Avizul 32/2021 referitor la Proiectul de decizie de punere în aplicare a Comisiei Europene în temeiul Regulamentului (UE) 2016/679 privind protecția adecvată a datelor cu caracter personal în Republica Coreea

Versiunea 1.0

Adoptat la 24 septembrie 2021

CUPRINS

Comitetul european pentru protecția datelor

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

având în vedere Acordul privind Spațiul Economic European (**„SEE”**), în special Anexa XI și Protocolul 37, astfel cum au fost modificate prin Decizia nr. 154/2018 a Comitetului mixt al SEE din 6 iulie 2018[1],

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

A ADOPTAT URMĂTORUL AVIZ:

1. REZUMAT

1. Comisia Europeană a lansat procesul formal în vederea adoptării proiectului său de decizie de punere în aplicare (**„proiectul de decizie”**) privind protecția adecvată a datelor cu caracter personal în Republica Coreea, conform Legii privind protecția informațiilor cu caracter personal (LPICP), în temeiul RGPD, la 16 iunie 2021[2].

2. La aceeași dată, Comisia Europeană a solicitat avizul Comitetului european pentru protecția datelor (**„CEPD”**)[3]. Evaluarea efectuată de CEPD privind adecvarea nivelului de protecție asigurat în Republica Coreea a fost realizată în baza examinării proiectului de decizie ca atare, precum și în baza analizării documentației puse la dispoziție[4] de Comisia Europeană.

3. CEPD s-a axat atât pe evaluarea aspectelor generale legate de RGPD din proiectul de decizie, cât și pe accesul autorităților publice la datele cu caracter personal transferate din SEE în scopuri de aplicare a legii și de securitate națională, inclusiv căile de atac pe care le au la dispoziție persoanele fizice din SEE. De asemenea, CEPD a evaluat dacă garanțiile oferite pe baza cadrului juridic coreean sunt puse în aplicare și funcționează.

4. Ca referință principală pentru această activitate, CEPD a folosit Criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD (**„Criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD”**)[5] adoptate în februarie 2018 și Recomandările 02/2020 ale CEPD privind garanțiile esențiale europene pentru măsurile de supraveghere[6].

[1] Referirile la **„Statele Membre”** din prezentul aviz trebuie înțelese ca referiri la „Statele Membre ale SEE”.
[2] Vezi comunicatul de presă https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964.
[3] Ibid.
[4] CEPD și-a bazat analiza pe traducerile oficiale realizate de guvernul coreean.
[5] WP 254, Criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD, 6 februarie 2018 (avizate de CEPD, vezi https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines).
[6] Vezi Recomandările 02/2020 ale CEPD privind garanțiile esențiale europene pentru măsurile de supraveghere, adoptate la 10 noiembrie 2020 https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_en.

1.1. Arii de convergență

5. Principalul obiectiv al CEPD este să furnizeze Comisiei Europene un aviz privind caracterul adecvat al nivelului de protecție acordat persoanelor fizice ale căror date cu caracter personal sunt transferate în Republica Coreea. Este important de recunoscut că CEPD nu se așteaptă la reproducerea legislației europene în domeniul protecției datelor în cadrul legislativ coreean privind protecția datelor.

6. Cu toate acestea, CEPD reamintește că, pentru a se considera că oferă un nivel de protecție adecvat, articolul 45 din RGPD și jurisprudența Curții de Justiție a Uniunii Europene (denumită în continuare **„CJUE"**) impun ca legislația țării terțe să fie aliniată la esența principiilor fundamentale prevăzute în RGPD. În acest context, cadrul legislativ coreean privind protecția datelor prezintă numeroase similitudini cu cadrul european privind protecția datelor, existând un act legislativ principal care acoperă atât sectorul public, cât și pe cel privat, și care este completat cu acte legislative specifice la nivel de sector.

7. În ceea ce privește conținutul, CEPD constată existența unor domenii principale de aliniere între cadrul RGPD și cadrul coreean privind protecția datelor în ceea ce privește anumite dispoziții esențiale, precum, de exemplu, conceptele (de exemplu, „informații cu caracter personal", „prelucrare", „persoană vizată"); temeiurile pentru prelucrarea legală și echitabilă în scopuri legitime; limitări legate de scop, calitatea și proporționalitatea datelor; păstrarea, securitatea și confidențialitatea datelor; transparența și categorii speciale de date.

8. Pe lângă aspectele de mai sus, CEPD salută eforturile depuse de Comisia Europeană și de autoritățile coreene pentru a se asigura că Republica Coreea oferă un nivel adecvat de protecție în conformitate cu cel al RGPD prin adoptarea Notificărilor de către autoritatea coreeană de supraveghere (aplicabile nu numai în cazul datelor cu caracter personal transferate din SEE în Coreea) cu scopul de a acoperi lacunele dintre RGPD și cadrul coreean privind protecția datelor. În acest context, CEPD dorește să evidențieze relevanța acestor Notificări pentru evaluarea adecvării Republicii Coreea constatând, de exemplu, că acestea furnizează clarificări relevante privind unele garanții importante, printre altele în ceea ce privește sfera de aplicare a excepțiilor de la LPICP, pentru prelucrarea informațiilor cu caracter personal pseudonimizate în scopuri științifice, de cercetare și statistice, transferurile ulterioare și normele aplicabile în contextul accesului autorităților publice la date.

1.2. Provocări

9. Deși CEPD a identificat numeroase aspecte ale cadrului coreean privind protecția datelor drept echivalente, în esență, cu cadrul european privind protecția datelor, acesta a concluzionat și că există anumite aspecte care ar putea necesita o analiză mai detaliată și clarificări. În mod special, CEPD consideră că următoarele aspecte ar trebui evaluate suplimentar, pentru a se asigura că nivelul de protecție echivalent în esență este îndeplinit și că ele ar trebui să fie monitorizate îndeaproape de Comisia Europeană.

1.2.1. Aspecte generale

10. CEPD constată că Notificarea nr. 2021-1 *are statutul unei norme administrative cu forță juridică obligatorie asupra operatorului de informații cu caracter personal, în sensul că orice încălcare a Notificării poate fi considerată o încălcare a dispozițiilor relevante ale LPICP*[7]. Totuși, având în vedere că Notificarea nu include norme suplimentare în sine, ci mai degrabă clarificări privind modul în care ar trebui să se înțeleagă aplicarea textului obligatoriu al LPICP și ținând cont de importanța sa generală, în special în ceea ce privește dispozițiile în materie de pseudonimizare prevăzute în LPICP, cu privire la care CEPD înțelege că fac obiectul unor cauze judiciare aflate pe rol, CEPD invită Comisia Europeană să furnizeze informații suplimentare privind caracterul obligatoriu, forța executorie și valabilitatea

[7] Vezi secțiunea I din anexa I la proiectul de decizie.

Notificării nr. 2021-1 și ar recomanda o monitorizare atentă a respectării sale în practică, în special în ceea ce privește aplicarea sa nu numai de către autoritatea coreeană de supraveghere, ci și de către instanțe, mai ales în cazul în care nivelul echivalent de protecție acordat de cadrul juridic coreean se bazează pe clarificările prevăzute în aceasta.

1.2.2. Aspecte generale privind protecția datelor

11. În ceea ce privește sfera de aplicare a deciziei privind caracterul adecvat al nivelului de protecție, CEPD constată că aceasta va acoperi transferurile din cadrul juridic al SEE către „operatorii de informații cu caracter personal" atât publici, cât și privați, care fac obiectul LPICP. CEPD înțelege că sunt incluse în acest termen entitățile care îndeplinesc rolul de persoană împuternicită de operator în sensul RGPD; totuși, pentru a evita neînțelegerile, acesta invită Comisia Europeană să clarifice faptul că decizia privind caracterul adecvat al nivelului de protecție se va aplica și în cazul transferurilor către „persoanele împuternicite de operator" din Coreea.

12. Un aspect important asupra căruia CEPD ar dori să atragă atenția se referă la conceptul de informații pseudonimizate în cadrul coreean privind protecția datelor. Conform dreptului coreean, în cazul prelucrării de informații cu caracter personal pseudonimizate se aplică excepții de la o serie de dispoziții relevante, inclusiv de la cele referitoare la drepturile individuale ale persoanelor vizate și la păstrarea datelor. Potrivit Comisiei Europene, acest lucru este valabil doar în cazul în care informațiile cu caracter personal pseudonimizate sunt prelucrate în scopuri statistice, de cercetare științifică sau de arhivare în interes public. Totuși, această afirmație este sprijinită în special de Notificarea nr. 2021-1, ceea ce face ca în acest context să fie extrem de relevante nevoia deja menționată de informații suplimentare privind această notificare și monitorizarea caracterului obligatoriu, a forței executorii și a valabilității acesteia. În plus, CEPD invită Comisia Europeană să evalueze mai amănunțit impactul pseudonimizării în temeiul dreptului coreean și, mai ales, cum ar putea afecta aceasta drepturile și libertățile fundamentale ale persoanelor vizate ale căror date cu caracter personal sunt transferate în Republica Coreea în temeiul deciziei privind caracterul adecvat al nivelului de protecție. În special, CEPD invită Comisia Europeană să evalueze mai amănunțit derogările prevăzute la articolul 28 alineatul (7) din LPICP și la articolul 40 alineatul (3) din Legea privind utilizarea și protecția informațiilor legate de credite și să monitorizeze cu atenție aplicarea acestora și jurisprudența relevantă, pentru a se asigura că drepturile persoanelor vizate nu sunt restricționate în mod necorespunzător atunci când se prelucrează în aceste scopuri datele cu caracter personal transferate în temeiul deciziei privind caracterul adecvat al nivelului de protecție.

13. În plus, CEPD constată că, în temeiul dreptului coreean, dreptul de a retrage consimțământul există doar în circumstanțe specifice și, prin urmare, invită Comisia Europeană să evalueze mai amănunțit impactul lipsei unui drept general de retragere a consimțământul și să ofere garanții suplimentare pentru a se asigura că se garantează în permanență un nivel esențial de protecție a datelor, inclusiv, acolo unde este necesar, prin clarificarea rolului dreptului la suspendare în temeiul LPICP în absența unui drept general de retragere a consimțământul.

14. În ceea ce privește transferurile ulterioare, CEPD recunoaște că consimțământul informat al persoanei vizate va fi folosit în general drept bază pentru transferurile de date de la un operator de informații cu caracter personal cu sediul în Coreea către un destinatar care are sediul într-o țară terță și că Notificarea nr. 2021-1 prevede că persoanele fizice trebuie să fie informate cu privire la țara terță căreia îi vor fi furnizate datele lor. Cu toate acestea, CEPD invită Comisia Europeană să se asigure că informațiile care trebuie furnizate persoanei vizate includ și informații privind posibilele riscuri ale transferurilor, care rezultă din absența unei protecții adecvate în țara terță, precum și din absența unor garanții adecvate. În plus, CEPD ar saluta prezența, în decizia privind caracterul adecvat al nivelului de protecție, a unor asigurări că datele cu caracter personal nu vor fi transferate de la operatorii coreeni de informații cu caracter personal către o țară terță în nicio situație în care nu s-ar

putea acorda un consimțământ valid în temeiul RGPD, de exemplu din cauza unui dezechilibru de putere.

15. În ceea ce privește numirea membrilor autorității coreene de supraveghere, deși procedura oficială ar fi în conformitate cu RGPD și, prin urmare, ar îndeplini testul echivalenței cu cadrul legislativ al SEE, CEPD ar invita Comisia Europeană să monitorizeze orice evoluții care ar putea afecta independența membrilor autorității de supraveghere din Coreea de Sud.

16. În ceea ce privește bugetul, tot pe baza informațiilor furnizate de Comisia Europeană, nu se face nicio referire la particularitățile personalului alocat Comisiei pentru protecția informațiilor cu caracter personal (CPICP) sau la resursele financiare puse la dispoziția acestuia. Prin urmare, CEPD ar saluta prezența, în proiectul de decizie, a unor informații suplimentare privind aceste două subiecte relevante.

1.2.3. În ceea ce privește accesul autorităților publice la datele transferate în Republica Coreea

17. De asemenea, CEPD a analizat cadrul juridic coreean în ceea ce privește accesul guvernului la datele cu caracter personal transferate din SEE în Coreea, în scopuri de aplicare a legii și de securitate națională. Deși CEPD recunoaște declarațiile și asigurările oferite de guvernul coreean, după cum se arată în anexa II la proiectul de decizie, acesta a identificat o serie de aspecte care trebuie clarificate sau care ridică semne de întrebare.

18. CEPD constată că dispozițiile LPICP se aplică fără limitări în domeniul aplicării legii. De asemenea, CEPD constată că prelucrarea datelor în domeniul securității naționale face obiectul unui set mai limitat de dispoziții prevăzute în LPICP.

19. În ceea ce privește divulgarea voluntară de informații cu caracter personal de către furnizorii de telecomunicații către autoritățile naționale de securitate, CEPD este îngrijorat că relația dintre secțiunea 3 din anexa I la proiectul de decizie, care prevede că furnizorii, în principiu, trebuie să notifice persoana vizată atunci când se conformează în mod voluntar unei cereri, și de la articolul 58 alineatul (1) punctul 2 din LPICP, adică exceptarea parțială din rațiuni de siguranță națională, este neclară. Aceasta ar putea face ca cerințele privind informarea să fie neaplicabile, iar persoanelor vizate le-ar fi mult mai dificil să își afirme drepturile în materie de protecție a datelor, în special în ceea ce privește căile de atac judiciare.

20. Deși proiectul de decizie nu prevede în mod explicit acest lucru, CEPD înțelege din explicațiile furnizate de Comisia Europeană că cadrul juridic coreean nu permite interceptarea în masă a datelor de telecomunicații. Prin urmare, jurisprudența recentă a Curții Europene a Drepturilor Omului (**„CtEDO”**) cu privire la regimurile de interceptare în masă nu ar fi relevantă în mod direct pentru evaluarea nivelului de protecție a datelor în Coreea.

21. Proiectul de decizie nu conține informații privind cadrul juridic pentru transferurile ulterioare în domeniul securității naționale. Deși CEPD a înțeles că, din punctul de vedere al Comisiei Europene, transferurile ulterioare în scopul securității naționale sunt reglementate suficient de garanțiile generale și de principiile ce rezultă din cadrul constituțional și din LPICP, CEPD este îngrijorat cu privire la măsura în care se poate considera că aceasta îndeplinește cerințele de precizie și claritate a legii și asigură garanții efective și executorii. Garanțiile la care se referă Comisia Europeană au un caracter foarte general și nu abordează, într-un temei juridic, circumstanțele și condițiile specifice în care pot avea loc transferurile ulterioare în scopul securității naționale. În acest context, CEPD constată, de asemenea, că Comisia Europeană nu a luat în considerare existența acordurilor internaționale încheiate între Republica Coreea și țări terțe sau organizații internaționale, care pot prevedea dispoziții specifice pentru transferul internațional al datelor cu caracter personal de către serviciile de aplicare a legii și/sau de informații către țări terțe. CEPD consideră că încheierea de acorduri bilaterale sau

multilaterale cu țări terțe în scopul asigurării respectării legii sau al cooperării în materie de informații este probabil să afecteze cadrul juridic coreean privind protecția datelor, astfel cum a fost evaluat.

22. CEPD constată că supravegherea asigurării respectării dreptului penal, precum și a autorităților naționale de securitate este asigurată de o combinație de diferite organisme interne și externe, în special CPICP, care este dotat cu suficiente competențe de executare.

23. Existența de remedii și căi de atac eficiente impune ca persoanele vizate să poată apela la un organism competent, care îndeplinește cerințele de la articolul 47 din Carta drepturilor fundamentale a Uniunii Europene (**„Carta”**), care are competența de a stabili faptul că are loc o prelucrare a datelor și de a verifica legalitatea prelucrării și care are competențe de remediere executorii în cazul în care prelucrarea datelor este ilegală. În acest context, CEPD invită Comisia Europeană să clarifice dacă o plângere introdusă la CPICP sau orice acțiune introdusă în instanță face obiectul cerințelor de fond și/sau de procedură, precum sarcina probei și dacă persoanele din SEE ar putea îndeplini o astfel de condiție prealabilă.

1.3. Concluzie

24. CEPD consideră că această decizie privind caracterul adecvat al nivelului de protecție este de o importanță deosebită, ținând cont și de faptul că – sub rezerva excepțiilor evidențiate în aviz – ea va acoperi atât transferurile din sectorul public, cât și pe cele din sectorul privat.

25. CEPD salută eforturile Comisiei Europene și ale autorităților coreene de a alinia cadrul juridic coreean la cel european. Îmbunătățirile urmărite să fie aduse prin Notificarea nr. 2021-1 în vederea eliminării unora dintre diferențele existente între cele două cadre juridice sunt foarte importante și bine primite. Cu toate acestea, CEPD constată că există în continuare o serie de preocupări, inclusiv în ceea ce privește Notificarea nr. 2021-1, coroborate cu necesitatea unor clarificări suplimentare asupra altor aspecte, și recomandă Comisiei Europene să abordeze preocupările și solicitările de clarificare prezentate de CEPD și să furnizeze informații și explicații suplimentare privind aspectele evidențiate în prezentul aviz.

2. INTRODUCERE

2.1. Cadrul coreean privind protecția datelor

26. Principalul act legislativ care reglementează protecția datelor în Republica Coreea este Legea privind protecția informațiilor cu caracter personal (Legea nr. 10465 din 29 martie 2011, modificată ultima dată prin Legea nr. 16930 din 4 februarie 2020, **„LPICP”**). Aceasta este completată printr-un Decret de punere în aplicare (Decretul prezidențial nr. 23169 din 29 septembrie 2011, modificat ultima dată prin Decretul prezidențial nr. 30892 din 4 august 2020, „Decretul de punere în aplicare a LPICP”), care are, din punct de vedere juridic, caracter obligatoriu și executoriu.

27. Pe lângă LPICP, cadrul coreean privind protecția datelor include „Notificări” de reglementare emise de Autoritatea coreeană de supraveghere, Comisia pentru protecția informațiilor cu caracter personal (**„CPICP”**), care oferă norme suplimentare privind interpretarea și aplicarea LPICP. Recent, CPICP a adoptat Notificarea nr. 2021-1 din 21 ianuarie 2021 (care a modificat notificarea anterioară nr. 2020-10 din 1 septembrie 2020, denumită în continuare **„Notificarea nr. 2021-1”**) privind interpretarea, aplicarea și punerea în aplicare a anumitor dispoziții ale LPICP. Mai exact, această notificare a rezultat din discuțiile privind caracterul adecvat purtate între autoritățile coreene și Comisia Europeană. Ea conține clarificări privind aplicarea anumitor dispoziții ale LPICP, inclusiv în ceea ce privește prelucrarea datelor cu caracter personal transferate în Coreea în baza deciziei privind caracterul

adecvat al nivelului de protecție avute în vedere[8] și *are statutul unei norme administrative cu forță juridică obligatorie asupra operatorului de informații cu caracter personal, în sensul că orice încălcare a Notificării poate fi considerată o încălcare a dispozițiilor relevante ale LPICP*[9]. În acest context, CEPD ar dori să precizeze că, deși în proiectul de decizie este menționată drept „norme suplimentare", notificarea nu include norme suplimentare în sine, ci mai degrabă explicații menite să clarifice modul în care ar trebui înțeles textul legal al LPICP în vederea aplicării, în special în ceea ce privește datele transferate din SEE. În acest context, CEPD ar recomanda o monitorizare atentă a respectării Notificării nr. 2021-1 în practică, în special în ceea ce privește aplicarea acesteia nu numai de către CPICP, ci și de către instanțe, mai ales atunci când nivelul echivalent de protecție acordat de cadrul juridic coreean se bazează pe clarificările furnizate în Notificarea nr. 2021-1.

