



Avizul 28/2025 referitor la proiectul de decizie de punere în aplicare a Comisiei Europene în temeiul Regulamentului (UE) 2016/679 privind protecția adekvată a datelor cu caracter personal de către Brazilia

Versiunea 1.0

Adoptat la 04 November 2025

Rezumat

La 5 septembrie 2025, Comisia Europeană a început procesul în vederea adoptării proiectului său de decizie de punere în aplicare (denumit în continuare „proiectul de decizie”) privind protecția adecvată a datelor cu caracter personal de către Republica Federativă a Braziliei (denumită în continuare „Brazilia”).

La 5 septembrie 2025, Comisia Europeană a solicitat avizul Comitetului European pentru Protecția Datelor (CEPD). Evaluarea CEPD cu privire la caracterul adecvat al nivelului de protecție oferit de Brazilia s-a bazat pe examinarea proiectului de decizie în sine, precum și pe analiza documentației disponibile public pe site-urile oficiale ale autorităților braziliene.

CEPD s-a axat atât pe evaluarea aspectelor generale privind RGPD din proiectul de decizie, cât și a accesului autorităților publice la datele cu caracter personal transferate din SEE în scopul asigurării respectării legii și al securității naționale, inclusiv a căilor de atac aflate la dispoziția persoanelor fizice în SEE. De asemenea, CEPD a evaluat dacă garanțiile prevăzute în cadrul juridic din Brazilia sunt în vigoare și eficace.

CEPD a utilizat ca referință principală pentru această activitate criteriile de referință privind caracterul adecvat al nivelului de protecție adoptate la 28 noiembrie 2017 de Grupul de lucru „Articolul 29”², astfel cum au fost revizuite ultima dată și adoptate la 6 februarie 2018 de CEPD („Criteriile de referință privind caracterul adecvat al nivelului de protecție”) și Recomandările CEPD 02/2020 privind garanțiile esențiale europene pentru măsurile de supraveghere.

CEPD ia act cu satisfacție de faptul că cadrul de protecție a datelor, în special Legea generală privind protecția datelor din Brazilia („LGPD”), împreună cu decretele prezidențiale și reglementările cu caracter obligatoriu emise de Autoritatea pentru Protecția Datelor din Brazilia (*Agencia Nacional de Proteção de Dados* – „ANPD”), stabilesc cerințe (inclusiv în ceea ce privește principiile, drepturile persoanelor vizate, transferurile, supravegherea și căile de atac) care sunt strâns aliniate la RGPD și la jurisprudența Curții de Justiție a Uniunii Europene („CJUE”).

De asemenea, CEPD a concluzionat că Comisia Europeană ar trebui să clarifice în proiectul de decizie anumite aspecte ale cadrului juridic al Braziliei și să monitorizeze atent evoluțiile acestuia.

În ceea ce privește principiul responsabilității și cerințele pentru evaluarea impactului asupra protecției datelor, CEPD consideră că este important ca aceasta să fie efectuată în cazurile în care prelucrarea ar putea genera un risc ridicat pentru drepturile și libertățile persoanelor fizice și ca EIPD să acopere evaluarea necesității și a proporționalității

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

² Grupul de lucru „Articolul 29”, WP 254 rev.01, adoptat la 28 noiembrie 2017 și revizuit ultima dată și adoptat la 6 februarie 2018, aprobat de CEPD.

prelucrării. Prin urmare, CEPD invită Comisia Europeană să monitorizeze punerea în aplicare practică a acestor cerințe.

LGPD prevede o limitare a furnizării de informații către persoanele vizate sau către autoritatea de supraveghere în baza principiului „secretului comercial și industrial” în anumite cazuri. Ținând seama de importanța cerințelor de transparență pentru posibilitatea persoanelor vizate de a controla modul în care sunt prelucrate datele lor, precum și de importanța obligațiilor de a coopera cu autoritatea de supraveghere, în special de a furniza informațiile necesare pentru sarcinile sale de supraveghere, CEPD invită Comisia Europeană să monitorizeze punerea în aplicare a acestor limitări în practică pentru a înțelege mai bine impactul acestora asupra drepturilor la informare și acces, precum și asupra competențelor ANPD, dacă este cazul.

În ceea ce privește normele privind transferurile ulterioare, CEPD invită Comisia Europeană să clarifice în proiectul de decizie dacă transferurile pot fi efectuate în conformitate cu condiții echivalente cu articolul 49 din RGPD numai în circumstanțele excepționale în care nu pot fi utilizate alte instrumente de transfer. De asemenea, Comisia este invitată să clarifice dacă persoanele vizate sunt informate cu privire la: riscurile posibile ale transferului atunci când acesta se bazează pe consimțământul lor și pe circumstanțele transferului (durata și scopul transferului, țările de destinație, responsabilitățile părților implicate, drepturile persoanelor vizate și mijloacele de exercitare a acestora), indiferent de instrumentul de transfer utilizat.

În plus, CEPD invită Comisia Europeană să ofere mai multe detalii în legătură cu sarcinile Consiliului național pentru protecția datelor cu caracter personal și a vieții private și interacțiunea acestuia cu ANPD.

