ascultării liniilor telefonice este menționat la pagina 33 din proiectul de decizie privind nivelul de protecție adecvat. Cu toate acestea, CEPD nu i-a fost prezentat acest text și nu poate, așadar, să evalueze în ce măsură se aplică această obligație de notificare și în ce cazuri ar putea fi limitată.

210. Această evaluare arată că niciun mecanism de recurs din legislația japoneză nu pare să permită accesul, rectificarea sau ștergerea datelor persoanelor vizate care nu au statut de victimă, persoană suspectată sau acuzată în contextul unei proceduri penale, de exemplu remedierea colectării sau păstrării ilegale a datelor acestora. Aceasta arată, de asemenea, că toate mecanismele de recurs și compensare disponibile în temeiul legislației japoneze pentru victime, persoane suspectate sau acuzate implică cunoașterea faptului că datele sunt colectate, lucru care pare restricționat în practică deoarece acestea beneficiază de drepturi limitate de acces și informare. În plus, mai multe clarificări par să fie necesare privind demonstrarea conduitei ilegale a autorităților, în special când o astfel de conduită include prelucrarea ilegală a datelor cu caracter personal sau un prejudiciu suferit de persoana fizică.

211. Așadar, în lipsa unei documentații și a elementelor suplimentare, CEPD este îngrijorat dacă aceste căi de atac prevăzute prin legislația japoneză și proiectul de decizie privind nivelul de protecție adecvat sunt suficient de eficiente comparativ cu standardele din legislația UE.

4.2 Accesul în scopuri de securitate națională

4.2.1 Domeniul de aplicare a supravegherii

212. În cadrul proiectului de decizie privind nivelul de protecție adecvat, capitolul privind „accesul și utilizarea de autoritățile publice japoneze în scopuri de securitate națională” este introdus printr-o declarație cu caracter general, în conformitate cu noua asigurare oferită de guvernul japonez în anexa II, potrivit căreia legislația japoneză nu prevede și nu permite așadar „solicitări obligatorii de informații sau ascultarea liniilor telefonice în scop administrativ, în afara cercetărilor penale”. În concluzie, se specifică faptul că „pot fi obținute informații pe baza unor motive de securitate națională doar dintr-o sursă de informare care poate fi accesată gratuit de oricine sau prin prezentare voluntară de informații. Aceasta exclude orice activități de supraveghere sub acoperire în acest domeniu. Operatorii economici care primesc o solicitare de cooperare voluntară (sub forma prezentării de informații în format electronic) nu au obligația legală de a furniza astfel de informații.”[81]

213. În contextul acestor limitări, sunt enumerate patru entități guvernamentale care au competența de a colecta informații în format electronic deținute de operatorii economici japonezi pe considerente de securitate națională. În ceea privește Ministerul Apărării, care este una dintre cele patru entități, se specifică că acesta „are doar autoritatea de a colecta informații (în format electronic) în baza prezentării voluntare de informații”.[82]

214. În vederea evaluării cadrului general de colectare de date în scopuri de securitate națională, CEPD dorește să reamintească prima dintre cele patru așa-numite „garanții esențiale”, potrivit cărora „prelucrarea ar trebui să se bazeze pe reguli clare, precise și accesibile”[83]. Mai precis, CEDP a fost foarte clară asupra faptului că programele de supraveghere sunt „în conformitate cu legea” numai dacă măsurile de supraveghere „se bazează pe prevederi din dreptul intern”. Curtea a clarificat că compatibilitatea cu statul de drept cere ca legea care autorizează această măsură trebuie să fie accesibilă și previzibilă în ceea ce privește efectele sale. Referitor la riscul comportamentului arbitrar, curtea a solicitat „reguli clare, detaliate asupra măsurilor de securitate cu caracter secret”; „suficient de clare pentru a furniza

[81] Decizia privind nivelul de protecție adecvat, paragraful 151.
[82] Decizia privind nivelul de protecție adecvat, paragraful 153.
[83] GL29, WP 237: Documentul de lucru 01/2016 asupra justificării interferențelor cu drepturile fundamentale la viața privată și protecția datelor prin măsuri de supraveghere în momentul transferării datelor cu caracter personal (Garanții esențiale europene).

cetățenilor o indicație adecvată în ceea ce privește circumstanțele în care și condițiile care îndreptățesc autoritățile publice să recurgă la o asemenea măsură”.[84]

215. În vederea aplicării acestor garanții esențiale sistemului juridic din Japonia, CEPD este conștient de faptul că, în chestiunile privind securitatea națională, statele au o marjă largă de apreciere, recunoscută de Curtea Europeană a Drepturilor Omului. De asemenea, competențele în materie de securitate națională reflectă experiențele istorice ale națiunilor. Astfel, CEPD înțelege că, după cum subliniază guvernamentul japonez, după cel de-al Doilea Război Mondial, serviciile japoneze naționale de informații au fost înzestrate cu competențe mai limitate decât în alte state.