28. Alte legi relevante privind protecția datelor din cadrul juridic coreean prevăd norme referitoare la prelucrarea datelor cu caracter personal în sectoare industriale specifice, precum:

- Legea privind utilizarea și protecția informațiilor legate de credite (**„LIC"**), inclusiv Decretul de punere în aplicare a acesteia (**„Decretul de punere în aplicare a LIC"**), care prevăd norme specifice aplicabile operatorilor comerciali și entităților specializate (precum agențiile de rating de credit, instituțiile financiare), atunci când prelucrează informații cu caracter personal legate de credite necesare pentru a stabili bonitatea părților la tranzacțiile financiare sau comerciale;
- Legea privind promovarea utilizării rețelei de informații și comunicații și protecția datelor (**„Legea privind rețeaua"**); și
- Legea privind protecția confidențialității comunicațiilor (**„LPCC"**)

29. În domeniul accesului guvernului, pe lângă dispozițiile relevante din LPICP și din LPCC, CEPD a luat în considerare și alte acte legislative, și anume Legea privind procedura penală (**„LPP"**), Legea privind activitățile de telecomunicații comerciale (**„LAT"**), Legea privind raportarea și utilizarea de informații specificate privind tranzacțiile financiare (**„LRUISTF"**) și Legea privind serviciul național de informații (**„LSNI"**).

2.2. Sfera de aplicare a evaluării CEPD

30. Proiectul de decizie a Comisiei Europene este rezultatul unei evaluări a cadrului coreean privind protecția datelor, care a fost urmată de discuții cu guvernul coreean. În conformitate cu articolul 70 alineatul (1) litera (s) din RGPD, se așteaptă ca CEPD să prezinte un aviz independent cu privire la constatările Comisiei Europene, să identifice, dacă există, insuficiențele din cadrul privind caracterul adecvat și să depună eforturi pentru a face propuneri în vederea rezolvării acestora.

31. Pentru a evita repetițiile și cu scopul de a contribui la evaluarea cadrului juridic coreean, CEPD a ales să se axeze pe unele aspecte specifice prezentate în proiectul de decizie și să își prezinte analiza și avizul cu privire la acestea, abținându-se de la a reproduce cea mai mare parte a constatărilor factuale și a evaluărilor acolo unde CEPD nu a avut niciun motiv pentru a presupune că dreptul Republicii Coreea nu ar fi echivalent, în esență, cu dreptul din SEE. În plus, în conformitate cu jurisprudența CJUE, o parte foarte importantă a analizei vizează regimul juridic al accesului securității naționale la datele cu caracter personal transferate în Republica Coreea și practica aparatului său de securitate națională.

32. În evaluarea sa, CEPD a ținut cont de cadrul european aplicabil privind protecția datelor, inclusiv de articolele 7, 8 și 47 din Cartă, care protejează dreptul 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, precum și de articolul 8 din Convenția Europeană a Drepturilor Omului, care protejează dreptul la viața privată și

[8] Vezi secțiunea I din anexa I la proiectul de decizie.
[9] Ibid.

de familie. În plus față de cele de mai sus, CEPD a luat în considerare cerințele RGPD, precum și jurisprudența relevantă.

33. Obiectivul acestui exercițiu este să furnizeze Comisiei Europene un aviz privind evaluarea caracterului adecvat al nivelului de protecție din Republica Coreea. Conceptul de „nivel de protecție adecvat", care exista deja în temeiul Directivei 95/46/CE, a fost dezvoltat mai detaliat de către CJUE. Este important să reamintim standardul stabilit de CJUE în cauza Schrems I, și anume că - în timp ce „nivelul de protecție" din țara terță trebuie să fie „echivalent, în esență", cu cel garantat în UE - *„mijloacele la care această țară terță a recurs, în această privință, pentru a asigura un astfel de nivel de protecție poate diferi de cele utilizate în cadrul Uniunii"*[10]. 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 cu caracter personal sau care exercită controlul asupra unor astfel de prelucrări și supravegherea de către organisme independente. Cu toate acestea, normele de protecție a datelor își produc efectele doar dacă au forță executorie și sunt respectate în practică. Este așadar necesar să se ia în considerare nu numai conținutul normelor aplicabile datelor cu caracter personal transferate într-o țară terță sau unei organizații internaționale, ci și sistemul 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[11].

2.3. Observații și preocupări de ordin general

2.3.1. Angajamente internaționale la care a aderat Republica Coreea

34. Potrivit articolului 45 alineatul (2) litera (c) din RGPD și Criteriilor de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD[12], atunci când evaluează caracterul adecvat al nivelului de protecție dintr-o țară terță, Comisia Europeană trebuie să 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.

35. Coreea este parte la mai multe acorduri internaționale care garantează dreptul la viață privată, precum Pactul internațional cu privire la drepturile civile și politice (articolul 17), Convenția Națiunilor Unite privind drepturile persoanelor cu handicap (articolul 22) și Convenția cu privire la drepturile copilului (articolul 16). În plus, în calitate de membră a OCDE, Coreea aderă la cadrul OCDE privind viața privată, în special la Orientările ce reglementează Protecția vieții private și Fluxurile transfrontaliere de date cu caracter personal.

36. De asemenea, CEPD ia act de participarea Coreei în calitate de Stat Observator la activitatea Comitetului Consultativ al Convenției 108(+) a Consiliului Europei, deși încă nu s-a hotărât dacă să adere sau nu.

2.3.2. Domeniul de aplicare al deciziei privind caracterul adecvat al nivelului de protecție

37. Potrivit considerentului 5 din proiectul de decizie, Comisia Europeană concluzionează că Republica Coreea asigură un nivel adecvat de protecție pentru datele cu caracter personal transferate de la un operator de date sau de la o persoană împuternicită de operator din Uniune către operatori de

[10] Hotărârea pronunțată în cauza C-362/14, *Maximilian Schrems /Data Protection Commissioner*, 6 octombrie 2015, ECLI:EU:C:2015:650, punctele 73-74.
[11] WP 254, p.2.
[12] WP 254, p.2.

informații cu caracter personal (de exemplu, persoane fizice sau juridice, organizații, instituții publice) care fac obiectul LPICP, cu excepția prelucrării datelor cu caracter personal pentru activități misionare de către organizații religioase și pentru desemnarea candidaților de către partidele politice[13] sau pentru prelucrarea informațiilor cu caracter personal legate de credite în temeiul LIC, de către operatori de date care sunt supravegheați de către Comisia pentru Servicii Financiare.

38. CEPD constată că decizia privind caracterul adecvat al nivelului de protecție va acoperi transferurile din cadrul juridic al SEE către „operatorii de informații cu caracter personal" atât publici, cât și privați care fac obiectul LPICP. CEPD înțelege că entitățile care îndeplinesc rolul de persoane împuternicite de operator în sensul RGPD sunt, de asemenea, vizate de termenul „operator de informații cu caracter personal", ținând cont de faptul că LPICP se va aplica în mod egal acestora și că se aplică obligații specifice atunci când un operator de informații cu caracter personal („entitatea care externalizează servicii") angajează o terță parte pentru prelucrarea informațiilor cu caracter personal („entitatea care prestează servicii externalizate"), însă, pentru a evita neînțelegerile, CEPD invită Comisia Europeană să clarifice faptul că decizia privind caracterul adecvat al nivelului de protecție se va aplica și în cazul transferurilor către „persoane împuternicite de operator" din Coreea și că nivelul de protecție a datelor cu caracter personal transferate din SEE nu va fi subminat nici în aceste cazuri.

39. De asemenea, ținând cont de faptul că decizia privind caracterul adecvat al nivelului de protecție se va aplica și în cazul transferurilor de date cu caracter personal între organisme publice, CEPD înțelege că aceasta se aplică și în cazul transferurilor dintre autoritățile de supraveghere a protecției datelor și, din rațiuni de claritate, invită Comisia Europeană să abordeze în mod explicit această problemă.

40. În plus, în ceea ce privește entitățile excluse din domeniul de aplicare al deciziei privind caracterul adecvat al nivelului de protecție, CEPD ar dori să sublinieze că decizia privind caracterul adecvat ar putea beneficia de o identificare mai clară a „organizațiilor comerciale" care fac obiectul supravegherii CPICP [articolul 45 alineatul (3) din LIC], astfel încât operatorii de date și persoanele împuternicite de operatori cu sediul în SEE să poată evalua cu ușurință dacă importatorul face, de asemenea, obiectul deciziei privind caracterul adecvat înainte de a transfera date entităților care intră sub incidența LIC sau, cel puțin, să fie avertizați cu privire la necesitatea evaluării acestui aspect.

41. În ceea ce privește domeniul de aplicare al deciziei privind caracterul adecvat al nivelului de protecție, CEPD a înțeles, din explicațiile suplimentare ale Comisiei Europene, că Unitatea de Informații Financiare din Coreea („UIFC"), care este instituită sub egida Comisiei pentru Servicii Financiare și care supraveghează prevenirea spălării banilor și a finanțării terorismului în temeiul LRUISTF[14], este, de asemenea, exclusă din domeniul de aplicare, întrucât are jurisdicție doar asupra instituțiilor financiare care nu fac nici ele obiectul proiectului de decizie. Totuși, articolul 1 alineatul (2) litera (c) din proiectul de decizie îi exclude din domeniul de aplicare doar pe acei operatori de informații cu caracter personal care sunt supravegheați de Comisia pentru servicii financiare și prelucrează informații cu caracter personal legate de credite în temeiul LIC. În acest context, CEPD solicită Comisiei Europene să clarifice dacă UIFC și activitățile de prelucrare a datelor întreprinse chiar de UIFC fac obiectul proiectului de decizie.

3. ASPECTE GENERALE PRIVIND PROTECȚIA DATELOR

3.1. Principii privind conținutul

42. Capitolul 3 din Criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD e dedicat „Principiilor privind conținutul". Sistemul unei țări terțe trebuie să le includă pentru

[13] Pentru un context mai amplu, vezi secțiunea 3.1.2 de mai jos din prezentul aviz.
[14] Vezi anexa II, secțiunea 2.2.3.1.

ca nivelul de protecție conferit să fie considerat echivalent, în esență, cu cel garantat prin legislația UE.

43. Deși dreptul la protecția datelor cu caracter personal nu este prevăzut în mod explicit, per se, în Constituția Coreei, acesta este recunoscut ca un drept de bază, ce derivă din drepturile constituționale la demnitate umană și la căutarea fericirii (articolul 10), la viață privată (articolul 17) și la confidențialitatea comunicațiilor (articolul 18). Aceste aspecte au fost confirmate atât de Curtea Supremă, cât și de Curtea Constituțională, astfel cum se menționează în proiectul de decizie al Comisiei Europene[15]. CEPD ia act de această recunoaștere, întrucât din ea rezultă că protecția datelor ca drept de bază, potrivit articolului 37 din Constituția Coreei, *„poate fi restricționată doar prin lege și atunci când acest lucru este necesar pentru securitatea națională sau pentru menținerea legii și a ordinii ori pentru bunăstarea publică”* și că *„inclusiv atunci când sunt impuse astfel de restricții, ele nu pot să afecteze esența libertății sau a dreptului”.*

44. Potrivit Comisiei Europene[16], Curtea Constituțională a decis că drepturile de bază se aplică și în cazul cetățenilor străini. Conform declarațiilor oficiale ale guvernului coreean[17], deși până în prezent jurisprudența nu a abordat în mod explicit dreptul la viață privată al cetățenilor care nu sunt coreeni, este acceptat la modul general de specialiști că articolele 12-22 din Constituție stabilesc „drepturi ale ființelor umane”. În plus, Republica Coreea a adoptat o serie de legi în domeniul protecției datelor care oferă garanții tuturor persoanelor, indiferent de cetățenie, precum LPICP. În acest sens, CEPD constată că articolul 6 alineatul (2) din Constituție prevede că statutul cetățenilor străini este garantat conform dreptului internațional și tratatelor și jurisprudenței menționate în proiectul de decizie conform căreia un „cetățean străin” poate fi titular de „drepturi de bază”. Ținând cont de relevanța recunoașterii dreptului la protecția datelor pentru „cetățenii străini”, CEPD atrage atenția Comisiei Europene asupra nevoii de a monitoriza în continuare jurisprudența privind protecția datelor, ca un drept de bază recunoscut nu numai pentru cetățenii coreeni, ci pentru toate persoanele vizate, pentru a se asigura faptul că nivelul de protecție a persoanelor fizice, garantat prin RGPD, nu este subminat atunci când datele cu caracter personal sunt transferate în Coreea în temeiul deciziei privind caracterul adecvat al nivelului de protecție.

3.1.1. Concepte

45. Pe baza Criteriilor de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD, cadrul juridic al țării terțe ar trebui să includă concepte și/sau principii de bază privind protecția datelor. Chiar dacă acestea nu trebuie să corespundă terminologiei RGPD, ele ar trebui să reflecte și să fie în concordanță cu conceptele consacrate în legislația europeană privind protecția datelor. 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 sensibile”[18].

46. LPICP include o serie de definiții precum, printre altele, cele pentru „informații cu caracter personal”, „prelucrare” și „persoană vizată”, care seamănă îndeaproape cu termenii corespunzători din RGPD.

3.1.1.1. Conceptul de date pseudonimizate

47. Printre definițiile prevăzute în LPICP, articolul 2 alineatul (1) din aceasta definește în special informațiile cu caracter personal drept oricare dintre următoarele informații referitoare la o persoană aflată în viață: (a) informații care identifică o anumită persoană după numele său complet, după codul

[15] Vezi considerentul 8 din proiectul de decizie și jurisprudența relevantă menționată la nota de subsol nr. 10 din proiectul de decizie, pentru care sunt disponibile doar rezumate în limba engleză.
[16] Vezi considerentul 9 din proiectul de decizie.
[17] Secțiunea 1.1 din anexa II la proiectul de decizie.
[18] WP 254, p. 4.

de înregistrare a rezidenților, după imagine etc. și (b) informații care, chiar dacă, în sine, nu identifică o anumită persoană, pot fi combinate cu ușurință cu alte informații pentru a identifica o anumită persoană. În această ultimă situație, ușurința combinării se stabilește prin evaluarea rezonabilă a timpului, costului, tehnologiei etc. folosite pentru a identifica persoana, precum și probabilitatea ca celelalte informații să poată fi obținute.

48. În plus, potrivit articolului 2 alineatul (1) litera (c) din LPICP, și „informațiile pseudonimizate" sunt considerate informații cu caracter personal. Informațiile pseudonimizate sunt definite drept informațiile prevăzute la literele (a) sau (b) de mai sus care sunt pseudonimizate în conformitate cu punctele 1-2 și, astfel, devin incapabile să identifice o anumită persoană fără utilizarea sau combinarea de informații în vederea revenirii la starea inițială. Informațiile complet anonimizate sunt excluse din sfera de aplicare a LPICP. Conform articolului 58 alineatul (2) din LPICP, legea nu se aplică în cazul informațiilor care nu mai identifică o anumită persoană atunci când sunt combinate cu alte informații, ținând cont în mod rezonabil de timp, costuri, tehnologie etc.

49. La considerentul 17 din proiectul său de decizie, Comisia Europeană precizează că aceasta corespunde domeniului de aplicare material al RGPD și noțiunilor sale de „date cu caracter personal", „pseudonimizare" și „informații anonimizate".

50. Totuși, potrivit articolului 28 alineatul (7) din LPICP, articolul 20, articolul 21, articolul 27, articolul 34 alineatul (1), articolele 35-37 și articolul 39 alineatele (3), (4), (6)-(8) nu se aplică în cazul informațiilor cu caracter personal pseudonimizate.

51. În proiectul său de decizie, Comisia Europeană afirmă că articolul 28 alineatul (7) din LPICP se aplică doar în cazul informațiilor cu caracter personal pseudonimizate atunci când acestea sunt prelucrate în scopuri statistice, de cercetare științifică sau de arhivare în interes public[19]. Totuși, acest lucru nu rezultă direct din litera legii, ci din explicațiile furnizate în Notificarea nr. 2021-1[20]. Deși CEPD recunoaște că un argument poate fi susținut pe baza structurii și raționamentului LPICP în sensul că articolul 28 alineatul (2) din LPICP ar trebui înțeles și interpretat în mod logic ca aplicându-se și articolului 28 alineatul (7) din LPICP, în considerararea importanței Notificării nr. 2021-1 în evaluarea Uniunii Europene a adecvării nivelului de protecție a datelor cu caracter personal în Republica Coreea și pentru a se evita orice dubii, CEPD invită Comisia Europeană să furnizeze informații suplimentare privind caracterul obligatoriu, forța executorie și valabilitatea Notificării nr. 2021-1 și să monitorizeze aplicarea sa în acest context specific.

52. În acest context, CEPD ar dori să reamintească faptul că, în temeiul RGPD, pseudonimizarea este înțeleasă ca o măsură de securitate recomandată. Cu alte cuvinte, în temeiul RGPD, datele pseudonimizate rămân date cu caracter personal cu privire la care RGPD se aplică pe deplin. Pe baza acestor considerente, CEPD este îngrijorat de faptul că nivelul de protecție a datelor cu caracter personal pseudonimizate, astfel cum este prevăzut în RGPD, ar putea fi subminat atunci când sunt transferate date cu caracter personal în Coreea,. Prin urmare, CEPD invită Comisia Europeană să evalueze mai detaliat impactul pseudonimizării în temeiul LPICP și, mai ales, cum ar putea afecta aceasta drepturile și libertățile fundamentale ale persoanelor vizate ale căror date cu caracter personal ar fi transferate în Republica Coreea în temeiul deciziei privind caracterul adecvat al nivelului de protecție. Așadar, CEPD invită Comisia Europeană să ofere asigurări că nivelul de protecție a datelor cu caracter personal de la persoanele vizate din SEE nu va fi redus după transferul în Republica Coreea, chiar și atunci când datele cu caracter personal transferate sunt pseudonimizate.

[19] Vezi, printre altele, considerentul 82 din proiectul de decizie.
[20] Secțiunea 4 din anexa I la proiectul de decizie.

3.1.1.2. Conceptul de operator de informații cu caracter personal

53. Articolul 2 alineatul (5) din LPICP include o definiție a „operatorului de informații cu caracter personal", adică o instituție publică, o persoană juridică, o organizație sau o persoană fizică etc. care prelucrează informații cu caracter personal în mod direct sau indirect pentru a opera dosare de informații cu caracter personal *„în cadrul activităților sale".* Totuși, în garanțiile suplimentare prevăzute în Notificarea nr. 2021-1, termenul „operator de informații cu caracter personal" este definit ca o instituție publică, o persoană juridică, o organizație sau o persoană fizică etc. care prelucrează informații cu caracter personal în mod direct sau indirect pentru a opera dosare de informații cu caracter personal *„în scopuri comerciale".* În schimb, nota de subsol nr. 272 din proiectul de decizie precizează următoarele cu privire la noțiunea de operator de informații cu caracter personal: *„Astfel cum este definită la articolul 2 din LPICP, adică o instituție publică, o persoană juridică, o organizație sau o persoană fizică etc. care prelucrează informații cu caracter personal în mod direct sau indirect pentru a opera dosare de informații cu caracter personal «în scopuri oficiale sau comerciale»".*

54. CEPD recunoaște că aceste inconsecvențe se pot datora traducerilor textului original, astfel cum au fost furnizate de autoritățile coreene, și invită Comisia Europeană să verifice în mod regulat calitatea și certitudinea traducerilor. Totuși, CEPD precizează că, pentru a putea evalua echivalența în esență a nivelului de protecție a datelor în cadrul juridic coreean, este necesară o înțelegere clară a scopurilor prelucrării ce se încadrează în domeniul de aplicare material al LPICP. Mai mult, în acest context, CEPD constată că LPICP nu folosește aceeași terminologie a RGPD în ceea ce privește noțiunile de „operator" și „persoană împuternicită de operator" și invită Comisia Europeană să clarifice definiția corectă și sfera de aplicare a conceptului de „operator de informații cu caracter personal" și să precizeze în mod explicit dacă acest termen se referă și la persoanele împuternicite de operator în sensul RGPD, întrucât aceasta afectează în mod direct domeniul de aplicare al deciziei privind caracterul adecvat al nivelului de protecție.[21]

3.1.2. Excepții parțiale prevăzute în LPICP

55. Articolul 58 alineatul (1) din LPICP exclude aplicarea unor părți din LPICP (și anume a articolelor 15-57) în ceea ce privește patru categorii de prelucrare a datelor cu caracter personal, astfel cum sunt descrise mai jos. Mai exact, excepțiile se referă la dispozițiile LPICP cu privire la temeiurile specifice pentru prelucrare, la anumite obligații privind protecția datelor, la regulile detaliate pentru exercitarea drepturilor individuale și la normele care reglementează soluționarea litigiilor. Totuși, CEPD constată că unele dispoziții generale ale LPICP încă rămân aplicabile, precum cele referitoare la principiile privind protecția datelor (articolul 3 din LPICP) și la drepturile individuale (articolul 4 din LPICP). În plus, articolul 58 alineatul (4) din LPICP stabilește obligații specifice privind acele patru categorii de prelucrare a datelor.

56. În primul rând, excepția parțială se referă la informațiile cu caracter personal colectate în temeiul Legii privind statisticile în vederea prelucrării de către instituțiile publice. La considerentul 27 din proiectul său de decizie, Comisia Europeană precizează că, potrivit clarificărilor primite de la guvernul coreean, datele cu caracter personal prelucrate în acest context se referă în mod normal la cetățenii coreeni și ar putea include doar în mod excepțional informații privind cetățenii străini, și anume în cazul statisticilor legate de intrarea pe teritoriul țării și părăsirea acestuia sau privind investițiile străine. Totuși, potrivit proiectului de decizie, chiar și în aceste situații, astfel de date nu se transferă în mod normal de la operatorii/persoanele împuternicite de operatori din SEE, ci, mai degrabă, ar fi colectate direct de autoritățile publice din Coreea.

57. CEPD recunoaște raționamentul Comisiei Europene privind caracterul excepțional al aplicării Legii privind statisticile în cazul prelucrării datelor cu caracter personal transferate în temeiul deciziei privind caracterul adecvat al nivelului de protecție; totuși, ar saluta furnizarea unor informații și

[21] Vezi și punctul 38 de mai sus.

asigurări suplimentare privind garanțiile specifice care s-ar aplica în cazul în care datele cu caracter personal transferate din SEE sunt colectate ulterior în temeiul Legii privind statisticile pentru prelucrarea de către instituțiile publice, în special în ceea ce privește exercitarea drepturilor individuale de către persoanele vizate în conformitate cu articolul 89 alineatul (2) din RGPD în măsura în care aceste drepturi nu sunt susceptibile de a împiedica sau a îngreuna în mod semnificativ atingerea scopurilor specifice, iar aceste derogări nu sunt necesare pentru atingerea acelor scopuri.

58. Din această perspectivă, aplicarea articolului 4 din LPICP și în cazul acestui tip de prelucrare pare să ofere asigurări; totuși, CEPD ar saluta informații și clarificări suplimentare în decizia privind caracterul adecvat al nivelului de protecție cu privire la obligațiile specifice impuse asupra activităților de prelucrare respective în conformitate cu articolul 58 alineatul (4) din LPICP, și anume în ceea ce privește minimizarea datelor, păstrarea limitată a datelor, măsurile de securitate și soluționarea plângerilor.

59. În al doilea rând, excepția parțială vizează informațiile cu caracter personal colectate sau solicitate spre furnizare pentru analiza informațiilor referitoare la securitatea națională. CEPD este conștient de faptul că, în probleme care țin de securitatea națională, statele au o marjă largă de apreciere recunoscută de CtEDO. De asemenea, CEPD constată că, potrivit articolului 37 alineatul (2) din Constituția Coreei, orice restricționare a libertăților și a drepturilor, de exemplu atunci când este necesară pentru protecția securității naționale, nu poate încălca aspectul esențial al libertății sau al dreptului în cauză. În plus, CEPD ia act de garanțiile prevăzute în secțiunea 6 din Notificarea nr. 2021-1 privind prelucrarea informațiilor cu caracter personal în scopuri de securitate națională, inclusiv pentru anchetarea încălcărilor și pentru aplicarea legii. Totuși, în acest context, CEPD invită Comisia Europeană să clarifice suplimentar sfera de aplicare a excepțiilor, întrebându-se dacă toate excepțiile prevăzute la articolul 58 alineatul (1) punctul 2 din LPICP (capitolele III-VII) sunt relevante pentru activitatea serviciilor de informații și dacă acestea asigură echivalența cu principiile necesității și proporționalității. În special, CEPD invită Comisia Europeană să ofere clarificări suplimentare privind circumstanțele în care un serviciu de informații s-ar putea baza pe excepții. CEPD consideră că este nevoie să se monitorizeze îndeaproape impactul acestor limitări în practică, în special asupra exercitării efective și a asigurării respectării drepturilor persoanelor vizate.

60. În al treilea rând, excepția parțială se aplică în cazul „*informațiilor cu caracter personal prelucrate temporar, atunci când acest lucru este necesar de urgență din rațiuni legate de siguranță și securitate publică, sănătate publică etc.*”. Potrivit considerentului 29 din proiectul de decizie al Comisiei Europene, această categorie este interpretată în mod strict de CPICP și se aplică doar în situații de urgență care necesită măsuri urgente, de exemplu pentru urmărirea agenților contagioși sau pentru salvarea și ajutorarea victimelor dezastrelor naturale.

61. De asemenea, CEPD subliniază că orice derogare de la nivelul de protecție a datelor cu caracter personal ar trebui interpretată cu strictețe. Totodată, CEPD constată că dispoziția nu este definită în mod strict și nu conține o listă exhaustivă de exemple de situații în care prelucrarea informațiilor cu caracter personal ar putea fi considerată *„necesară de urgență”*. De exemplu, CEPD este îngrijorat de măsura în care transferurile internaționale de date privind sănătatea în timpul actualei pandemii de COVID-19 ar face, de asemenea, obiectul acestei excepții. În contextul celor expuse mai sus, CEPD invită Comisia Europeană să furnizeze clarificări suplimentare privind sfera de aplicare a acestei excepții și să monitorizeze pe deplin aplicarea și obiectul acesteia pentru a se asigura că ea nu conduce la scăderea nivelului de protecție a datelor cu caracter personal din SEE după ce sunt transferate în Coreea în baza deciziei privind caracterul adecvat al nivelului de protecție.

62. În final, excepția parțială se aplică în cazul informațiilor cu caracter personal colectate sau utilizate în cadrul raportării de către presă, a activităților de misionariat ale organizațiilor religioase și a

desemnării candidaților de către partidele politice[22]. În ceea ce privește prelucrarea informațiilor cu caracter personal de către presă pentru activități jurnalistice, Comisia Europeană precizează la considerentul 31 din proiectul său de decizie că echilibrul dintre libertatea de exprimare și alte drepturi, inclusiv dreptul la viață privată, este asigurat prin Legea privind arbitrajul și căile de atac etc. pentru daunele provocate de relatări în presă (numită în continuare **„Legea privind presa”**) și prezintă garanții specifice care decurg din Legea privind presa. Totuși, CEPD ar invita Comisia Europeană să monitorizeze pe deplin această excepție și jurisprudența relevantă pentru a se asigura că un nivel echivalent de protecție a datelor este asigurat și în practică în cadrul juridic coreean.

3.1.3. Temeiuri pentru prelucrarea legală și echitabilă în scopuri legitime

63. Potrivit Criteriilor de referință privind caracterul adecvat al nivelului de protecție, în conformitate cu RGPD datele trebuie prelucrate în mod legal, corect și legitim. Temeiul juridic în baza căruia datele cu caracter personal pot fi prelucrate în mod legal, corect și legitim ar trebui stabilit 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 interesele legitime ale operatorului de date sau ale unui terț care nu prevalează asupra intereselor persoanei.

64. Urmând o structură similară RGPD, LPICP introduce mai întâi principiul legalității, al echității și al transparenței [articolul 3 alineatele (1) și (2) din LPICP], prevăzând ulterior regulile specifice pentru aplicarea acestora (articolele 15-19 din LPICP). Mai exact, articolul 15 din LPICP include un catalog al temeiurilor juridice pe care se pot baza operatorii de informații cu caracter personal pentru a colecta informații cu caracter personal și pentru a le utiliza în scopul colectării. Aceste temeiuri juridice constau în: (1) consimțământul informat al persoanei vizate; (2) autorizarea statutară sau necesitatea respectării unei obligații legale; (3) necesitatea îndeplinirii îndatoririlor unei instituții publice; (4) necesitatea în vederea executării sau a derulării unui contract cu o persoană vizată; (5) necesitatea în vederea protejării vieții, a integrității fizice sau a proprietății persoanei vizate sau ale unei terțe părți de un pericol iminent (și dacă nu se poate obține consimțământul prealabil); (6) necesitatea obținerii unui interes justificabil al unui operator de informații cu caracter personal care este superior celui al unei persoane vizate.

65. În plus, articolul 17 din LPICP enumeră temeiurile juridice aplicabile pentru partajarea de informații cu caracter personal cu o terță parte, care includ: (1) consimțământul informat al persoanei vizate; (2) autorizarea statutară sau necesitatea în vederea respectării unei obligații legale; (3) necesitatea în vederea îndeplinirii îndatoririlor unei instituții publice; și (4) necesitatea în vederea protejării vieții, a integrității fizice sau a proprietății persoanei vizate sau ale unei terțe părți de un pericol iminent (și dacă nu se poate obține consimțământul prealabil). Chiar și în absența consimțământului persoanei vizate, partajarea de informații cu caracter personal este permisă atunci când aceasta are loc în sfera de aplicare care are legătură, în mod rezonabil, cu scopurile pentru care au fost colectate inițial informațiile cu caracter personal [articolul 17 alineatul (4) din LPICP].

66. Articolul 18 din LPICP prevede norme specifice pentru utilizarea și partajarea informațiilor cu caracter personal atunci când acest lucru se întâmplă în afara scopului inițial al colectării sau al furnizării. Printre altele, consimțământul reprezintă o astfel de normă de autorizare și în acest caz.

67. Deși recunoaște similitudinile substanțiale dintre dreptul coreean și RGPD în ceea ce privește principiul legalității și existența unui drept general la suspendare (articolul 37 din LPICP), care se pot invoca și

[22] În consecință, prelucrarea informațiilor cu caracter personal de către organizații religioase pentru activitățile lor de misionariat și prelucrarea informațiilor cu caracter personal de către partide politice în contextul desemnării candidaților sunt, de asemenea, excluse din sfera de aplicare a deciziei privind caracterul adecvat al nivelului de protecție. Vezi și punctul 37 de mai sus, de la secțiunea 2.3.2.

atunci când sunt prelucrate date cu caracter personal pe baza consimțământului, CEPD ar dori să remarce lipsa unui drept general de a retrage consimțământul în temeiul LPICP[23]. În lumina importanței consimțământului ca temei juridic în toate scenariile descrise mai sus și ținând cont de rolul drepturilor individuale într-un sistem juridic de protecție a datelor în vederea garantării drepturilor și libertăților fundamentale ale persoanelor vizate, CEPD invită Comisia Europeană să evalueze în continuare impactul lipsei unui drept general de a retrage consimțământul în temeiul dreptului coreean și să ofere asigurări suplimentare pentru a se asigura că se garantează în permanență un nivel esențial de protecție a datelor echivalent cu cel acordat prin RGPD, inclusiv, acolo unde este necesar, prin clarificarea rolului dreptului la suspendare în acest context specific.

3.1.4. Principiul limitărilor legate de scop

68. Criteriile de referință privind caracterul adecvat al nivelului de protecție, în conformitate cu RGPD, prevăd că datele cu caracter personal ar trebui prelucrate într-un anumit scop și folosite ulterior doar în măsura în care această utilizare nu este incompatibilă cu scopul prelucrării.

69. În conformitate cu articolul 3 alineatele (1) și (2) din LPICP, operatorii de informații cu caracter personal ar trebui să specifice și să detalieze scopurile prelucrării și să se asigure că prelucrarea este compatibilă cu aceste scopuri. Deși acest principiu este confirmat în alte dispoziții [și anume, la articolul 15 alineatul (1), la articolul 18 alineatul (1) și la articolul 19 alineatul (1) din LPICP], prelucrarea în scopuri care au „legătură, în mod rezonabil" este permisă în anumite circumstanțe [vezi articolul 17 alineatul (4) din LPICP][24], la fel ca utilizarea și furnizarea de informații cu caracter personal în afara scopului (vezi articolele 18 și 19 din LPICP)[25].

70. CEPD înțelege că, în cazul transferurilor de date cu caracter personal din SEE în Republica Coreea pe baza deciziei privind caracterul adecvat al nivelului de protecție, scopul colectării efectuate de operatorii cu sediul în SEE constituie scopul pentru care sunt transferate datele, aplicabil prelucrării de către operatorul de informații cu caracter personal din Coreea, care primește datele. O modificare a scopului de către operatorul de informații cu caracter personal din Coreea ar fi permisă doar conform articolului 18 alineatul (2) punctul 1-3 din LPICP, *„cu excepția cazului în care o astfel de situație ar putea încălca în mod neechitabil interesul unei persoane vizate sau al unei terțe părți"*[26]. În acest context, CEPD recunoaște afirmația Comisiei Europene de la considerentul 55 din proiectul de decizie, potrivit căreia, atunci când legea permite schimbările de scop, aceste legi trebuie să respecte dreptul fundamental la viață privată și la protecția datelor. Totuși, CEPD constată că nu au fost furnizate informații concrete care să susțină această afirmație; de exemplu, nu s-a făcut nicio referire la articolul 37 din Constituția Coreei. Prin urmare, CEPD invită Comisia Europeană să ofere, în proiectul de decizie, asigurări și garanții suplimentare pentru a se asigura că orice legi care autorizează schimbarea scopului

[23] Chiar dacă persoanele vizate pot refuza consimțământul în anumite circumstanțe, vezi, de exemplu, articolul 18 alineatul (3) punctul 5 din LPICP. Dimpotrivă, dreptul de a retrage consimțământul pare să existe doar în anumite situații; în temeiul articolului 27 alineatul (1) punctul 2 din LPICP, persoanele vizate au dreptul de a-și retrage consimțământul atunci când nu doresc ca informațiile lor cu caracter personal să fie transferate către o terță parte ca urmare a transferului integral sau parțial al activității unui operator de informații cu caracter personal, a unei fuziuni etc.; în temeiul articolului 39 alineatul (7) din LPICP, utilizatorii își pot retrage în orice moment consimțământul în ceea ce privește colectarea, utilizarea și furnizarea informațiilor cu caracter personal de către furnizorul de servicii de informații și comunicații etc.; și în temeiul articolului 37 din LIC, o persoană vizată de informațiile legate de credite poate revoca consimțământul pe care l-a acordat unui furnizor/utilizator al informațiilor legate de credite.

[24] Unde compatibilitatea scopului trebuie constatată în prealabil, pe baza criteriilor prevăzute la articolul 14-2 din Decretul de punere în aplicare a LPICP.

[25] Vezi și punctul 66 de mai sus.

[26] Articolul 18 alineatul (2) din LPICP.

prelucrării trebuie să respecte drepturile și libertățile fundamentale ale persoanelor vizate la viață privată și la protecția datelor.

3.1.5. Principiul calității și proporționalității datelor

71. Criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD precizează că datele ar trebui să fie exacte și, atunci când este nevoie, actualizate. Datele ar trebui să fie adecvate, relevante și neexcesive în ceea ce privește scopurile în care sunt prelucrate.

72. În conformitate cu LPICP, operatorii de informații cu caracter personal trebuie să se asigure că informațiile cu caracter personal sunt corecte, complete și actualizate în măsura necesară pentru scopurile în care sunt prelucrate informațiile cu caracter personal [articolul 3 alineatul (3) din LPICP]. Operatorii de informații cu caracter personal trebuie să colecteze cât mai puține informații cu caracter personal este nevoie pentru a atinge un anumit scop. Acestora le revine sarcina probei în acest sens [articolul 16 alineatul (1) din LPICP].

73. În acest context, CEPD împărtășește evaluarea Comisiei Europene în ceea ce privește echivalența în esență a nivelului de protecție asigurat prin LPICP comparativ cu RGPD în acest sens.

3.1.6. Principiul păstrării datelor

74. În conformitate cu Criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD, ca o regulă generală datele nu ar trebui păstrate pe o perioadă mai lungă decât este necesar în scopurile pentru care sunt prelucrate datele cu caracter personal. Conform articolului 21 alineatul (1) din LPICP, acest principiu există și în dreptul coreean. În temeiul LPICP, operatorii de informații cu caracter personal trebuie să distrugă fără întârziere informațiile cu caracter personal atunci când acestea devin inutile la expirarea perioadei de păstrare sau la realizarea scopului urmărit al prelucrării, cu excepția cazului în care se aplică perioade obligatorii de păstrare.

75. Totuși, CEPD este îngrijorat de faptul că articolul 21 alineatul (1) din LPICP nu se aplică în cazul informațiilor cu caracter personal pseudonimizate. CEPD ia act de faptul că, potrivit secțiunii 4 punctul (iii) din Notificarea nr. 2021-1, *„atunci când un operator de informații cu caracter personal prelucrează informații pseudonimizate cu scopul de a compila statistici, de a desfășura cercetări științifice, de a menține evidențe publice etc. și dacă informațiile pseudonimizate nu au fost distruse odată ce scopul specific al prelucrării a fost atins în conformitate cu articolul 37 din Constituție și cu articolul 3 (Principiile privind protecția informațiilor cu caracter personal) din Lege, acesta anonimizează informațiile pentru a se asigura că acestea nu mai identifică o anumită persoană, singure sau în combinație cu alte informații, ținând cont în mod rezonabil de timp, costuri, tehnologie etc., în conformitate cu articolul 58 alineatul (2) din LPICP.”* Având în vedere, și în acest caz, importanța Notificării nr. 2021-1 și pentru a asigura securitatea juridică în ceea ce privește echivalența nivelului de protecție a datelor cu caracter personal transferate în Republica Coreea în temeiul deciziei privind caracterul adecvat al nivelului de protecție, CEPD își reiterează solicitarea adresată Comisiei Europene de a furniza informații suplimentare privind în mod specific modul prin care Notificarea nr. 2021-1 va căpăta un caracter obligatoriu și prin care i se vor asigura forța executorie și valabilitatea[27].