216. În interpretarea CEPD, proiectul de decizie privind nivelul de protecție adecvat, care este conform noii asigurări oferite de guvernul japonez, sugerează că entitățile guvernamentale japoneze nu derulează programe care monitorizează din punct de vedere strategic sau supervizează în sens larg comunicațiile (prin internet). Așa cum s-a menționat mai sus, guvernul japonez a oferit din nou asigurări, printr-o scrisoare semnată de Ministrul Justiției, că „pot fi obținute informații în baza unor considerente de securitate națională numai dintr-o sursă de informare care poate fi accesată în mod gratuit de oricine sau prin prezentarea voluntară de informații”.

217. În ceea ce privește temeiul legal al Ministerului Apărării, CEPD remarcă faptul că proiectul de decizie privind nivelul de protecție adecvat include informații cu caracter general despre competențele sale și citează misiunea sa „de a desfășura activități ca cele la care se face referință, în vederea asigurării păcii și independenței naționale și a siguranței naționale”. Cu toate acestea, CEPD nu i-a fost prezentată traducerea în limba engleză a temeiului legal.

218. În același timp, CEPD este conștient de rapoartele publicate pe diferite canale media care sugerează că sunt derulate programe de supraveghere de Direcția pentru informații derivate din semnale a Ministerului Apărării din Japonia (MA)[85]. În raport, este susținut și faptul că Ministerul Apărării din Japonia, care deși refuză să discute particularitățile raportului, a „recunoscut că Japonia deține „birouri în toată țara” care interceptează comunicațiile” și că acestea „se axează pe activități militare și „amenințări cibernetice” și că „nu colectează informațiile privind publicul larg”. Ultima declarație (faptul că MA nu colectează informații privind publicul larg) a fost inclusă în reformularea făcută de guvernul japonez.

219. Reiese că guvernul japonez a reafirmat, într-o scrisoare semnată de Ministerul de Justiție, că MA nu colectează informații privind publicul larg.

220. Nu ține de competența CEPD efectuarea unei evaluări generale ale posibilelor capacități de supraveghere ale guvernului japonez. Acele activități sunt importante pentru evaluarea sa doar dacă sunt relevante în ceea ce privește transferul datelor cu caracter personal între UE și Japonia. În acest context, CEPD ar dori să își reafirme abordarea deja adoptată de predecesorul său când i-a fost solicitat avizul cu privire la Scutul de Confidențialitate UE-S.U.A. În formularea avizului său asupra Scutului de Confidențialitate, GL29 a inclus în analiza sa competențele și limitările S.U.A. în supravegherea datelor „în drum” spre S.U.A[86]. Aplicând

[84] Vezi, de exemplu Big Brother Watch și alții/ Regatul Unit, punctul 305.

[85] În mai 2018, publicația de știri online „The Intercept” a publicat un raport cu titlul „Povestea nespusă a agenției de spionaj secret a Japoniei”.

[86] Vezi WP255, Scutul de Confidențialitate UE-S.U.A.- Prima revizuire unificată anuală, adoptată la 28 noiembrie 2017, p. 16: „GL29 este de părere că analiza legislației țării terțe al cărei caracter adecvat este examinat, nu ar trebui limitată la legea și practica care permit supravegherea în cadrul granițelor fizice ale țării, dar ar trebui să

același standard deciziei privind nivelul adecvat referitoare la Japonia, CEPD este de părere că informațiile asupra competențelor autorităților japoneze de a supraveghea datele „în drum” spre Japonia sunt relevante. În cazul în care astfel de competențe de supraveghere ar exista, decizia luată de CEDO în Big Brother Watch pare, de asemenea, să sugereze că astfel de competențe ar trebui să fie reglementate în conformitate cu standardele stabilite de CEDO.

221. În consecință, dacă interceptările au fost limitate la „acordarea de asistență acțiunilor militare”, acestea s-ar putea să nu fie relevante în evaluarea deciziei privind nivelul adecvat. Este, așadar, interesul CEPD să primească clarificări cu privire la măsurile de supraveghere ale entităților guvernamentale japoneze. Din acest punct de vedere, astfel de clarificări sunt binevenite pentru a stabili dacă datele supuse transferului în temeiul cadrului privind nivelul adecvat pot face obiectul accesării în scopuri de securitate națională de autoritățile japoneze cu competențe în acest domeniu.