3.1.7. Principiul securității și confidențialității

76. După cum este descris în Criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD, principiul securității și confidențialității prevede că entitățile de prelucrare a datelor trebuie să se asigure că datele cu caracter personal sunt prelucrate într-o manieră care să asigure securitatea acestora, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva

[27] Vezi mai sus și punctul 51 de la secțiunea 3.1.1.1 din prezentul aviz, precum și punctul 52, pentru preocupările generale ale CEPD privind impactul pseudonimizării în temeiul dreptului coreean.

pierderii, a distrugerii sau a deteriorării accidentale, folosind măsuri tehnice sau organizatorice adecvate. Nivelul de securitate ar trebui să țină cont de stadiul actual al tehnologiei și de costurile aferente.

77. Comisia Europeană a identificat un principiu similar cu cel al securității datelor la articolul 3 alineatul (4) din LPICP, care este detaliat ulterior la articolul 29 din LPICP. În plus, dispozițiile privind securitatea datelor se aplică atunci când operatorul informațiilor cu caracter personal angajează o „entitate care prestează servicii externalizate". Securitatea prelucrării trebuie asigurată prin garanții la nivel tehnic și managerial, care trebuie incluse, de asemenea, în acordul obligatoriu privind prelucrarea datelor (articolele 26 și 28 din Decretul de punere în aplicare a LPICP). În plus, conform LPICP, se aplică obligații specifice în cazul unei încălcări a securității datelor, inclusiv obligația de a notifica persoanele vizate afectate și autoritatea de supraveghere atunci când numărul persoanelor vizate afectate depășește pragul aplicabil (articolul 34 din LPICP în coroborare cu articolul 39 din Decretul prezidențial privind LPICP), cu excepția cazului în care datele afectate sunt informații cu caracter personal pseudonimizate, prelucrate în scopuri statistice, de cercetare științifică sau de arhivare în interes public [articolul 28 alineatul (7) din LPICP]. Și în acest caz[28], CEPD este îngrijorat de excepțiile ample aplicabile în cazul informațiilor pseudonimizate și își reiterează solicitarea adresată Comisiei Europene de a evalua suplimentar acest aspect pentru a se asigura că dreptul coreean prevede un nivel de protecție care, în esență, este echivalent[29].

78. Cu toate acestea, per ansamblu, CEPD este mulțumit de evaluarea și de concluziile Comisiei Europene privind echivalența în esență a dreptului coreean în ceea ce privește principiul securității și confidențialității.

3.1.8. Principiul transparenței

79. În temeiul articolului 5 alineatul (1) litera (a) din RGPD, transparența este un principiu fundamental al sistemului de protecție a datelor din UE. Considerentul 39 din RGPD evidențiază funcția esențială a acestui principiu, precizând că *„[a]r trebui să fie transparent pentru persoanele fizice că sunt colectate, utilizate, consultate sau prelucrate în alt mod datele cu caracter personal care le privesc și în ce măsură datele cu caracter personal sunt sau vor fi prelucrate. (...) Persoanele fizice ar trebui informate cu privire la riscurile, normele, garanțiile și drepturile în materie de prelucrare a datelor cu caracter personal și cu privire la modul în care să își exercite drepturile în legătură cu prelucrarea.~*

80. Criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD desemnează în mod explicit „transparența" drept unul dintre principiile privind conținutul care trebuie luate în considerare la evaluarea nivelului de protecție echivalent în esență asigurat de o terță țară. Mai exact, acestea prevăd că *„fiecare persoană ar trebui să fie informată cu privire la toate elementele principale ale prelucrării datelor sale cu caracter personal, într-o manieră clară, ușor accesibilă, concisă, transparentă și inteligibilă. Astfel de informații ar trebui să includă scopul prelucrării, identitatea operatorului de date, drepturile de care beneficiază persoana și alte informații, în măsura în care acest lucru este necesar pentru a asigura echitatea. În anumite condiții, pot exista unele excepții de la acest drept la informare, precum, de exemplu, pentru a proteja anchetele penale, securitatea națională, independența judiciară și procedurile judiciare sau alte obiective importante de interes public general, ca în cazul articolului 23 din RGPD."*

81. La fel ca în cazul RGPD, există și în LPICP un principiu general al transparenței, potrivit căruia operatorii de informații cu caracter personal trebuie să își facă publică politica de confidențialitate și alte aspecte legate de prelucrarea informațiilor cu caracter personal [articolul 3 alineatul (5) din LPICP]. Se aplică obligații specifice în materie de informare atunci când operatorii de informații cu caracter personal încearcă să obțină consimțământul persoanelor vizate pentru colectarea și prelucrarea informațiilor

[28] După cum s-a menționat deja la punctele 51-52 de mai sus și în secțiunea 3.1.1.1 din prezentul aviz.
[29] Vezi și secțiunile 3.1.6 și 3.1.10 din prezentul aviz.

cu caracter personal [articolul 15 alineatul (2) din LPICP], pentru partajarea informațiilor cu caracter personal cu o terță parte [articolul 17 alineatul (2) din LPICP] și pentru prelucrare în afara scopurilor urmărite [articolul 18 alineatul (3) din LPICP]. Trebuie menționat faptul că aceste obligații de informare se aplică *mutatis mutandis* și în cazul entității care prestează servicii externalizate [articolul 26 alineatul (7) din LPICP].

82. CEPD recunoaște și salută garanțiile suplimentare din secțiunea 3 punctele (i) și (iii) din Notificarea nr. 2021-1[30] referitoare la informațiile care trebuie furnizate persoanelor vizate atunci când datele lor sunt transferate de o entitate din SEE, ținând cont de faptul că, în temeiul articolului 20 alineatul (1) din LPICP, atunci când datele nu s-au obținut de la persoanele vizate, acestea sunt informate doar la cerere, în timp ce un drept general de a fi informat este recunoscut doar în temeiul articolului 20 alineatul (2) din LPICP, atunci când anumite operațiuni de prelucrare depășesc pragurile prevăzute în Decretul de punere în aplicare a LPICP [articolul 15 alineatul (2)].

83. Per ansamblu, CEPD este mulțumit că nivelul de protecție asigurat în temeiul dreptului coreean în ceea ce privește principiul transparenței este echivalent în esență cu cel asigurat în temeiul RGPD.

3.1.9. Categorii speciale de date cu caracter personal

84. Pentru ca sistemul de protecție a datelor dintr-o țară terță să fie recunoscut drept oferind un nivel de protecție a datelor cu caracter personal echivalent în esență cu cel al RGPD, ar trebui să existe garanții specifice atunci când sunt implicate categorii speciale de date cu caracter personal, în sensul articolelor 9 și 10 din RGPD.

85. Conform LPICP, se aplică dispoziții specifice în cazul prelucrării așa-numitelor informații sensibile, care includ informații cu caracter personal ce dezvăluie ideologia, convingerile, înscrierea sau retragerea dintr-un sindicat sau dintr-un partid politic, opiniile politice, sănătatea, viața sexuală și alte informații cu caracter personal care ar putea amenința vizibil viața privată a oricărei persoane vizate, precum și, prin trimitere la Decretul de punere în aplicare a LPICP, informații privind ADN-ul obținute în urma testării genetice, date care constituie cazier judiciar, informații cu caracter personal ce rezultă din prelucrarea tehnică specifică a datelor privind caracteristicile fizice, fiziologice sau comportamentale ale unei persoane în scopul identificării unice a acelei persoane și informații cu caracter personal care dezvăluie originea rasială sau etnică.

86. În mod asemănător cu RGPD, dreptul coreean privind protecția datelor interzice prelucrarea informațiilor sensibile cu excepția cazului în care se aplică excepții specifice, și anume (1) informarea persoanei vizate și obținerea unui consimțământ explicit și (2) dispoziții legale care autorizează prelucrarea [articolul 23 alineatul (2) din LPICP].

87. În acest sens, CEPD este de acord în principiu cu concluzia Comisiei Europene privind echivalența în esență a dreptului coreean în ceea ce privește prelucrarea categoriilor speciale de date cu caracter personal. Totuși, CEPD ar dori să remarce că nu i s-au pus la dispoziție Manualul LPICP sau clarificări din partea CPICP cu privire la faptul că termenul „viață sexuală” este interpretat drept cuprinzând și orientarea sau preferințele sexuale ale persoanei, care nu au fost incluse în Notificarea nr. 2021-1. Prin urmare, CEPD solicită Comisiei Europene să furnizeze aceste informații, pentru a le putea evalua în mod independent. De asemenea, CEPD invită Comisia Europeană să menționeze în mod explicit documentele în care se pot găsi informațiile la care face referire în această privință.

[30] Anexa I la proiectul de decizie.

3.1.10. Dreptul de acces, dreptul la rectificare, dreptul la ștergerea datelor și dreptul la opoziție

88. Conform cadrului juridic coreean, drepturile persoanelor vizate sunt recunoscute la articolul 3 alineatul (5) din LPICP – potrivit căruia operatorul de informații cu caracter personal trebuie să garanteze drepturile persoanelor vizate enumerate la articolul 4 din LPICP și menționate în continuare la articolele 35-37, 39 și 39 alineatul (2) din LPICP și, în ceea ce privește „informațiile cu caracter personal legate de credite" (adică „informațiile legate de credite care sunt informații necesare pentru a stabili bonitatea părților la tranzacții financiare sau comerciale – vezi considerentul 3 din propunerea de decizie), la articolele 37, 38, 38 alineatul (3) din LIC.

89. CEPD constată că dreptul de acces (și dreptul la rectificare și dreptul la ștergerea datelorcare pot fi exercitate de o *„persoană vizată care și-a accesat propriile informații cu caracter personal în temeiul articolului 35"* din LPICP) poate fi limitat sau refuzat *„atunci când accesul este interzis sau limitat prin legi", „atunci când accesul poate dăuna vieții sau organismului unei părți terțe sau în cazul încălcării nejustificate a proprietății și a altor interese ale oricărei alte persoane"* și, în plus, în cazul instituțiilor publice, atunci când acordarea accesului *„ar genera dificultăți grave"* în îndeplinirea anumitor funcții, specificate în continuare la articolul 35 alineatul (4) din LPICP[31]. La articolul 37 din LPICP sunt menționate dispoziții similare privind dreptul de suspendare a prelucrării informațiilor cu caracter personal.

90. Articolul 23 din RGPD permite dreptului Uniunii sau al Statelor Membre să restricționeze drepturile individuale atunci când o astfel de restricționare respectă esența drepturilor și libertăților fundamentale și este o măsură necesară și proporțională într-o societate democratică, și are în vedere astfel de restricții pentru a asigura, printre altele, protecția persoanei vizate sau drepturile și libertățile altor persoane și o *„funcție de monitorizare, inspectare sau reglementare legată, chiar și ocazional, de exercitarea autorității oficiale în cazurile menționate la literele (a)-(e) și (g) din același articol"*.

91. În acest context, CEPD ar saluta prevederea unor asigurări generale în proiectul de decizie în ceea ce privește necesitatea ca orice lege sau statut care limitează drepturile persoanelor vizate să îndeplinească cerințele Constituției Coreei, care prevăd că un drept fundamental poate fi restricționat doar atunci când acest lucru este necesar pentru securitatea națională sau pentru a menține legea și ordinea pentru bunăstarea publică, iar această limitare nu poate afecta esența dreptului sau a libertății vizate [articolul 37 alineatul (2) din Constituția coreeană].

92. În plus, în ceea ce privește excepția legată de *„o încălcare nejustificată a proprietății sau a altor interese ale oricăror altor persoane"*, CEPD recunoaște că *„aceasta înseamnă că ar trebui să existe o echilibrare între drepturile și libertățile persoanei, astfel cum sunt protejate prin constituție, pe de o parte, și cele ale altor persoane, pe de altă parte"*[32], însă ar invita Comisia Europeană să monitorizeze pe deplin aplicarea acestei excepții și jurisprudența relevantă pentru a se asigura că în cadrul juridic coreean se asigură și în practică un nivel echivalent de protecție a drepturilor persoanei vizate.

93. În același sens, CEPD ar saluta monitorizarea cu atenție a aplicării excepției pentru organismele publice, în special în ceea ce privește cazurile când s-ar considera că acordarea accesului ar cauza *„dificultăți grave"* în îndeplinirea îndatoririlor acestora, considerând că această expresie pare mai largă decât cea folosită în alte dispoziții ale LPICP, de exemplu la articolul 18 alineatul (2) punctul 5[33] și ar

[31] Aceleași condiții și excepții de la drepturile de acces și rectificare prevăzute de LPICP se aplică și în ceea ce privește drepturile de acces și de rectificare prevăzute de LIC pentru informațiile cu caracter personal legate de credite (nota de subsol nr. 135 din proiectul de decizie).
[32] Considerentul 76 din proiectul de decizie.
[33] În ceea ce privește excepțiile de la limitarea utilizării și a furnizării de informații cu caracter personal în afara scopurilor prevăzute, articolul 18 alineatul (2) punctul 5 din LPICP se referă la situații în care instituțiilor publice le este *„imposibil"* să își îndeplinească îndatoririle.

trebui interpretată în mod restrictiv, pentru a evita orice restricții necorespunzătoare asupra drepturilor persoanei vizate.

94. În plus, CEPD este preocupat dacă excepțiile potrivit cărora dispozițiile referitoare la transparența la cerere (articolul 20 din LPICP) și la drepturile individuale (articolele 35-37 din LPICP) – precum și dispozițiile similare referitoare la cerințele pentru furnizorii de servicii de informații și comunicații [articolul 39 alineatele (2), (6)-(8) din LPICP] și cele din LIC [vezi excepțiile prevăzute la articolul 40 alineatul (3) din LIC] – nu se aplică în cazul informațiilor pseudonimizate, atunci când acestea sunt prelucrate în scopuri statistice, de cercetare științifică sau de arhivare în interes public [articolul 28 alineatul (7) din LPICP] sunt conforme cu garanțiile prevăzute în cadrul juridic european.

95. Aceste dispoziții par să introducă o derogare generală pentru o astfel de prelucrare, în timp ce RGPD prevede că, atunci când datele cu caracter personal (inclusiv datele cu caracter personal pseudonimizate) sunt prelucrate în scopuri de cercetare științifică sau istorică sau în scopuri statistice, dreptul Uniunii sau al Statelor Membre poate prevedea derogări de la drepturile persoanelor vizate, dar numai *„în măsura în care drepturile respective sunt de natură să facă imposibilă sau să afecteze în mod grav realizarea scopurilor specifice, iar derogările respective sunt necesare pentru îndeplinirea acestor scopuri”*, pseudonimizarea fiind doar una dintre măsurile tehnice și organizatorice care trebuie adoptate pentru a asigura respectarea principiului reducerii la minimum a datelor [articolul 89 alineatul (1) din RGPD].

96. Comisia Europeană consideră că derogarea prevăzută la articolul 28 alineatul (7) din LPICP se justifică și în lumina articolului 28 alineatul (5) din LPICP, prin care operatorului de informații cu caracter personal i se interzice în mod explicit să prelucreze informațiile pseudonimizate în vederea identificării unei anumite persoane și face referire la abordarea de la articolul 11 alineatul (2) din RGPD (coroborat cu considerentul 57 din RGPD) referitoare la prelucrarea care nu necesită identificare[34].

97. Într-adevăr, potrivit articolului 11 din RGPD, operatorul nu are obligația de a *„păstra, obține sau prelucra informații suplimentare pentru a identifica persoana vizată*” în scopul unic al respectării RGPD dacă, pentru scopurile urmărite, acesta poate prelucra date cu caracter personal care nu necesită sau nu mai necesită identificarea unei persoane vizate; în astfel de cazuri, când operatorul poate demonstra că nu este în măsură să identifice persoana vizată, nu se aplică drepturile persoanei vizate. După cum a recunoscut Comisia Europeană[35], RGPD impune, prin urmare, în astfel de cazuri, o imposibilitate „practică” pentru operatorul de date și, în conformitate cu principiul reducerii la minimum a datelor, recunoaște că nu trebuie prelucrate date suplimentare „din cauza” RGPD.

98. Totuși, CEPD consideră că această situație diferă față de cea în care un operator este practic în măsură să identifice persoana vizată, dar nu are voie să facă acest lucru din cauza unei dispoziții obligatorii, precum cea de la articolul 28 alineatul (5) din LPICP. În această privință, CEPD salută clarificările furnizate de CPICP în Notificarea nr. 2021-1[36], confirmând că secțiunea 3 din LPICP [inclusiv articolul 28 alineatul (7)] și excepția de la articolul 40 alineatul (3) din LIC se aplică doar atunci când se prelucrează informații pseudonimizate în scopuri de cercetare științifică, statistice sau de arhivare în interes public. Totuși – și pe lângă preocupările deja menționate cu privire la caracterul obligatoriu efectiv al Notificării nr. 2021-1[37], CEPD încă se întreabă dacă derogările prevăzute la articolul 28

[34] A se nota că același raționament nu ar fi aplicabil ca atare în cazul excepției prevăzute la articolul 40 alineatul (3) din LIC pentru prelucrarea informațiilor pseudonimizate legate de credite, fiindcă articolul 40 alineatul (2) punctul 6 prevede că: *„O societate de informații de credit etc. nu ar trebui să prelucreze informațiile pseudonimizate astfel încât o anumită persoană să poată fi identificată în scopuri lucrative sau abuzive”* și, prin urmare, ar putea permite reidentificarea într-un scop echitabil, precum cel de a îndeplini o solicitare a unei persoane vizate.

[35] Vezi considerentul 82 din proiectul de decizie.

[36] Secțiunea 4 din anexa I la proiectul de decizie.

[37] Vezi secțiunea 3.1.1.1 de mai sus.

alineatul (7) din LPICP și la articolul 40 alineatul (3) din LIC ar putea fi considerate necesare și proporționale într-o societate democratică în măsura în care restricționează drepturile persoanelor vizate în toate cazurile în care sunt prelucrate informații pseudonimizate în aceste scopuri – adică chiar și atunci când operatorul de informații cu caracter personal este practic în măsură să identifice persoana vizată, iar drepturile nu sunt susceptibile de a face imposibilă sau de a afecta în mod semnificativ atingerea scopurilor specifice.

99. În special, CEPD este îngrijorat de faptul că aceste derogări nu ar fi justificate și ar trebui analizate în continuare, mai ales dacă se aplică de către operatorul de informații cu caracter personal care pseudonimizează datele *„în scopuri statistice, de cercetare științifică și de arhivare în interes public etc.”*, în conformitate cu articolul 28 alineatul (2) din LPICP *„fără consimțământul persoanelor vizate”* (și fără a furniza informațiile prevăzute la articolul 20 din LPICP)[38], în măsura în care acest operator păstrează informațiile care permit reidentificarea. În temeiul RGPD, persoanele ar trebui să își poată exercita drepturile în ceea ce privește orice informație care le poate identifica sau evidența, chiar dacă se consideră că informațiile sunt „pseudonimizate”, cu excepția cazului în care se aplică articolul 11 din RGPD, deja menționat. În acest sens, CEPD constată că, doar atunci când aceste date sunt furnizate unei părți terțe în aceleași scopuri statistice, de cercetare științifică și de arhivare, informațiile care pot fi folosite pentru a identifica o anumită persoană nu ar trebui incluse și, prin urmare, doar operatorul de informații cu caracter personal căruia i se furnizează date pseudonimizate conform articolului 28-2 alineatul (2) din LPICP nu ar fi probabil „practic” în măsură să identifice persoana vizată fără informații suplimentare.

100. În concluzie, având în vedere faptul că, după cum recunoaște Comisia Europeană, *„în loc să se bazeze pe pseudonimizare ca o posibilă garanție, LPICP o impune ca o condiție prealabilă pentru efectuarea anumitor activități de prelucrare în scopuri statistice, de cercetare științifică și de arhivare în interes public (de exemplu, pentru a putea prelucra datele fără consimțământ sau pentru a combina diferite seturi de date)”*[39], însă are în vedere, pentru astfel de cazuri, restricții importante asupra drepturilor persoanelor vizate, CEPD invită Comisia Europeană să evalueze mai amănunțit derogările prevăzute la articolul 28 alineatul (7) din LPICP și la articolul 40 alineatul (3) din LIC și să monitorizeze cu atenție aplicarea acestora și jurisprudența relevantă[40], pentru a se asigura că drepturile persoanei vizate nu vor fi restricționate în mod necorespunzător atunci când datele cu caracter personal transferate în temeiul deciziei privind caracterul adecvat al nivelului de protecție sunt prelucrate în aceste scopuri, ținând cont de faptul că, în multe cazuri, aceste drepturi îl ajută și pe operator să asigure calitatea datelor prelucrate.

3.1.11. Restricții privind transferurile ulterioare

101. Criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD clarifică faptul că nivelul de protecție a persoanelor fizice ale căror date cu caracter personal sunt transferate în temeiul unei decizii privind caracterul adecvat al nivelului de protecție nu trebuie să fie subminat de transferul ulterior și, prin urmare, orice transfer ulterior *„ar trebui permis doar atunci când destinatarul ulterior (adică destinatarul transferului ulterior) este supus tot unor norme (inclusiv normelor contractuale) care acordă un nivel adecvat de protecție și respectă instrucțiunile relevante atunci când prelucrează date în numele operatorului de date”.*

[38] Vezi articolul 28 alineatul (7) din LPICP, astfel cum este explicat în Notificarea nr. 2021-1, potrivit căreia anumite garanții prevăzute în LPICP, și anume *„articolele 20, 21, 27, articolul 34 alineatul (1), articolele 35-37 și articolul 39 alineatele (3), (4), (6)-(8)*”, nu ar trebui să se aplice în cazul informațiilor pseudonimizate prelucrate în scopul realizării de statistici, în scopuri de cercetare științifică, pentru păstrarea evidențelor publice etc.

[39] Considerentul 42 din proiectul de decizie.

[40] Vezi, de exemplu, provocările constituționale ale Open Net (informații la adresa https://opennet.or.kr/19909, disponibile doar în limba coreeană).

102. În ceea ce privește transferurile ulterioare către entitățile care prestează servicii externalizate („persoanele împuternicite de operator”) stabilite în alte țări terțe, CEPD constată că în cadrul juridic coreean nu sunt instituite norme speciale care să acopere aceste situații și că, după cum consideră Comisia Europeană[41], un operator de informații cu caracter personal din Coreea trebuie să asigure respectarea dispozițiilor LPICP privind externalizarea (articolul 26 din LPICP) prin intermediul unui instrument obligatoriu din punct de vedere juridic și va fi responsabil pentru informațiile cu caracter personal care au fost externalizate (articolul 26 din LPICP).

103. În ceea ce privește transferurile ulterioare către părți terțe (adică alți operatori de informații cu caracter personal), potrivit articolului 17 alineatul (3) din LPICP, un operator de informații cu caracter personal din Coreea trebuie să informeze persoanele vizate cu privire la transferurile în străinătate și să obțină consimțământul lor în acest sens și *„să nu încheie un contract pentru transferul transfrontalier de informații cu caracter personal cu încălcarea LPICP”*. CEPD constată că această ultimă dispoziție va asigura – în opinia Comisiei Europene[42] – că niciun contract pentru transferuri transfrontaliere nu ar putea conține obligații care contravin cerințelor impuse de LPICP asupra operatorului de informații cu caracter personal și, prin urmare, ar putea fi considerat drept o garanție; totuși, această măsură nu impune vreo obligație de a institui garanții pentru a asigura faptul că destinatarul va acorda același nivel de protecție prevăzut de LPICP. Prin urmare, CEPD recunoaște că, în general, consimțământul în cunoștință de cauză al persoanei vizate va fi folosit drept temei pentru transferurile de date de la un operator de informații cu caracter personal cu sediul în Coreea către un destinatar cu sediul într-o țară terță.

104. În acest sens, clarificările suplimentare oferite de CPICP în Notificarea nr. 2021-1 privind obligația de a informa persoanele cu privire la țara terță în care vor fi furnizate datele lor[43] sunt bine-venite întrucât acestea – astfel cum sunt evidențiate de Comisia Europeană[44] – ar ajuta persoanele vizate din SEE să ia o decizie în deplină cunoștință de cauză cu privire la aprobarea furnizării în străinătate sau nu.

105. Totuși, după cum se prevede și în avizul nr. 28/2018 referitor la Proiectul de decizie de punere în aplicare al Comisiei Europene privind protecția adecvată a datelor cu caracter personal în Japonia, trebuie evidențiat faptul că, în temeiul RGPD, persoanele vizate trebuie să fie informate în mod explicit cu privire la posibilele riscuri ale unor astfel de transferuri, ce rezultă din absența unei protecții adecvate în țara terță și din absența garanțiilor corespunzătoare anterioare consimțământului. Această notificare ar trebui să includă, de exemplu, informații cu privire la posibilitatea să nu existe o autoritate de supraveghere și/sau principii de prelucrare a datelor și/sau drepturi ale persoanelor vizate în țara terță[45]. Pentru CEPD, furnizarea acestor informații este esențială pentru a permite persoanelor vizate să-și acorde consimțământul în deplină cunoștință a acestor elemente specifice transferului[46]. Prin urmare, CEPD este îngrijorat de constatările Comisiei Europene din proiectul de decizie privind caracterul adecvat al nivelului de protecție referitoare la acest tip de transferuri. De regulă, persoanele vizate nu cunosc cadrul de protecție a datelor din țări terțe. Așadar, nu se poate concluziona că o persoană vizată ar putea evalua riscul unui transfer doar știind care este țara de destinație. Trebuie să existe mai degrabă o informare clară cu privire la riscurile specifice ale unui astfel de transfer de date cu caracter personal către o țară din afara teritoriului Republicii Coreea, înainte de consimțământul persoanei vizate.

[41] Considerentul 87 din proiectul de decizie.
[42] Considerentul 88 din proiectul de decizie.
[43] Ibid.
[44] Ibid.
[45] Orientările CEPD 2/2018 privind derogările de la articolul 49 în conformitate cu Regulamentul (UE) 2016/679, 25 mai 2018, p.8.
[46] Orientările CEPD 2/2018 privind derogările de la articolul 49 în conformitate cu Regulamentul (UE) 2016/679, 25 mai 2018, p.7.

106. Astfel, CEPD invită Comisia Europeană să se asigure că informațiile care trebuie furnizate persoanei vizate *„cu privire la circumstanțele asociate transferului”* includ și informații privind posibilele riscuri ale transferului ce rezultă din absența unei protecții adecvate în țara terță și a unor garanții adecvate. Acest lucru este important pentru ca CEPD să evalueze dacă cerințele privind consimțământul sunt echivalente în esență cu RGPD.

107. În plus, ținând cont de faptul că consimțământul trebuie să fie acordat în mod liber, în cunoștință de cauză, clar și neambiguu, CEPD ar saluta prezența, în decizia privind caracterul adecvat al nivelului de protecție, a unor asigurări ferme că datele cu caracter personal nu vor fi transferate de la operatorii coreeni de informații cu caracter personal către o parte terță dintr-o țară terță în nicio situație în care nu s-ar putea acorda un consimțământ valid în temeiul RGPD, de exemplu din cauza unui dezechilibru de putere.

108. În ceea ce privește situațiile în care operatorul de informații cu caracter personal poate furniza informații cu caracter personal unei părți terțe din străinătate fără consimțământul persoanei vizate – adică, (1) dacă sunt furnizate informații cu caracter personal într-un context care are o legătură rezonabilă cu scopul inițial al colectării potrivit articolului 17 alineatul (4) din LPICP; și (2) dacă pot fi furnizate informații cu caracter personal unei părți terțe în cazurile excepționale menționate la articolul 18 alineatul (2) din LPICP – CEPD ia act de clarificările furnizate de CPICP în secțiunea 2 din Notificarea nr. 2021-1 [și salută obligația avută în vedere spre a fi impusă operatorului cu sediul în Coreea și destinatarului din străinătate de a asigura, printr-un instrument obligatoriu din punct de vedere juridic (precum un contract), un nivel de protecție echivalent cu LPICP, inclusiv în ceea ce privește drepturile persoanei vizate].

3.1.12. Marketingul direct

109. Potrivit articolului 21 alineatul (2) și articolului 21 alineatul (3) din RGPD și Criteriilor de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD, persoana vizată trebuie să fie întotdeauna în măsură să obiecteze, în mod gratuit, față de prelucrarea datelor în vederea creării de profiluri și a marketingului direct.

110. În ceea ce privește dreptul la suspendare prevăzut la articolul 37 din LPICP, CEPD recunoaște că Comisia Europeană consideră că acest drept se aplică și atunci când datele se folosesc în scopuri de marketing direct[47]. Totuși, CEPD ar saluta furnizarea, în proiectul de decizie, a unor informații și clarificări suplimentare cu privire la această evaluare și, în special, cu privire la aplicarea practică a dreptului la suspendare în contextul marketingului direct (de exemplu, trimiteri la jurisprudența relevantă etc.). În acest sens, CEPD ar evidenția și faptul că dreptul de a solicita unui furnizor/utilizator de informații legate de credite să nu mai contacteze persoana vizată pentru a prezenta bunuri sau servicii sau pentru a solicita achiziționarea acestora este prevăzut în mod explicit în LIC [articolul 37 alineatul (2)].

111. În plus, după cum recunoaște Comisia Europeană[48], în cadrul juridic coreean o astfel de prelucrare impune de obicei consimțământul explicit (suplimentar) al persoanei vizate [vezi articolul 15 alineatul (1) punctul 1, articolul 17 alineatul (2) punctul 1 din LPICP].

112. Întrucât nu se poate exclude posibilitatea ca date cu caracter personal transferate din SEE să fie prelucrate în Coreea în astfel de scopuri, CEPD ar saluta, de asemenea, în decizia privind caracterul adecvat al nivelului de protecție clarificări cu privire la existența dreptului persoanei vizate de a-și

[47] Considerentul 79 din proiectul de decizie.
[48] Ibid.

retrage consimțământul[49] și a dreptului ca datele sale cu caracter personal să fie șterse și să nu mai fie prelucrate atunci când prelucrarea se bazează pe consimțământ (de exemplu, în cazul prelucrării efectuate în scopuri de marketing), iar persoana vizată și-a retras consimțământul.

3.1.13. Procesul decizional automatizat și crearea de profiluri

113. După cum a recunoscut Comisia Europeană în proiectul său de decizie[50], LPICP și decretul său de punere în aplicare a acesteia nu conțin dispoziții generale care să abordeze problema deciziilor care afectează persoana vizată și care se bazează exclusiv pe prelucrarea automată a datelor cu caracter personal. Totuși, sistemul juridic coreean prevede un astfel de drept în LIC, care conține norme privind deciziile automatizate [articolul 36 alineatul (2)], chiar dacă aplicarea acestora pare să nu intre sub incidența supravegherii CPICP (și, ca atare, nu intră sub incidența acestui proiect de decizie – vezi secțiunea 2.3.2 de mai sus privind domeniul de aplicare al proiectului de decizie).

114. După cum a remarcat deja Grupul de lucru Articolul 29[51], în avizul său nr. 1/2016 privind Scutul de confidențialitate, și CEPD, în avizul său precedent referitor la decizia privind caracterul adecvat al nivelului de protecție cu privire la Japonia[52], importanța tot mai mare a procesului decizional automatizat, a creării de profiluri și a IA ar sugera adoptarea unei abordări mai protectoare în acest sens. Contrar argumentelor Comisiei Europene[53], potrivit cărora este puțin probabil ca absența unor norme specifice privind procesul decizional automatizat în LPICP să afecteze nivelul de protecție în ceea ce privește datele cu caracter personal care au fost colectate în Uniune (întrucât orice decizie bazată pe prelucrarea automată ar fi luată, în mod normal, de operatorul din Uniune care are o relație directă cu persoana vizată în cauză), CEPD consideră că nu se poate exclude ca procesul decizional automatizat să fie folosit de un operator de informații cu caracter personal din Coreea în cazul datelor transferate în temeiul deciziei privind caracterul adecvat al nivelului de protecție (de exemplu, în contextul angajării, pentru evaluarea performanței în muncă, a seriozității, a conduitei etc.).

115. Dezvoltarea de noi tehnologii permite societăților să pună mai ușor în aplicare sau să ia în considerare punerea în aplicare de sisteme decizionale automatizate care ar putea conduce la slăbirea poziției persoanelor. Atunci când deciziile adoptate exclusiv de aceste sisteme automatizate impactează situația juridică a persoanelor sau le afectează semnificativ (de exemplu, prin introducerea lor pe o listă neagră și, astfel, prin privarea persoanelor de drepturile lor), este esențial să se asigure suficiente garanții, inclusiv dreptul de a fi informat cu privire la motivele specifice care stau la baza deciziei și la logica implicată, de a corecta informații inexacte sau incomplete și de a contesta decizia, dacă aceasta a fost adoptată pe o bază factuală incorectă[54].

116. În acest context, CEPD este îngrijorat de absența din LPICP a unor dispoziții legale privind procesul decizional automatizat și, prin urmare, invită Comisia Europeană să abordeze această preocupare și să monitorizeze în continuare evoluția cadrului juridic coreean în acest sens.

---

[49] Vezi și punctul 67 de mai sus: Deși posibilitatea de a revoca consimțământul este prevăzută în mod clar la articolul 37 alineatul (1) din LIC, acest drept este menționat doar de două ori în LPICP pentru circumstanțe specifice, și anume la articolul 27 alineatul (1) punctul 2 și la articolul 39 alineatul (7).

[50] Vezi considerentul 81 din proiectul de decizie.

[51] 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. WP 29 a devenit acum CEPD.

[52] Avizul 28/2018 referitor la Proiectul de decizie de punere în aplicare a Comisiei privind protecția adecvată a datelor cu caracter personal în Japonia, adoptat la 5 decembrie 2018.

[53] Considerentul 81 din proiectul de decizie.

[54] WP 254, p. 7.

3.1.14. Responsabilitatea

117. Cadrul juridic coreean conține mai multe norme menite să asigure faptul că operatorii de informații cu caracter personal instituie măsuri tehnice și organizatorice adecvate pentru a-și îndeplini în mod efectiv obligațiile privind protecția datelor și pentru a putea demonstra această conformitate, printre altele inclusiv autorității de supraveghere competente. În special, CEPD salută existența unor norme care prevăd adoptarea unui plan de management intern (articolul 29 din LPICP), a obligației de a efectua o așa-numită evaluare a impactului asupra vieții private (**„EIC"**) pentru cazurile în care prelucrarea prezintă un risc mai ridicat de posibile încălcări ale vieții private [articolul 33 alineatul (1) din LPICP și articolul 35 din Decretul de punere în aplicare a LPICP], a normelor privind formarea și supravegherea personalului (articolul 28 din LPICP), precum și a obligației de a desemna un responsabil cu protecția vieții private (articolul 31 din LPICP coroborat cu articolul 32 din Decretul de punere în aplicare a LPICP).

118. CEPD împărtășește opinia Comisiei Europene în ceea ce privește protecția echivalentă în esență pe care o asigură aceste norme – chiar și în cazurile când normele par să difere oarecum de cele prevăzute în RGPD, de exemplu atunci când nu există nicio dispoziție care să prevadă că responsabilul cu protecția vieții private trebuie să fie independent, însă este prevăzut în mod clar că acesta trebuie să raporteze conducerii operatorului informațiilor cu caracter personal [articolul 31 alineatul (4) din LPICP] și că nu trebuie să fie defavorizat în mod nejustificat ca urmare a îndeplinirii acestor funcții [articolul 31 alineatul (5) din LPICP] – și ar sugera Comisiei Europene să monitorizeze, atunci când revizuiește decizia privind caracterul adecvat al nivelului de protecție, aplicarea efectivă a acestor dispoziții pentru a evalua punerea lor reală în aplicare.

3.2. Mecanisme procedurale și de punere în aplicare

119. În baza criteriilor prevăzute în Criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD, CEPD a analizat următoarele aspecte ale cadrului juridic coreean privind protecția datelor așa cum este reglementat în proiectul de decizie: existența și funcționarea efectivă a unei autorități independente de supraveghere; existența unui sistem care să asigure un nivel de conformitate adecvat și un sistem de acces la mecanismele de recurs adecvate care să asigure persoanelor fizice din SEE mijloacele de exercitare a drepturilor și căi de atac fără obstacole dificile în calea accesului la mecanismele de recurs judiciare și administrative.

120. În conformitate cu capitolul VI din RGPD și cu capitolul 3 din Criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD, trebuie să existe una sau mai multe autorități de supraveghere independente, însărcinate cu monitorizarea, asigurarea și impunerea respectării dispozițiilor privind protecția datelor și viața privată într-o țară terță, pentru a asigura un nivel de protecție echivalent cu cel din SEE.

121. În acest context, autoritatea de supraveghere din țara terță trebuie să acționeze într-o manieră pe deplin independentă și imparțială în îndeplinirea atribuțiilor și în exercitarea competențelor sale și, prin aceasta, nu va solicita și nici nu va accepta instrucțiuni. În plus, autoritatea de supraveghere ar trebui să dispună de toate competențele și misiunile necesare și disponibile pentru a asigura respectarea drepturilor privind protecția datelor și pentru a promova conștientizarea. De asemenea, ar trebui avute în vedere personalul și bugetul autorității de supraveghere. Totodată, autoritatea de supraveghere ar trebui să fie în măsură să declanșeze proceduri din proprie inițiativă.

3.2.1. Autoritatea de supraveghere independentă competentă

122. În Republica Coreea, autoritatea independentă însărcinată cu monitorizarea și aplicarea LPICP este CPICP. CPICP este formată dintr-un președinte, un vicepreședinte și șapte comisari. Președintele și vicepreședintele sunt numiți de președintele statului, la recomandarea prim-ministrului. Dintre comisari, doi sunt numiți la recomandarea președintelui, doi la recomandarea reprezentanților

partidului politic din care face parte președintele, iar ceilalți trei la recomandarea reprezentanților celorlalte partide politice [articolul 7 alineatul (2) (2) din LPICP]. CPICP este asistată de un secretariat [articolul 7 alineatul (13)] și poate institui subcomisii (formate din trei comisari) care să trateze încălcările minore și aspectele recurente [articolul 7 alineatul (12) din LPICP].