4.2.2 Prezentarea voluntară de informații în cazul securității naționale

222. Proiectul de decizie privind nivelul de protecție adecvat menționează că cele patru entități guvernamentale au autoritatea de a colecta informații (în format electronic) numai dacă sunt prezentate voluntar. Potrivit proiectului de decizie și Anexei II, există anumite limitări din motive legale, ceea ce înseamnă că colectarea de date este limitată la ceea ce este necesar pentru executarea sarcinilor de către entități.

223. În domeniul legii penale, așa cum se precizează în secțiunea referitoare la aplicarea legii, prezentarea voluntară de informații este permisă doar în cadrul cercetării penale, și presupune, așadar, o suspiciune concretă a unei infracțiuni deja comise. Investigațiile din domeniul securității naționale diferă de cele din domeniul aplicării legii. CEPD recunoaște faptul că, potrivit Anexei II, principiile centrale ale „necesității de efectuare a investigației” și „oportunitatea metodei” se aplică în mod similar și în domeniul securității naționale și trebuie respectate luând în considerare circumstanțele specifice ale fiecărui caz[87]. Acesta regretă faptul că aplicarea nu este clarificată mai mult, inclusiv prin intermediul unei trimiteri la jurisprudență. Cu toate acestea, CEPD declară că, utilizarea acestei proceduri trebuie să fie proporțională sau necesară.

224. Potrivit proiectului de decizie, după colectarea („obținerea”) informațiilor cu caracter personal, gestionarea acestora este asigurată de APPIHAO cu excepția Poliției prefecturii[88]. Anexa II precizează că gestionarea informațiilor cu caracter personal de Poliția prefecturii este reglementată prin ordonanțele prefecturii care stipulează principiile pentru protecția informațiilor cu caracter personal, drepturile și obligațiile echivalente celor din APPIHAO[89]. Deoarece nu există traduceri în limba engleză disponibile pentru aceste ordonanțe, CEPD nu este în măsură să evalueze dacă principiile sunt echivalente celor din APPIHAO.

225. În ceea ce privește celelalte observații referitoare la prezentarea voluntară de informații, se face trimitere la secțiunea asupra aplicării legii.

---

ia în considerare și o analiză a temeiurilor juridice din legislația țării terțe în baza cărora aceasta poate desfășura activități de supraveghere în afara teritoriului său atât timp cât acestea vizează și date UE. Așa cum s-a subliniat în avizul precedent, „ar trebui să fie clar dacă Principiile Scutului de Confidențialitate se vor aplica din momentul în care datele sunt transferate, ceea ce include și datele „în drum” spre țara respectivă.”

[87] Vezi anexa II, pp. 23.

[88] Decizia privind nivelul de protecție adecvat, paragraful 118 și 157.

[89] Vezi anexa II, pp. 3.

4.2.3 Supravegherea

4.2.3.1 Aspecte generale

226. Cele patru entități guvernamentale care au competența de a colecta informații în format electronic deținute de operatorii economici japonezi pe considerente de securitate națională sunt: (i) Biroul de cercetare și informații a Cabinetului (BCIC); (ii) Ministerul Apărării („MA"), (iii) poliția (atât Agenția Națională de Poliție (ANP)[90], cât și Poliția prefecturii); și (iv) Agenția de investigare a securității publice („AISP").

227. Potrivit proiectului de decizie privind nivelul de protecție adecvat, aceste entități guvernamentale fac obiectul mai multor niveluri de supraveghere exercitate de trei ramuri ale guvernului[91]. CEPD notează faptul că există un mecanism de supraveghere în cadrul ramurii legislative (Dieta japoneză) și a ramurii executive (Biroul inspectorului general pentru conformitate juridică (BIG), Comisiile prefecturii pentru siguranță publică și Comisia de examinare a securității publice). CEPD subliniază faptul că COM ar trebui să clarifice supravegherea judiciară (*ex-officio*/garanția C din WP 237; în ceea ce privește recursul, există un capitol separat în decizia privind nivelul adecvat și o garanție suplimentară în WP 237) a organismelor guvernamentale mai sus menționate, deoarece nu este clar dacă există o astfel de supraveghere judiciară în domeniul colectării de informații cu caracter personal în scopuri de securitate națională fără mijloace obligatorii.