123. În acest sens, CEPD recunoaște că, în pofida reorganizării sale recente, care i-a modificat profund statutul și competențele, CPICP a depus eforturi majore pentru construirea infrastructurii necesare pentru punerea în aplicare a LPICP și a celor mai recente modificări ale acesteia. Printre aceste eforturi se poate aminti instituirea normelor LPICP, elaborarea de orientări pentru facilitarea interpretării LPICP și înființarea unei linii de asistență pentru informarea operatorilor comerciali și a persoanelor fizice cu privire la dispozițiile în domeniul protecției datelor, precum și a unui serviciu de mediere pentru tratarea plângerilor. În special, sarcinile CPICP includ consilierea cu privire la legi și reglementări referitoare la protecția datelor, elaborarea de politici și orientări privind protecția datelor, investigarea încălcărilor drepturilor individuale, tratarea plângerilor și medierea conflictelor, aplicarea LPICP, asigurarea educației și promovării în domeniul protecției datelor și schimburile și cooperarea cu autoritățile pentru protecția datelor din țări terțe[55].

124. Numirea și componența CPICP sunt prevăzute la articolul 7 alineatul (2) din LPICP. Deși CPICP se află sub jurisdicția prim-ministrului (iar președintele și vicepreședintele sunt numiți de președintele statului la recomandarea prim-ministrului), cadrul juridic prevede obligația comisarilor de a-și îndeplini îndatoririle în mod independent, conform legii și propriei conștiințe. CEPD recunoaște garanțiile instituționale și procedurale prevăzute în LPICP și mai ales la articolul 7 alineatele (4)-(7). Totuși, CEPD ar recomanda Comisiei Europene să monitorizeze eventuale evoluții care ar putea afecta independența membrilor autorității de supraveghere din Coreea de Sud.

125. În plus, proiectul de decizie încă nu cuprinde o analiză a bugetului CPICP, inclusiv a surselor de finanțare și a transparenței bugetare. CEPD este de părere că acest element, menționat atât la articolul 56 alineatul (1) din RGPD, cât și în principiile și mecanismele procedurale și de aplicare a protecției datelor care trebuie avute în vedere în temeiul Criteriilor de referință privind caracterul adecvat al nivelului de protecție în temeiul RGPD atunci când se evaluează sistemul unei țări sau al unei organizații internaționale, trebuie luat în considerare în mod deosebit, fiind un indicator al resurselor economice și umane pe care le are la dispoziție autoritatea de supraveghere pentru a-și îndeplini în mod independent obligațiile și sarcinile statutare privind protecția datelor și, prin urmare, ar recomanda Comisiei Europene să țină cont de el într-o manieră mai detaliată în proiectul de decizie.

3.2.2. Existența unui sistem de protecție a datelor care asigură un nivel adecvat de conformitate

126. În domeniul aplicării legii, CEPD recunoaște gama de competențe de punere în aplicare și de sancțiuni pe care le are la dispoziție CPICP, astfel cum este prevăzut în LPICP și în LIC și ia act de clarificările din Notificarea nr. 2021-1, potrivit cărora condițiile menționate la articolul 64 alineatul (1) din LPICP și la articolul 45 alineatul (4) din LIC[56] se vor aplica ori de câte ori se încalcă oricare dintre principiile, drepturile și îndatoririle incluse în legea privind protejarea informațiilor cu caracter personal. Totuși, CEPD ar recomanda Comisiei Europene să monitorizeze îndeaproape aplicarea în practică a competențelor CPICP de a ordona entității vinovate de încălcare să ia măsura pe care o consideră adecvată dintre cele enumerate la articolul 64 alineatul (1) sau la articolul 45 alineatul (4) din LIC.

[55] Sarcinile și competențele CPICP sunt prevăzute în principal la articolul 7 alineatele (8) și (9) și la articolele 61-66 din LPICP.

[56] Și anume, *„se consideră că o încălcare a legii poate aduce atingere drepturilor și libertăților persoanelor în ceea ce privește informațiile cu caracter personal, iar neluarea de măsuri poate provoca daune greu de remediat”.*

127. În plus, în ceea ce privește măsurile corective prevăzute la articolul 64 alineatul (1) din LPICP, în cazul nerespectării unei măsuri corective, CPICP este împuternicită să impună o amendă de cel mult 50 de milioane de woni coreeni [articolul 75 alineatul (2) punctul 13 din LPICP]. Această sumă este echivalentul a 36 564 EUR. CEPD consideră și este îngrijorat că această valoare limitată a sancțiunilor pecuniare ar putea să nu aibă un efect de descurajare suficient de puternic asupra entităților care încalcă dispozițiile, după cum ar intenționa legea pentru a asigura respectarea normelor privind protecția datelor, fiindcă nu pare suficientă pentru a descuraja încălcările, mai ales în cazul organizațiilor mari sau al întreprinderilor cu resurse financiare semnificative.

128. În ceea ce privește posibilitatea ca CPICP să solicite ca șeful unei agenții administrative centrale să investigheze operatorul de informații cu caracter personal sau să se implice într-o investigație comună privind încălcarea LPICP și chiar să impună măsuri corective în ceea ce-i privește pe operatorii de informații cu caracter personal din jurisdicția sa [articolul 63 alineatele (4)-(5) din LPICP], CEPD constată că, deși au fost furnizate unele informații la considerentul 122 din proiectul de decizie, natura acestor alte agenții și raporturile lor juridice cu CPICP rămân, mai degrabă, neclare. În plus, articolul 68 alineatul (1) din LPICP se referă la numeroase entități cărora li s-ar putea delega autoritatea CPICP. Chiar dacă pare că această dispoziție s-a aplicat doar în raport cu Agenția Coreeană pentru Internet și Securitate[57], CEPD ar saluta furnizarea de clarificări în ceea ce privește natura posibilelor interacțiuni dintre aceste entități și o monitorizare atentă a aplicării acestei dispoziții pe viitor pentru a asigura independența entităților însărcinate cu aplicarea normelor privind protecția datelor.

129. În ceea ce privește sancțiunile, sistemul coreean pare să combine diferite tipuri de sancțiuni, de la măsuri corective și amenzi administrative la sancțiuni penale, care sunt susceptibile de a avea un puternic efect de descurajare, iar autoritățile coreene au prezentat mai multe exemple de amenzi aplicate recent de CPICP, printre altele una de 6,7 miliarde woni coreeni, aplicată în decembrie 2020 unei societăți care a încălcat diferite dispoziții ale LPICP și o altă amendă de 103,3 milioane woni coreeni, la 28 aprilie 2021, aplicată unei societăți de tehnologie IA care a încălcat normele privind caracterul legal al prelucrării, în special în ceea ce privește consimțământul și prelucrarea de informații pseudonimizate.

130. Deși sumele menționate anterior pot avea un efect disuasiv, CEPD ar saluta furnizarea de informații suplimentare privind metoda folosită de CPICP pentru a calcula nivelul amenzilor administrative, de exemplu în ceea ce privește amenzile aplicate pentru nerespectarea unei măsuri corective aplicate în temeiul articolului 64 alineatul (1) din LPICP [vezi articolul 75 alineatul (2) punctul 13 din LPICP]. Acest aspect este relevant în special în ceea ce privește sancțiunile penale și aplicarea Legii penale (din Coreea).

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

131. În ceea ce privește măsurile reparatorii, sistemul coreean pare să ofere diferite modalități de asigurare a unei protecții adecvate și, în special, de aplicare a drepturilor individuale prin căi de atac administrative și judiciare eficace, inclusiv despăgubiri pentru prejudicii.

132. De asemenea, sistemul coreean oferă și mecanisme alternative la care persoanele pot apela pentru a obține reparații, pe lângă căile administrative și judiciare, după cum se explică la considerentele 132 și 133 din proiectul de decizie, legate de Centrul de asistență pentru confidențialitate și Comitetul de mediere a conflictelor. Întrucât acestea sunt căi de atac suplimentare, CEPD ar saluta furnizarea unor explicații mai detaliate privind modul în care ele completează posibilitățile de atac în fața CPICP și a instanțelor pentru persoanele vizate ale căror date cu caracter personal sunt transferate în Coreea în temeiul deciziei privind caracterul adecvat al nivelului de protecție.

[57] Vezi considerentul 117 din proiectul de decizie și articolul 62 din Decretul de punere în aplicare.

4. ACCESAREA ȘI UTILIZAREA DATELOR CU CARACTER PERSONAL TRANSFERATE DIN UNIUNEA EUROPEANĂ DE CĂTRE AUTORITĂȚILE PUBLICE DIN COREEA DE SUD

133. În ceea ce privește evaluarea nivelului de protecție a datelor în domeniul aplicării legii și al securității naționale, Comisia Europeană a furnizat informații cuprinzătoare în proiectul său de decizie și în anexele puse la dispoziție. Prin urmare, CEPD se abține de la a reproduce în prezentul aviz cea mai mare parte a constatărilor factuale și a evaluărilor.

134. Comisia Europeană ajunge la concluzia că, în domeniile menționate anterior, există un nivel de protecție a datelor care corespunde cerințelor prevăzute în jurisprudența CJUE și care, prin urmare, poate fi considerat echivalent în esență cu cel al Uniunii Europene.

135. Ca observație generală, CEPD ar dori să sublinieze faptul că, și în cazurile în care pare sau Comisia Europeană susține că este puțin probabil ca datele transferate din UE în Coreea de Sud să fie afectate de legislația coreeană relevantă, tot se recomandă evaluarea caracterului adecvat al nivelului de protecție a datelor din Coreea în raport cu astfel de cazuri. Relevanța lor este demonstrată și de faptul că însăși Comisia Europeană le-a abordat în proiectul de decizie.

4.1. Cadrul general privind protecția datelor în contextul accesului guvernului

136. În ceea ce privește accesul autorităților publice la datele cu caracter personal, trebuie analizate mai multe legi coreene pentru a evalua nivelul de protecție a dreptului la viață privată și la protecția datelor. În primul rând, CEPD constată că LPICP, ca lege principală privind protecția datelor, susține că are o aplicabilitate largă. Totuși, în timp ce LPICP se aplică pe deplin în domeniul aplicării legii, aplicarea sa în cazul prelucrării datelor în scopuri de securitate națională este limitată. În temeiul articolului 58 alineatul (1) punctul 2 din LPICP, capitolele III-VII nu se aplică în cazul prelucrării datelor cu caracter personal în scopuri de securitate națională. Totuși, capitolele I, II, IX și X se aplică în continuare în domeniul securității naționale. Astfel, principiile fundamentale ale LPICP, precum și garanțiile fundamentale pentru drepturile persoanelor vizate și dispozițiile privind supravegherea, aplicarea legii și căile de atac se aplică în cazul accesării și utilizării datelor cu caracter personal de către autoritățile naționale de securitate.

137. Și Constituția Coreei de Sud stabilește principii esențiale privind protecția datelor, și anume principiile legalității, necesității și proporționalității. Aceste principii sunt aplicabile și în cazul accesului autorităților publice sud-coreene la datele cu caracter personal în domeniul aplicării legii și al securității naționale[58].

138. În domeniul aplicării legii, poliția, procurorii, instanțele și alte organisme publice pot colecta date cu caracter personal în temeiul legislației specifice, și anume al Legii privind procedura penală (**„LPP”**), al Legii privind protecția confidențialității comunicațiilor (**„LPCC”**), al Legii privind activitatea de telecomunicații (**„LAT”**) și al Legii privind raportarea și utilizarea de informații specificate privind tranzacțiile financiare (**„LRUISTF”**), care se aplică în cazul urmăririi penale și al prevenirii spălării banilor și a finanțării terorismului. Aceste legi specifice stabilesc limitări, garanții și excepții suplimentare.

139. În domeniul securității naționale, în temeiul Legii privind Serviciul Național de Informații (**„LSNI”**) și al altor „legi privind securitatea națională”[59], Serviciul Național de Informații (**„SNI”**) poate colecta date

[58] Vezi considerentul 145 din proiectul de decizie.

[59] Legile privind securitatea națională includ, de exemplu, Legea privind protecția confidențialității comunicațiilor, Legea privind combaterea terorismului pentru protejarea cetățenilor și a securității publice sau Legea privind activitatea de telecomunicații.

cu caracter personal și poate intercepta comunicații. CEPD înțelege că, în exercitarea competențelor sale, SNI trebuie să respecte dispozițiile legale menționate anterior, precum și LPICP.

140. CEPD invită Comisia să clarifice dacă în Coreea există și alte autorități, pe lângă SNI, care sunt responsabile de domeniul securității naționale, întrucât, în secțiunea 6 din anexa I, Comisia Europeană dă impresia că SNI este un exemplu de agenție de securitate națională.

4.2. Măsuri de protecție și garanții pentru datele de confirmare a comunicațiilor în contextul accesului guvernului în vederea aplicării legii

141. În baza dreptului relevant, LPCC, autoritățile de aplicare a legii pot lua două tipuri de măsuri pentru a accesa informațiile privind comunicațiile. LPCC face distincția între măsuri de restricționare a comunicațiilor, care se referă atât la colectarea conținutului corespondenței obișnuite, cât și la interceptarea directă a conținutului telecomunicațiilor[60], și colectarea așa-numitelor date de confirmare a comunicațiilor. Acestea din urmă includ data telecomunicațiilor, ora începerii și a încheierii acestora, numărul apelurilor efectuate și primite, precum și codul de abonat al celeilalte părți, frecvența de utilizare, fișiere-jurnal privind utilizarea serviciilor de telecomunicații și informații privind localizarea[61].

142. CEPD constată că datele de confirmare a comunicațiilor par să nu beneficieze de aceleași garanții precum datele colectate prin intermediul măsurilor de restricționare a comunicațiilor, adică datele referitoare la conținut. Într-adevăr, CEPD observă că colectarea de conținut beneficiază de mai multe garanții decât colectarea de date de confirmare a comunicațiilor în scopul aplicării legii: în primul rând, spre deosebire de colectarea datelor referitoare la conținut, colectarea de date de confirmare a comunicațiilor nu se rezumă la investigarea anumitor infracțiuni grave, ci poate fi efectuată atunci când se consideră necesară efectuarea „oricărei investigații sau executarea oricărei pedepse” [articolul 13 alineatul (1) din LPCC]. În al doilea rând, colectarea de date de confirmare a comunicațiilor nu este structurată, în principiu, ca măsură de ultimă instanță ce trebuie folosită doar atunci când este dificil să se prevină altfel comiterea unei infracțiuni, să fie arestat infractorul sau să se colecteze dovezi[62]. Datele de confirmare a comunicațiilor pot fi colectate ori de câte ori un procuror sau un ofițer de poliție judiciară „consideră că este necesar” pentru investigarea unei infracțiuni sau pentru executarea unei pedepse. Totuși, există o excepție în acest sens pentru datele de urmărire în timp real și datele de confirmare a comunicațiilor referitoare la o anumită stație de bază, conform articolului 13 alineatul (2) din LPCC. În al treilea rând, agențiile de aplicare a legii care colectează conținutul comunicațiilor trebuie să înceteze imediat să facă acest lucru odată ce se consideră că nu mai este necesar accesul continuu[63]. În ceea ce privește datele de confirmare a comunicațiilor, acestea cel puțin nu sunt stipulate în mod explicit în LPCC sau în decretul de punere în aplicare a acesteia.

143. CEPD ia act de faptul că colectarea datelor de confirmare a comunicațiilor poate avea loc doar în baza unui mandat emis de o instanță. În plus, LPCC prevede furnizarea de informații detaliate atât în cererea de mandat, cât și în mandat[64]. O astfel de autorizare judiciară prealabilă servește la limitarea marjei de apreciere a autorităților competente în ceea ce privește aplicarea legii și la verificarea existenței, în fiecare caz, de motive suficiente pentru colectarea de date de confirmare a comunicațiilor. De asemenea, CEPD recunoaște că dreptul Republicii Coreea nu pare să prevadă păstrarea generală, fără discriminări, a datelor de confirmare a comunicațiilor. Astfel, accesul guvernului la astfel de date se

[60] Articolul 3 alineatul (2), articolul 2 alineatul (6), articolul 2 alineatul (7) din LPCC.
[61] Articolul 2 alineatul (11) din LPCC.
[62] Acesta este cazul datelor referitoare la conținut conform articolului 3 alineatul (2) și articolului 5 alineatul (1) din LPCC.
[63] Articolul 2 din Decretul de punere în aplicare a LPCC.
[64] Vezi considerentul 156 din proiectul de decizie.

referă întotdeauna la date care încă sunt păstrate pentru facturare și pentru prestarea serviciilor de comunicații.

144. Totuși, CEPD subliniază că CJUE a pus sub semnul întrebării faptul că datele privind traficul sunt mai puțin sensibile decât altele, și în special decât datele referitoare la conținut[65]. Ținând cont de faptul că în cazul datelor de confirmare a comunicațiilor se asigură un nivel de protecție inferior celui pentru datele referitoare la conținut din mai multe puncte de vedere, CEPD invită Comisia Europeană să monitorizeze îndeaproape dacă garanțiile prevăzute în dreptul coreean pentru această categorie de date cu caracter personal asigură un nivel de protecție echivalent în esență cu cel garantat în UE, în special în ceea ce privește caracterul proporțional și previzibil al legii.

4.3. Accesul autorităților publice coreene la informații privind comunicațiile, în scopuri de securitate națională

145. În ceea ce privește cadrul juridic pentru accesul autorităților de securitate națională la informații privind comunicațiile transferate din SEE în Coreea, CEPD a identificat două aspecte îngrijorătoare, ambele referitoare la regimul de acces la comunicații între cetățeni care nu sunt coreeni, care se încadrează într-o serie specifică de cazuri de utilizare (vezi punctul 29). În acele cazuri, în ceea ce privește atât datele de confirmare a comunicațiilor, cât și datele referitoare la conținut, nu sunt aplicabile anumite garanții disponibile în alte cazuri. Cu alte cuvinte, în aceste situații specifice, aceste date nu beneficiază de aceleași garanții precum datele comunicate atunci când în comunicare este implicat cel puțin un cetățean coreean.

4.3.1. Absența obligației de a informa persoanele privind accesul guvernului la comunicații între cetățeni străini

146. Într-un scenariu precum cel descris mai sus, adică atunci când niciuna dintre părțile la comunicare nu este cetățean coreean, autoritățile de securitate națională nu au obligația de a informa persoanele cu privire la colectarea și prelucrarea datelor acestora. CEPD recunoaște că această problemă afectează doar anumite situații. În primul rând, după cum s-a evidențiat deja, ori de câte ori într-o comunicare este implicat cel puțin un cetățean coreean, cerințele de notificare în temeiul LPCC se aplică tuturor părților la comunicare, indiferent de cetățenia acestora[66]. În al doilea rând, colectarea de date cu caracter personal ce rezultă din comunicații desfășurate exclusiv între cetățeni străini face obiectul unei serii specifice de cazuri de utilizare. În special, dreptul de acces în astfel de cazuri se extinde la comunicațiile efectuate de a) țări ostile Republicii Coreea, b) agenții, grupuri sau cetățeni străini, suspectați de implicare în activități anticoreene[67] sau c) membri ai unor grupuri care își desfășoară activitatea în Peninsula Coreea, dar, în fapt, în afara suveranității Republicii Coreea, și grupurile-umbrelă ale acestora, cu sediul în țări străine. Astfel, comunicațiile între cetățeni din UE, transferate

[65] Vezi hotărârea CJUE în cauza C-623/17, *Privacy International*, 6 octombrie 2020, ECLI:EU:C:2020:790, punctul 71: *„Ingerința pe care o implică transmiterea datelor de trafic și a datelor de localizare pentru agențiile de securitate și de informații în dreptul consacrat la articolul 7 din Cartă trebuie considerată ca fiind deosebit de gravă, ținând seama printre altele de caracterul sensibil al informațiilor pe care le pot furniza aceste date și în special de posibilitatea de a stabili profilul persoanelor în cauză pe baza acestora, o asemenea informație fiind la fel de sensibilă ca și conținutul însuși al comunicațiilor. În plus, aceasta este susceptibilă să genereze în mintea persoanelor vizate sentimentul că viața lor privată face obiectul unei supravegheri constante (vezi prin analogie Hotărârea din 8 aprilie 2014, Digital Rights Ireland și alții, C‑293/12 și C‑594/12, EU:C:2014:238, punctele 27 și 37, precum și Hotărârea din 21 decembrie 2016, Tele2, C‑203/15 și C‑698/15, EU:C:2016:970, punctele 99 și 100).”*

[66] Vezi considerentul 192 din proiectul de decizie.

[67] Vezi anexa II, nota de subsol nr. 244, potrivit căreia noțiunea de activități anticoreene se referă la activități care amenință existența și siguranța națiunii, ordinea democratică sau supraviețuirea și libertatea populației.

din SEE în Coreea, pot fi colectate doar în scopuri de securitate națională, dacă se încadrează în una dintre cele trei categorii menționate mai sus[68]. Ca factor suplimentar de limitare, CEPD a înțeles, din explicațiile suplimentare ale Comisiei Europene, că cadrul juridic aplicabil nu prevede interceptarea datelor aflate în tranzit în afara Coreei.

147. Așadar, criticalitatea lipsei unei cerințe privind notificarea ar putea fi considerată limitată, din punctul de vedere al impactului său practic. Totuși, CEPD subliniază importanța notificării (ulterioare) privind accesul guvernului, în special în ceea ce privește asigurarea unor căi de atac eficiente. Potrivit CJUE, notificarea este necesară *„pentru a permite persoanelor respective să își exercite drepturile rezultate din articolele 7 și 8 din Cartă de a solicita accesul la datele lor cu caracter personal care au facut obiectul acestor măsuri și, dacă este cazul, de a obține rectificarea sau ștergerea acestora, precum și să beneficieze, în conformitate cu articolul 47 primul paragraf din Cartă, de o cale de atac efectivă în fața unei instanțe judecătorești”*[69]*.* Deseori, accesul guvernului în scopuri de securitate națională include măsuri de supraveghere secretă, ceea ce înseamnă că obiectele supravegherii, persoanele vizate, nu știu că le sunt prelucrate datele. Astfel, *„persoana vizată are posibilități reduse de a apela la instanță, cu excepția cazului în care aceasta este informată despre măsurile luate fără știrea sa și, astfel, este în măsură să le conteste legalitatea retroactiv sau, ca alternativă, atunci când orice persoană care bănuiește că îi sunt ori i-au fost interceptate comunicațiile are posibilitatea de a sesiza instanțele, astfel încât competența acestora să nu depindă de notificarea subiectului interceptării că a avut loc o interceptare a comunicărilor sale”*[70]*.* În acest context și în acord cu cele menționate în prezentul document, CEPD și-a exprimat de numeroase ori îngrijorarea în ceea ce privește căile de atac eficiente în cazurile de supraveghere. CEPD subliniază că natura secretă a măsurilor guvernamentale nu trebuie să conducă la o situație în care astfel de măsuri, practic, nu pot fi contestate. În acest context, dacă lipsa unei cerințe privind notificarea în cazul comunicațiilor dintre cetățeni străini afectează sau nu nivelul de protecție a datelor, astfel cum este evaluat în proiectul de decizie, trebuie evaluată în cadrul unei evaluări generale, punând în special accentul pe mecanismele de supraveghere și de atac prevăzute în dreptul coreean (vezi secțiunile 4.7 și 4.8).

148. În plus, CEPD precizează, în acest context, că legea se referă la termeni destul de largi, precum activități anticoreene sau antinaționale[71], și că este greu de prevăzut în ce mod sunt interpretate aceste concepte în temeiul dreptului coreean. CEPD invită Comisia Europeană să monitorizeze modul în care sunt descriși acești termeni în dreptul coreean și dacă aplicarea lor în practică respectă cerințele de proporționalitate ce decurg din dreptul UE.

4.3.2. Absența unei autorizări independente prealabile pentru colectarea informațiilor referitoare la comunicațiile între cetățeni străini

149. Atunci când în Coreea urmează să fie prelucrate date cu caracter personal din SEE ce decurg din comunicații între cetățeni care nu sunt coreeni (și care se încadrează în unul dintre cazurile de utilizare menționate anterior), în scopuri de securitate națională, colectarea acestor date nu face obiectul unei autorizări prealabile de către un organism independent (așa cum se întâmplă în cazul comunicațiilor în care cel puțin una dintre persoanele vizate este cetățean coreean).[72]

[68] Vezi considerentul 187 din proiectul de decizie.

[69] CJUE, cauzele conexate C-511/18, C-512/18 și C-520/18, *La Quadrature du Net și alții*, 6 octombrie 2020, ECLI:EU:C:2020:791, punctul 190.

[70] CtEDO, *Big Brother Watch și alții/Regatul Unit*, 25 mai 2021, ECLI:CE:ECHR:2021:0525JUD005817013, punctul 337 și CtEDO, *Roman Zaharov/Rusia*, 4 decembrie 2015, ECLI:CE:ECHR:2015:1204JUD004714306, punctul 234.

[71] Comisia Europeană a explicat că, potrivit explicațiilor guvernului coreean, acești termeni se referă la „activități care amenință existența și siguranța națiunii, ordinea democratică sau supraviețuirea și libertatea persoanelor”; vezi și nota de subsol nr. 319 din proiectul de decizie privind caracterul adecvat al nivelului de protecție.

[72] Vezi considerentul 190 din proiectul de decizie.

150. Mai ales în lumina hotărârilor recente ale Curții Europene a Drepturilor Omului (**„CtEDO”**) „Big Brother Watch și alții/Regatul Unit” și „Centrum för Rättvisa/Suedia”, CEPD consideră că trebuie analizat dacă aceasta constituie o lacună critică a cadrului coreean privind protecția datelor. În acest sens, CEPD reamintește că, după cum s-a subliniat în recomandările sale actualizate referitoare la garanțiile europene esențiale pentru măsurile de supraveghere[73], articolul 6 alineatul (3) din Tratatul privind Uniunea Europeană stabilește că drepturile fundamentale prevăzute în Convenția europeană a drepturilor omului reprezintă principii generale ale dreptului Uniunii, în timp ce, după cum reamintește CJUE în jurisprudența sa, aceasta nu constituie, atât timp cât Uniunea Europeană nu a aderat la ea, un instrument juridic care să fi fost integrat în mod oficial în dreptul Uniunii[74]. Astfel, nivelul de protecție a drepturilor fundamentale prevăzut la articolul 45 din RGPD trebuie să fie determinat pe baza dispozițiilor acestui regulament, interpretate în lumina drepturilor fundamentale consacrate în Cartă. Acestea fiind spuse, potrivit articolului 52 alineatul (3) din Cartă, drepturile prevăzute în aceasta care corespund drepturilor garantate de Convenția europeană a drepturilor omului trebuie să aibă același sens și același domeniu de aplicare precum cele prevăzute în Convenție. Prin urmare, trebuie să se țină cont de jurisprudența CtEDO referitoare la drepturi care sunt prevăzute și în Cartă ca nivel minim de protecție pentru interpretarea drepturilor corespunzătoare din Cartă, adică în măsura în care Carta, astfel cum este interpretată de CJUE, nu asigură un nivel superior de protecție[75].

151. CEPD constată că, deși aprobarea prealabilă (independentă) a măsurilor de supraveghere este considerată o garanție importantă împotriva caracterului arbitrar, o astfel de aprobare nu poate decurge din jurisprudența CJUE ca o cerință absolută pentru proporționalitatea măsurilor de supraveghere. Totuși, CtEDO a stabilit acum, în mod explicit, obligativitatea unei autorizări ex ante independente pentru interceptarea în masă[76]. Deși proiectul de decizie nu prevede în mod explicit acest lucru, CEPD înțelege că cadrul juridic al Republicii Coreea nu prevede interceptarea în masă, ci doar interceptarea țintită a telecomunicațiilor[77]. Comisia Europeană a confirmat această interpretare.

152. Acestea fiind spuse, hotărârile CtEDO menționate mai sus, în linie cu jurisprudența CJUE[78] și cu jurisprudența anterioară a CtEDO[79], arată din nou importanța unei supravegheri cuprinzătoare din partea autorităților de supraveghere independente. CEPD subliniază că supravegherea independentă în toate fazele procesului de acces al guvernului în scopul aplicării legii și în scopuri de securitate națională este o garanție importantă împotriva măsurilor arbitrare de supraveghere și, astfel, pentru evaluarea unui nivel adecvat de protecție a datelor. Garanția independenței autorităților de supraveghere în sensul articolului 8 alineatul (3) din Cartă este menită să asigure o monitorizare eficace și fiabilă a conformării cu normele privind protecția persoanelor fizice în ceea ce privește

[73] Vezi Recomandările 02/2020 ale CEPD privind garanțiile esențiale europene pentru măsurile de supraveghere, punctele 10, 11.

[74] Vezi hotărârea CJUE în cauza C-311/18, *Data Protection Commissioner/Facebook Ireland Ltd. și Maximilian Schrems*, 16 iulie 2020, ECLI:EU:C:2020:559 (denumită în continuare „*Schrems II*”), punctul 98.

[75] Vezi CJUE, cauzele conexate C-511/18, C-512/18 și C-520/18, *La Quadrature du Net și alții*, 6 octombrie 2020, punctul 124.

[76] Vezi CtEDO, *Big Brother Watch și alții/Regatul Unit*, 25 mai 2021, ECLI:CE:ECHR:2021:0525JUD005817013, punctul 351: „Interceptarea în masă ar trebui să facă obiectul unei autorizări independente de la început”, „interceptarea în masă ar trebui să fie autorizată de un organism independent, adică de un organism independent față de puterea executivă”.

[77] Doar secțiunea 3.2 din anexa II conține o declarație explicită în scopuri de securitate națională, prevăzându-se că limitările și garanțiile *„asigură faptul că colectarea și prelucrarea informațiilor se limitează la ceea ce este strict necesar pentru a atinge un obiectiv legitim. Aceasta exclude orice colectare în masă, fără discriminări, a informațiilor cu caracter personal în scopuri de securitate națională”.*

[78] Vezi, de exemplu, cauzele conexate ale CJUE C-203/15 și C-698/15, *Tele2 Sverige AB și alții*, ECLI:EU:C:2016:970.

[79] Vezi, de exemplu, CtEDO, *Roman Zaharov/Rusia*, 4 decembrie 2015, ECLI:CE:ECHR:2015:1204JUD004714306.

prelucrarea datelor cu caracter personal. Acest lucru este valabil mai ales în circumstanțele în care, având în vedere natura supravegherii secrete, persoana este împiedicată să solicite reevaluarea sau să participe în mod direct la orice procedură de reevaluare anterioară sau concomitentă cu executarea măsurii de supraveghere.

153. Lipsa unei aprobări independente prealabile nu poate fi considerată ea însăși ca o lacună substanțială a dreptului coreean în ceea ce privește evaluarea unui nivel de protecție a datelor echivalent în esență. Evaluarea caracterului adecvat depinde, din nou, de toate circumstanțele cazului, în special de eficacitatea supravegherii ex post și a căilor de atac, astfel cum sunt prevăzute în cadrul juridic coreean (vezi secțiunile 4.7 și 4.8).

4.4. Dezvăluirile voluntare

154. Potrivit articolului 83 alineatul (3) din LAT, furnizorii de servicii de telecomunicații pot preda în mod voluntar autorităților de securitate națională și de aplicare a legii, la cerere, așa-numitele „date privind abonații”[80]. Deși CEPD constată că, cel mai probabil, situațiile în care sunt implicate date cu caracter personal care au fost transferate din SEE în Coreea sunt rare, acestea tot trebuie analizate pentru a se evalua nivelul de protecție a datelor, astfel cum s-a menționat deja mai sus.

155. CEPD înțelege că, în aceste cazuri, se aplică garanțiile de protecție a datelor prevăzute în LPICP, iar autoritățile publice, precum și furnizorii de telecomunicații trebuie să respecte aceste cerințe[81] și că ambele părți pot fi trase la răspundere pentru orice încălcare a drepturilor și libertăților persoanelor vizate[82]. În plus, CEPD înțelege că furnizorii de telecomunicații nu sunt obligați să dea curs unor astfel de solicitări.

156. Totuși, în ceea ce privește conceptul de acces al autorităților naționale la datele privind abonații, în vederea aplicării legii, precum și, în special, în scopuri de securitate națională, prin „divulgarea voluntară” de către operatorii din domeniul telecomunicațiilor, există o îngrijorare în ceea ce privește riscul sporit pentru drepturile și libertățile persoanelor vizate, în special în ceea ce privește dreptul la informare al acestora.

157. Potrivit articolului 58 alineatul (1) punctul 2 din LPICP, dispozițiile de la capitolele III-VII nu se aplică informațiilor cu caracter personal a căror furnizare se solicită în temeiul securității naționale. În acest sens, de exemplu, dispozițiile articolului 18 (Limitarea utilizării și a furnizării de informații cu caracter personal în afara scopurilor prevăzute) și articolului 20 (Notificarea cu privire la sursele etc. informațiilor cu caracter personal colectate de la terți) din LPICP nu se aplică în cazul unor astfel de solicitări. Atunci când este formulată o solicitare de o autoritate de securitate națională, aceasta ridică, pe de o parte, problema dacă articolul 58 alineatul (1) punctul 2 exclude aplicarea LPICP și în cazul furnizorilor de telecomunicații. Pe de altă parte, se pune problema dacă excluderea aplicării articolului 20 din LPICP în astfel de situații se aplică și în cazul dispoziției corespunzătoare de la secțiunea 3 din anexa I [Notificarea pentru date în cazul în care datele cu caracter personal nu au fost obținute de la persoana vizată (articolul 20 din lege]. Dacă s-ar întâmpla acest lucru, iar articolul 58 alineatul (1) punctul 2 s-ar aplica și în cazul furnizorilor de telecomunicații, ar exista riscul, potrivit informațiilor disponibile, să nu existe nicio obligație legală de a informa persoanele vizate cu privire la divulgarea voluntară.

[80] Seturile de date vizate ar fi: numele, codul de înregistrare al rezidenților, adresa și numărul de telefon al utilizatorilor, datele la care utilizatorii se abonează sau își încheie abonamentul, precum și codurile de identificare ale utilizatorilor (folosite pentru a identifica utilizatorul de drept al sistemelor informatice sau al rețelelor de comunicații).
[81] Vezi considerentele 164 și 194 din proiectul de decizie.
[82] Vezi considerentul 166 din proiectul de decizie.

158. Prin urmare, CEPD este preocupat că cerințele privind informațiile ar putea să devină neaplicabile, iar persoanelor vizate le-ar fi mult mai dificil să își afirme drepturile în materie de protecție a datelor, în special în ceea ce privește căile de atac. În acest sens, CEPD invită Comisia Europeană să clarifice sfera de aplicare a dispozițiilor relevante.

4.5. Utilizarea ulterioară a informațiilor

159. Principiul limitării scopurilor este o cerință legală esențială în ceea ce privește protecția datelor. Potrivit acestui principiu, datele cu caracter personal se colectează doar în scopuri specificate, explicite și legitime și nu trebuie să fie prelucrate ulterior într-o manieră incompatibilă cu aceste scopuri. În plus, conform dreptului Uniunii, autoritățile publice pot prelucra date cu caracter personal pentru prevenirea, investigarea sau urmărirea penală a infracțiunilor chiar dacă datele respective au fost obținute inițial în alte scopuri, dacă autoritățile respective au un temei juridic pentru prelucrarea acestor date în temeiul legilor relevante și dacă prelucrarea ulterioară nu este disproporționată.[83]

160. În consecință, CEPD constată că cadrul coreean privind protecția datelor prevede garanții și limitări similare celor prevăzute în dreptul Uniunii în ceea ce privește utilizarea ulterioară a informațiilor colectate pentru aplicării legii și în scopuri de securitate națională, de exemplu principiul limitării scopurilor prevăzut la articolul 3 alineatele (1)-(2) din LPICP.

4.6. Transferurile ulterioare și partajarea de informații

161. Articolul 44 din RGPD prevede că transferurile și transferurile ulterioare de date cu caracter personal au loc doar dacă nu este subminat nivelul de protecție garantat prin RGPD. Astfel, nivelul de protecție acordat datelor cu caracter personal transferate din SEE în Coreea nu trebuie să fie subminat de transferul ulterior către destinatari dintr-o țară terță, adică transferurile ulterioare ar trebui să fie permise doar atunci când se asigură un nivel continuu de protecție, echivalent în esență cu cel prevăzut conform dreptului Uniunii. Prin urmare, atunci când se evaluează dacă o țară terță asigură un nivel adecvat de protecție a datelor, trebuie luat în considerare cadrul juridic al țării respective privind transferurile ulterioare. Acest lucru este incontestabil și în conformitate cu opinia Comisiei Europene[84] și a CEPD.

162. În acest context, CEPD ia act de faptul că, în hotărârile sale recente „Big Brother Watch și alții/Regatul Unit" și „Centrum för Rättvisa/Suedia", CtEDO a furnizat orientări[85] privind precauțiile în materie de protecție a datelor care trebuie respectate în statele contractante atunci când se comunică date cu caracter personal către alte părți în vederea aplicării legii și în scopuri de securitate națională, în cazurile de colectare în masă: *„În primul rând, circumstanțele în care poate avea loc un astfel de transfer trebuie să fie prevăzute în mod clar în dreptul național. În al doilea rând, statul care transferă informațiile trebuie să se asigure că statul care le primește, atunci când gestionează datele, are instituite garanții capabile să prevină abuzurile și ingerințele disproporționate. În special, statul care primește informațiile trebuie să garanteze stocarea în siguranță a materialelor și să restricționeze divulgarea lor ulterioară. (...) În al treilea rând, vor fi necesare garanții îmbunătățite atunci când este*

[83] Vezi articolul 4 alineatul (2) din Directiva privind protecția datelor în materie de aplicare a legii.
[84] Vezi considerentul 84 și următoarele din proiectul de decizie.
[85] Următoarele elemente au fost stabilite cu ocazia cauzelor *Big Brother Watch* și *Centrum för Rättvisa*, care se referă la regimurile de interceptare în masă. Cerința privind măsurile de precauție care trebuie adoptate atunci când se comunică materiale altor părți era deja inclusă în criteriile elaborate de CEDO în contextul interceptării țintite și nu fusese detaliată mai mult de CtEDO (vezi *Big Brother Watch și alții/Regatul Unit*, punctele 335, 362).

clar că sunt transferate materiale care necesită o confidențialitate specială – cum ar fi materialele jurnalistice confidențiale."[86]

163. În aplicarea acestor standarde, CtEDO a constatat, în cauza „Centrum för Rättvisa/Suedia", că absența oricăror cerințe legale explicite în regimul de interceptare pentru a evalua necesitatea și proporționalitatea partajării de informații pentru impactul posibil al acestora asupra dreptului la viață privată constituie o încălcare a articolului 8 din Convenția europeană a drepturilor omului. CtEDO a criticat faptul că, urmare a nivelului de generalitate a legii, materialele interceptate ar putea fi trimise în general în străinătate oricând se consideră că acest lucru este în interesul național, indiferent dacă destinatarul străin oferă un nivel minim acceptabil de garanții[87].