4.2.3.2 Supravegherea de Dieta japoneză

228. CEPD remarcă faptul că Dieta japoneză poate conduce investigații cu privire la activitățile autorităților publice și, așadar, și cu privire la toate entitățile guvernamentale mai sus menționate. Mai mult, dieta poate solicita și prezentarea de documente și depoziția martorilor (*articolul 62 din Constituția Japoniei, articolul 104 din Legea dietei*). CEPD mai remarcă și faptul că, potrivit *articolelor 74 și 75 din Legea dietei*, membrii Dietei pot formula întrebări în scris Cabinetului care s-ar putea solda cu un răspuns din partea acestuia (*articolul 75 din Legea dietei*). În cele din urmă, se remarcă faptul că există obligații specifice de raportare, de ex. cele pentru Agenția de investigare a securității publice („AISP") (articolul 36 SAPA (Legea privind prevenirea activităților subversive)/Art 31 ACO (Legea privind controlul organizațiilor care au comis acte de crime de masă nediscriminatorii)), prin intermediul unui raport anual către Dietă. Un astfel de raport nu i-a fost prezentat CEPD.

4.2.3.3 Supravegherea efectuată de Biroul inspectorului general pentru conformitate juridică (BIG)

229. CEPD remarcă faptul că există un organism de supraveghere pentru MA, denumit BIG. CEPD nu i-a fost prezentată Decizia de instituire a MA (Decizia MA privind instituirea), ci doar declarații în cadrul Anexei II la proiectul de decizie. Din anexa II reiese că BIG este un birou independent în cadrul MA, care se află sub supravegherea directă a Ministerului Apărării potrivit articolului 29 din Decizia MA privind instituirea. BIG are competențe de efectuare a verificărilor privind respectarea legilor și reglementărilor de funcționarii MA („așa-numitele „verificări ale apărării") în tot ministerul, inclusiv forțele de autoapărare.

[90] Cu toate acestea, potrivit informațiilor primite, principalul rol al ANP este acela de a coordona investigațiile desfășurate de diferite departamente ale Poliției prefecturii, iar activitățile sale de colectare a informațiilor sunt limitate la schimburi cu autoritățile străine.
[91] Vezi anexa II, pp. 39.

230. Din anexa II reiese că BIG își îndeplinește îndatoririle în mod independent față de departamentele operaționale ale MA. CEPD remarcă faptul că BIG este un organism intern de supraveghere.

231. Verificările conduc la constatări și, în vederea asigurării conformității, măsuri care sunt raportate în mod direct Ministerului Apărării. În baza raportului BIG, Ministerul Apărării poate emite ordine de implementare a măsurilor necesare în vederea remedierii situației. Ministrul adjunct al Apărării este responsabil cu implementarea acestor măsuri și trebuie să raporteze Ministerului Apărării cu privire la stadiul respectivelor implementări.

232. Analizând anexa II, fără să-i fi fost furnizate prevederile juridice (decizia MA de instituire) pentru aceste considerații, CEPD apreciază posibilitatea de a ordona măsurile necesare de conformare în vederea remedierii situației. Cu toate acestea, CEPD are îndoieli cu privire la independența BIG, deoarece este un birou în cadrul MA și se află sub supravegherea directă a Ministrului Apărării după cum reiese din Anexa II (potrivit WP 237 „*independența funcțională nu este suficientă în sine în vederea protejării autorității de supraveghere împotriva influențelor externe*").

233. În conformitate cu jurisprudența CEDO și WP 237, respectiv în baza considerentelor din anexa II, Inspectorul General poate solicita rapoarte de la biroul în cauză (documente, situri, explicații). Clarificările dacă birourile vizate sunt obligate sau nu să dea curs acestor solicitări și dacă documentele solicitate includ materiale închise, așa cum precizează WP 237 sau nu, par necesare CEPD.

234. Cu toate că CEPD apreciază faptul că experți juridici cu o îndelungată experiență (fostul Procuror șef), conduc BIG, clarificarea cu privire la modul în care acest organism de supraveghere este desemnat pare necesară.

4.2.3.4 Supravegherea efectuată de Comisia de examinare a securității publice

235. Potrivit Anexei II (pagina 25), AISP derulează verificări de rutină și speciale ale operațiunilor efectuate de birourile și oficiile sale individuale (Biroul de investigare a securității publice, Oficiile și Suboficiile de investigare a securității publice etc.). În scopuri de verificări de rutină, sunt desemnați ca inspectori un Director General Adjunct și/sau un Director. Aceste verificări ar trebui să vizeze și gestiunea informațiilor cu caracter personal.