164. Recunoscând faptul că cadrul juridic al Coreei de Sud nu permite interceptarea în masă, tot în lumina implicațiilor jurisprudenței CtEDO astfel cum este evidențiat mai sus, CEPD consideră că, pe lângă cerințele ce decurg din dreptul Uniunii astfel cum sunt interpretate de CJUE, ar trebui avute în vedere argumentele CtEDO pentru a evalua în ce măsură cadrul juridic pentru transferurile ulterioare către o țară terță asigură standarde adecvate de protecție a datelor.

4.6.1. Cadrul juridic aplicabil pentru transferurile ulterioare de către autoritățile de aplicare a legii

165. În ceea ce privește transferurile ulterioare efectuate de autoritățile competente în scopul aplicării legii, CEPD înțelege din explicațiile Comisiei Europene că se aplică secțiunea 2 din anexa I la proiectul de decizie în ceea ce privește limitarea transferurilor ulterioare, inclusiv atunci când transferul are loc pe baza altei legi decât LPICP. Potrivit acestei norme, *„dacă se furnizează informații cu caracter personal unei terțe părți din străinătate, este posibil ca pentru aceste informații să nu se asigure nivelul de protecție garantat prin Legea privind protecția informațiilor cu caracter personal din Coreea, ca urmare a diferențelor dintre sistemele de protecție a informațiilor cu caracter personal din diferite țări. Prin urmare, se va considera că aceste cazuri sunt «cazuri în care se pot cauza dezavantaje persoanei vizate», astfel cum se menționează la articolul 17 punctul 4 din lege sau «cazuri în care interesul unei persoane vizate sau al unui terț este încălcat în mod neechitabil», astfel cum se menționează la articolul 18 punctul 2 din lege și la articolul 14 alineatul (2) din Decretul de punere în aplicare a aceleiași legi. Pentru a îndeplini cerințele acestor dispoziții, operatorul de informații cu caracter personal și partea terță trebuie, prin urmare, să asigure în mod explicit un nivel de protecție echivalent cu cel prevăzut de lege, inclusiv garantarea exercitării drepturilor persoanei vizate în documente cu caracter obligatoriu din punct de vedere juridic, precum contracte, chiar și după transferul în străinătate al informațiilor cu caracter personal"*[88].

166. CEPD salută această dispoziție care, plecând de la premisa că nivelul de protecție a datelor în Coreea este adecvat în acest scop, asigură continuitatea unui nivel de protecție echivalent cu cel acordat în esență de dreptul Uniunii pentru transferurile ulterioare. Comisia a confirmat că interpretarea CEPD este corectă, și anume că această secțiune din anexa I se aplică în cazul tuturor transferurilor ulterioare de către autoritățile competente în scopul aplicării legii. Totuși, CEPD subliniază că trebuie să se asigure faptul că acest regulament oferă un nivel continuu de protecție în practică, întrucât pot exista incertitudini în ceea ce privește garanțiile și obligațiile contractuale sau alte mecanisme similare care pot fi folosite pentru a atinge un astfel de nivel de protecție în cazul prelucrării în scopul aplicării legii. În acest sens, ar trebui să se precizeze în plus, de exemplu, că datele cu caracter personal pot fi partajate doar cu autoritățile competente relevante din țara terță.

[86] CtEDO, *Big Brother Watch și alții/Regatul Unit*, 25 mai 2021, ECLI:CE:ECHR:2021:0525JUD005817013, punctul 362.
[87] Vezi CtEDO, *Centrum för Rättvisa/Suedia*, 25 mai 2021, ECLI:CE:ECHR:2021:0525JUD005817013, punctul 326.
[88] Proiectul de decizie, anexa I, p. 7.

167. Sub rezerva clarificării solicitate mai sus, dacă UIFC intră sub incidența proiectului de decizie, CEPD constată că declarațiile oficiale privind accesul guvernului[89] explică faptul că, potrivit articolului 8 alineatul (1) din LRUISTF, comisarul UIFC poate furniza serviciilor străine de informații financiare anumite informații privind tranzacțiile financiare, în cazul în care consideră că acest lucru este necesar pentru a atinge obiectivele LRUISTF[90]. Articolul 8 din LRUISTF în sine nu prevede o obligație de a stabili dacă și de a garanta că țara străină oferă garanții adecvate privind protecția datelor. Anexa II nu face referire la noua secțiune din anexa I în acest sens. Prin urmare, CEPD invită Comisia Europeană să clarifice interdependența dintre secțiunea relevantă din anexa I cu privire la limitarea transferurilor ulterioare și temeiul juridic pentru transferurile ulterioare potrivit LRUISTF.

4.6.2. Cadrul juridic aplicabil pentru transferurile ulterioare în scopuri de securitate națională

168. Proiectul de decizie nu conține informații privind cadrul juridic pentru transferurile ulterioare în domeniul securității naționale. În acest scop, CEPD înțelege că, spre deosebire de scopurile de aplicare a legii, secțiunea 2 din anexa I nu se aplică în cazul transferurilor ulterioare în scopuri de securitate națională. Articolele 17 și 18 din LPICP care fac obiectul secțiunii în cauză din anexa I fac parte din capitolul III din LPICP care, la rândul său, nu se aplică în cazul prelucrării datelor cu caracter personal în scopuri de securitate națională [articolul 58 alineatul (1) din LPICP].

169. Totuși, CEPD presupune că Coreea ar putea fi nevoită să transmită și transmite date cu caracter personal serviciilor străine de informații în scopuri de securitate națională, de exemplu pentru a coopera în ceea ce privește combaterea amenințărilor transfrontaliere la adresa securității naționale, pentru a avertiza guvernele străine în acest sens sau pentru a le solicita ajutorul în identificarea unor astfel de amenințări.

170. CEPD a înțeles că, în opinia Comisiei Europene, transferurile ulterioare sunt reglementate suficient în dreptul coreean prin garanțiile ce rezultă din cadrul constituțional de ansamblu, în special prin principiile necesității și proporționalității, precum și prin principiile fundamentale în domeniul protecției datelor reglementate în LPICP, precum legalitatea și echitatea prelucrării, limitarea scopurilor, reducerea la minimum a datelor, securitatea și obligațiile generale de prevenire a abuzurilor și a utilizării necorespunzătoare a informațiilor cu caracter personal.

171. CEPD recunoaște și confirmă aplicabilitatea generală a acestor principii esențiale (privind protecția datelor), însă este îngrijorat de faptul că aceste garanții au un caracter foarte general și nu se referă în mod explicit sau nu abordează, într-un temei legal, circumstanțele și condițiile specifice pentru transferurile ulterioare de date transferate din SEE în scopuri de securitate națională și nici nu abordează problema acestora într-un temei juridic. Deși aceste principii generale și cuprinzătoare sunt aplicabile pe scară largă, CEPD se întreabă dacă s-ar putea considera că acestea îndeplinesc criteriile de norme clare și precise și că asigură garanții suficiente, eficace și aplicabile. Mai ales atunci când accesarea și prelucrarea datelor cu caracter personal de către guvern se exercită în secret, iar concluziile care ar putea fi formulate pe baza datelor sunt deosebit de grave, este esențial să existe norme clare și detaliate. Legea ar trebui să indice sfera de aplicare a oricărei marje conferite autorităților competente și maniera de exercitare a acestora, într-un mod suficient de clar, pentru a acorda o protecție adecvată persoanelor vizate. În hotărârea în cauza *Schrems II*, CJUE reamintește că, pentru a îndeplini cerințele principiilor necesității și proporționalității, un temei juridic care permite

[89] Vezi anexa II la proiectul de decizie.

[90] Vezi anexa II la proiectul de decizie, secțiunea 2.2.3.2. În timp ce un astfel de schimb poate avea loc doar cu condiția ca serviciul străin să nu folosească informațiile în alt scop decât în scopul inițial al divulgării și în special nu pentru o anchetă penală sau pentru un proces [articolul 8 alineatul (2) din LRUISTF], comisarul UIFC poate, la primirea unei solicitări din partea unei țări străine, să fie de acord cu utilizarea acestor date pentru desfășurarea unor anchete penale sau procese pentru infracțiuni, cu consimțământul prealabil al Ministerului Justiției [articolul 8 alineatul (3) din LRUISTF].

ingerința în drepturile fundamentale trebuie să definească el însuși sfera de aplicare a limitării exercitării dreptului în cauză, să prevadă norme clare și precise privind obiectul și aplicarea măsurii în cauză și să impună garanții minime[91]. Prin urmare, CEPD este îngrijorat de faptul că nu este suficient ca astfel de garanții să fie prevăzute în general în legislația de nivel superior fără ca noțiunea, de exemplu, de proporționalitate să fie pusă în aplicare în mod explicit chiar în temeiul juridic respectiv.

172. Aceste preocupări sunt sprijinite de decizia CtEDO menționată mai sus, în care instanța a considerat că o normă generală, fără vreo cerință explicită de evaluare a necesității și proporționalității sau de luare în considerare a preocupărilor legate de viața privată nu este compatibilă cu dreptul la viață privată în temeiul articolului 8 din Convenția europeană a drepturilor omului. În acest sens, CEPD constată că, în dreptul aplicabil în cauză (precum și în dreptul Coreei), există principii cuprinzătoare (garantate prin Constituție) privind necesitatea și proporționalitatea, de exemplu potrivit Cartei și prin aderarea la Convenția europeană a drepturilor omului.

173. CEPD invită Comisia Europeană să clarifice temeiul juridic, cum, în ce măsură și în ce condiții specifice agențiile serviciilor de informații au obligația de a lua în considerare preocupările legate de viața privată și garanțiile privind protecția datelor înainte de a divulga date cu caracter personal partenerilor străini, în scopuri de securitate națională. Dacă o astfel de obligație rezultă direct din principii constituționale, Comisia Europeană ar trebui să evalueze mai detaliat cerințele privind precizia și claritatea legislației relevante și să confirme că principiile constituționale generale și principiile privind protecția datelor sunt aplicate și puse în aplicare în mod corespunzător.

4.6.3. Acorduri internaționale

174. CEPD constată că Comisia Europeană nu a luat în considerare, în evaluarea sa privind caracterul adecvat al nivelului de protecție, existența acordurilor internaționale încheiate între Coreea și țări terțe sau organizații internaționale, care pot prevedea dispoziții specifice pentru transferul internațional de date cu caracter personal de către serviciile de aplicare a legii și/sau de informații către țări terțe. CEPD consideră că încheierea de acorduri bilaterale sau multilaterale cu țări terțe în scopul aplicării legii sau al cooperării în materie de informații poate afecta cadrul juridic privind protecția datelor din Coreea, astfel cum a fost evaluat.

175. Prin urmare, CEPD invită Comisia Europeană să clarifice dacă există astfel de acorduri, în ce condiții pot fi ele încheiate și să evalueze dacă dispozițiile acordurilor internaționale pot afecta nivelul de protecție acordat datelor cu caracter personal transferate din SEE în Coreea prin cadrul juridic și practicile asociate divulgărilor în străinătate, în scopuri de aplicare a legii și de securitate națională.

4.7. Supravegherea

176. CEPD constată că supravegherea punerii în aplicare a dreptului penal, precum și a autorităților naționale responsabile pentru securitate se asigură de mai multe organisme interne și externe diferite.

177. În acest context, trebuie remarcat că CJUE a subliniat în mod repetat necesitatea unei supravegheri independente, ca o componentă esențială a protecției persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal ale acestora. Conceptul de independență include autonomia constituțională, libertatea față de instrucțiuni și independența materială. Pentru a asigura o monitorizare și aplicare consecventă a dreptului privind protecția datelor, autoritățile de supraveghere trebuie să aibă puteri efective, inclusiv competențe corective și de remediere.

178. CEPD este de acord cu concluzia Comisiei Europene potrivit căreia, într-o evaluare de ansamblu, se poate considera că Republica Coreea are un sistem de supraveghere independent și eficace, deși mai multe organisme ale sistemului de supraveghere nu îndeplinesc ele însele cerințele de mai sus. De

[91] Vezi hotărârea în cauza *Schrems II*, punctele 175 și 180.

exemplu, majoritatea dintre acestea, precum Comisia Națională pentru Drepturile Omului sau Comitetul pentru Audituri și Inspecții, nu au competențe de executare, ci doar pot emite recomandări. În plus, majoritatea organismelor publice în cauză nu sunt exclusiv instituții pentru protecția datelor, ci au, de regulă, alte sarcini în domeniul protecției drepturilor fundamentale.

179. Totuși, potrivit explicațiilor Comisiei Europene, CEPD constată că supravegherea autorităților de aplicare a legii este garantată de CPICP în mod cuprinzător și fără excepție. Prin urmare, CPICP deține competențe de investigare, de remediere și de aplicare în temeiul LPICP și al altor legi privind protecția datelor (precum LPPC), care se aplică întregului domeniu al accesului autorităților de aplicare a legii și de securitate națională la datele cu caracter personal.

180. În acest context, CEPD ar dori să sublinieze din nou că, pentru a-și exercita sarcinile și competențele, autoritățile de supraveghere trebuie să fie dotate cu resurse umane, tehnice și financiare suficiente. În acest sens, din păcate, există o lipsă de informații privind organismele de supraveghere desemnate, în special privind CPICP. Prin urmare, CEPD reiterează solicitarea adresată Comisiei Europene de a furniza informații suplimentare în această privință.

181. Per ansamblu, CEPD ar dori să constate că în proiectul de decizie aproape că nu există declarații, exemple sau cifre privind activitățile de supraveghere sau privind punerea în aplicare a dreptului privind protecția datelor de către organismele de supraveghere din domeniul aplicării legii și al securității naționale. Acest lucru ar fi util în contextul evaluării eficacității organismelor de supraveghere.

4.8. Căi de atac și măsuri reparatorii

182. CEPD reamintește că, pentru un nivel adecvat de protecție a datelor, este esențial ca persoanelor vizate să li se pună la dispoziție căi de atac și măsuri reparatorii cuprinzătoare împotriva accesării sau prelucrării neautorizate a datelor. Aceste căi de atac trebuie să fie suficiente pentru a-i permite persoanei vizate să obțină acces la datele stocate cu privire la persoana sa și să solicite corectarea sau ștergerea acestora.

183. Având în vedere hotărârile pronunțate de CJUE în cauzele *Schrems I* și *Schrems II*, este clar că, pe lângă dreptul de a apela la autoritățile competente, o protecție judiciară eficace în sensul articolului 47 alineatul (1) din Cartă este de o importanță fundamentală pentru prezumarea caracterului adecvat al legislației unei țări terțe.

184. CEPD recunoaște că Coreea a stabilit diferite căi pentru exercitarea drepturilor de acces, păstrare, ștergere și suspendare ale persoanelor, în temeiul LPICP. Aceste drepturi pot fi exercitate în raport cu operatorul sau printr-o plângere introdusă la CPICP sau la alte organisme de supraveghere, precum Comisia Națională pentru Drepturile Omului. În plus, CEPD recunoaște posibilitatea de a contesta hotărârea operatorilor sau a autorităților publice, ca răspuns la solicitarea acestora pe baza Legii privind litigiile administrative.

185. În plus, CEPD înțelege din explicațiile furnizate de Comisia Europeană că persoanele fizice pot contesta acțiunile autorităților de aplicare a legii și de securitate națională în fața instanțelor competente, în temeiul Legii privind litigiile administrative și al Legii privind Curtea Constituțională, și pot obține despăgubiri pentru prejudiciile suferite, în temeiul Legii privind despăgubirile acordate de stat[92].

186. Totuși, în acest context, CEPD este îngrijorat în ceea ce privește măsurile reparatorii eficace pentru cetățenii din UE în cazurile de securitate națională în care nu este implicat niciun cetățean coreean. După cum se precizează la punctul 33 și următoarele, autoritățile de securitate națională nu au obligația de a informa persoanele vizate cu privire la colectarea și prelucrarea datelor lor cu caracter personal. Întrucât este mult mai greu să se obțină o protecție juridică eficace în aceste cazuri, CEPD ar

[92] Vezi secțiunea 3.2.4 din anexa II coroborată cu secțiunea 2.4.3.

dori să sublinieze că anumite garanții juridice sunt necesare dacă sunt implicate date transferate din SEE. Aceste garanții trebuie să le permită persoanelor vizate să ia măsuri eficace împotriva prelucrării ilegale a datelor într-o manieră sigură din punct de vedere juridic, fără ca aceste demersuri să fie îngreunate de cerințe procedurale excesiv de stricte, de exemplu prin impunerea unei sarcini a probei pe care nu o pot îndeplini fără a avea cunoștință de efectuarea prelucrării. În plus, persoanele trebuie să poată apela la un organism competent, care îndeplinește cerințele de la articolul 47 din Carta drepturilor fundamentale a Uniunii Europene, adică are competența de a stabili faptul că are loc o prelucrare a datelor și de a verifica legalitatea prelucrării, și care să aibă competențe de remediere executorii în cazul în care prelucrarea datelor este ilegală. În acest context, doar dreptul de a introduce o plângere la CNDR, de exemplu, nu ar fi suficient. Prin urmare, CEPD invită Comisia să explice mai în detaliu cum sunt puse în aplicare aceste cerințe în condiții procedurale și de fond, de exemplu, dacă este posibil pentru persoanele vizate să apeleze la CPICP, precum și la o instanță fără a fi nevoite să demonstreze respectiva prelucrare a datelor.

187. În plus, CEPD observă că proiectul de decizie prevede un mecanism de transferare a plângerilor, adică persoanele din UE pot transmite o plângere către CPICP prin intermediul autorității lor naționale de protecție a datelor sau prin intermediul CEPD. Apoi, CPICP va informa persoana prin același canal, odată încheiată investigația[93]. CEPD salută efortul de a facilita accesul la căile de atac împotriva autorităților coreene de securitate națională. Totodată, CEPD susține ideea ca un astfel de mecanism de transferare să fie canalizat mai degrabă prin autoritățile naționale europene pentru protecția datelor decât prin CEPD, întrucât acestea sunt competente și mai apropiate de tratarea plângerilor individuale.

188. În plus, CEPD constată o posibilă contradicție în ceea ce privește divulgarea voluntară. Pe de o parte, proiectul de decizie prevede că persoanele fizice pot obține reparații în cazul în care datele lor sunt divulgate în mod ilegal, în baza unei cereri de divulgare voluntară, inclusiv împotriva autorității de aplicare a legii care a emis solicitarea[94]. Pe de altă parte, proiectul de decizie face referire la cerința privind impactul direct în ceea ce privește dreptul persoanei de a contesta acțiunile autorităților publice, menționând (doar) solicitările privind divulgarea obligatorie ca exemplu de situație în care se consideră că acțiunile administrative afectează direct dreptul la viață privată[95]. Din explicațiile Comisiei Europene, CEPD înțelege că, de fapt, nu există nicio restricție asupra posibilităților de atac împotriva solicitărilor de divulgare voluntară și, prin urmare, invită Comisia Europeană să clarifice mai detaliat aceste aspecte în decizie, atât în ceea ce privește aplicarea legii, cât și în ceea ce privește securitatea națională (spre deosebire de secțiunea privind aplicarea legii, secțiunea privind divulgarea voluntară în scopuri de securitate națională nu conține nicio afirmație explicită privind reparațiile în acest context).

[93] Vezi considerentul 205 și anexa I, p. 19 din proiectul de decizie.
[94] Vezi considerentul 166 din proiectul de decizie.
[95] Vezi considerentul 181 (aplicării legii) și considerentele 208 și 181 (securitatea națională) din proiectul de decizie.