236. Conform considerentului 163 din proiectul de decizie, *Comisia de examinare a securității publice* acționează în calitate de organism de supraveghere ex ante independent pentru AISP, în ceea ce privește chestiuni aferente ACO[92] și SAPA[93]. CEPD apreciază acest aspect.

237. Cu toate că site-ul Ministerului de Justiție japonez oferă anumite informații[94], CEPD nu este în măsură să evalueze cu atenție independența Comisiei de examinare a securității publice

[92] Legea privind controlul organizațiilor care au comis acte de crime de masă nediscriminatorii (Legea nr. 147 din 7 decembrie 1999).
[93] Legea prevenirii activităților subversive (Legea nr. 240 din 21 iulie 1952).
[94] Vezi http://www.moj.go.jp/ENGLISH/MEOM/meom-01.html (septembrie 2018): organismul extraministerial „*este compus dintr-un președinte și șase membri. Aceștia sunt selectați din rândul persoanelor de bună credință care pot lua hotărâri corecte cu privire la controlul organizațiilor și al celor care dețin cunoștințe ample și experiență atât în domeniul juridic, cât și cel societal. Aceștia sunt numiți de prim-ministru și trebuie aprobați de ambele camere ale Dietei. În ceea ce privește aplicarea legilor menționate anterior (SAPA/ACO), membrii își îndeplinesc îndatoririle într-un mod relativ independent, liberi de orice îndrumare sau supraveghere a primului-ministru sau a ministrului de justiție.*"

deoarece nu i-a fost furnizată Decizia de instituire a Comisiei de examinare a securității publice[95] și Normele Comisiei de examinare a securității publice[96].

4.2.3.5 Supravegherea efectuată de Comisia națională pentru siguranța publică, Comisiile prefecturilor pentru siguranța publică și APPIHAO (executiv)

238. Vezi 3.1.2.2.1 (Comisia națională pentru siguranță publică), 3.1.2.2.2. (Comisiile prefecturilor pentru siguranță publică) și 3.1.2.2.4. (Executiv).

4.2.3.6 Supravegherea efectuată de CPP

239. CEPD invită COM fie să menționeze la considerentul 164 că CPP nu este un organism de supraveghere pentru entitățile guvernamentale mai sus menționate și că are competență doar în asigurarea mijloacelor de recurs pentru persoanele fizice, fie să mute paragraful din considerentul 164 cu privire la CPP la secțiunea „căi de atac individuale".

4.2.4 Mecanismul de recurs

240. În ceea ce privește analiza mecanismului de recurs negociat recent, se face trimitere la secțiunea asupra aplicării legii.

241. În plus, merită remarcat faptul că legislația japoneză pune la dispoziție o cale de atac individuală specifică în domeniul securității naționale. În accepțiunea CEPD, toate persoanele fizice, inclusiv persoanele fizice din UE, pot solicita în general dezvăluirea, corectarea (inclusiv ștergerea) sau suspendarea utilizării informațiilor de la organismele administrative, chiar dacă acestea sunt prelucrate în scopuri de securitate națională. În cazul în care o astfel de solicitare este „respinsă pe motivul că informația vizată este considerată ca neputând fi dezvăluită", se poate intenta un apel de reexaminare și trebuie consultat „Comitetul pentru revizuirea protecției și dezvăluirii informațiilor cu caracter personal". Comitetul este constituit din membri numiți de prim-ministru cu aprobarea ambelor Camere, înzestrat cu competențe de investigare, și acesta poate concluziona prin emiterea unui raport scris către persoana fizică în cauză care nu are caracter obligatoriu, dar este respectat aproape întotdeauna[97]. Potrivit anexei II, doar în două cazuri din 2000 autoritatea administrativă a luat o decizie diferită de cea din concluzia Comitetului.[98]

242. În baza explicației furnizate, rezultă că procedura de revizuire nu este disponibilă dacă informația poate fi „dezvăluită", dar persoana fizică nu este mulțumită de rezultate. CEPD recunoaște această cale de atac, dar dorește să obțină mai multe clarificări cu privire la ultimul aspect, care i-ar îngrădi în mod semnificativ domeniul de aplicare.

Pentru Comitetul European pentru Protecția Datelor

Președinte

(Andrea Jelinek)

[95] http://www.japaneselawtranslation.go.jp/law/detail_main?re=&vm=2&id=613 (septembrie 2018).
[96] Articolul 28 ACO.
[97] Anexa II, p. 25, 26. Decizia de instituire a Comitetului pentru revizuirea protecției și dezvăluirii informațiilor cu caracter personal, art. 4, 9, 11.
[98] Anexa II, nota de subsol 35.