În ceea ce privește accesul și utilizarea de către autoritățile publice braziliene a datelor cu caracter personal transferate operatorilor și persoanelor împuternicite de operatori din Brazilia în scopuri de asigurare a respectării dreptului penal și de securitate națională („accesul guvernului”), CEPD constată că LGPD nu se aplică prelucrării datelor efectuate în scopuri *exclusive* de siguranță publică, apărare națională, securitate a statului sau anchetare și urmărire penală a infracțiunilor. În același timp, CEPD ia act cu satisfacție de faptul că Curtea Supremă Federală a Braziliei a interpretat LGPD în jurisprudența sa într-un mod care a extins aplicabilitatea sa parțială la prelucrarea datelor cu caracter personal pentru anchetele penale și menținerea ordinii publice.

Având în vedere cele de mai sus, CEPD invită Comisia să evalueze și să clarifice în proiectul de decizie aplicabilitatea LGPD în cazul prelucrării datelor cu caracter personal în scopul asigurării respectării dreptului penal, inclusiv competențele de investigare și corective ale ANPD față de autoritățile de aplicare a legii, precum și să ia în considerare cu atenție orice evoluție relevantă în acest sens, ca parte a obligației sale de monitorizare.

Ținând seama de faptul că statelor li se acordă o marjă largă de apreciere în definirea aspectelor de securitate națională, care permite apoi derogări în materie de securitate națională în ceea ce privește prelucrarea datelor cu caracter personal, CEPD invită Comisia să descrie și să explice mai precis în proiectul de decizie conceptul de securitate națională în temeiul legislației braziliene. În acest sens, CEPD invită Comisia să clarifice suplimentar modul în care derogările de la LGPD în scopuri de securitate națională se raportează la colectarea și schimbul de date între entitățile publice din cadrul sistemului brazilian de informații (SISBIN).

Cuprins

1. INTRODUCERE	5
2. ASPECTE GENERALE PRIVIND PROTECȚIA DATELOR	6
2.1 Răspunderea și guvernanța datelor	6
2.2 Domeniu de aplicare și definiții	7
2.2.1 Domeniul de aplicare material și teritorial al LGPD	8
2.2.2. Definiții	8
2.3 Principii de protecție a datelor și temeuri juridice	9
2.3.1 Principiile prelucrării	9
2.3.2 Măsuri de securitate și încălcări ale securității	11
2.3.3 Legalitatea prelucrării	12
2.4 Drepturi individuale	12
2.5 Restricții privind transferurile ulterioare de date	13
2.6 Mecanisme procedurale și de asigurare a respectării legii	15
2.6.1 Supraveghere independentă	16
2.6.2 Căi de atac	17
2.6.3 Sancțiuni	17
3. ACCESAREA ȘI UTILIZAREA DE CĂTRE AUTORITĂȚILE PUBLICE DIN BRAZILIA A DATELOR CU CARACTER PERSONAL TRANSFERATE DIN UNIUNEA EUROPEANĂ.....	18
3.1 Accesarea și utilizarea datelor de către autoritățile publice braziliene în scopul aplicării dreptului penal	19
3.1.1 Cadrul juridic în domeniul asigurării respectării dreptului penal	19
3.1.2 Necesitatea și proporționalitatea	20
3.1.3 Utilizarea ulterioară a datelor și transferurile ulterioare	22
3.1.4 Supraveghere și căi de atac	23
3.2 Accesarea și utilizarea datelor de către autoritățile publice din Brazilia în scopuri legate de securitatea națională	24
3.2.1 Domeniul de aplicare al derogării de la articolul 4 alineatul (III) din LGPD și aplicabilitatea acestuia în cazul infracțiunilor împotriva securității statului	24
3.2.2 Cadrul juridic pentru securitatea națională	25

3.2.3 Transferuri ulterioare și acorduri internaționale	27
3.2.4 Supraveghere și căi de atac	28
4. PUNEREA ÎN APLICARE ȘI MONITORIZAREA PROIECTULUI DE DECIZIE	29

Comitetul European pentru Protecția Datelor

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

având în vedere Acordul privind Spațiul Economic European (denumit în continuare „SEE”), în special anexa XI și Protocolul 37 la acesta, astfel cum a fost modificat prin Decizia nr. 154/2018 a Comitetului mixt al SEE din 6 iulie 2018³,

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

ADOPTĂ PREZENTUL AVIZ:

³ Trimiterile la „statele membre” din prezentul aviz trebuie înțelese ca trimiteri la „statele membre ale SEE”.

1. INTRODUCERE

- (1) Capitolul V din RGPD stabilește condițiile pentru transferurile de date cu caracter personal către o țară terță sau către o organizație internațională. Transferurile de date cu caracter personal pot avea loc pe baza unei decizii a Comisiei Europene privind caracterul adecvat al nivelului de protecție (articolul 45 din RGPD) sau, în absența unei astfel de decizii privind caracterul adecvat al nivelului de protecție, atunci când operatorul sau persoana împuternicită de operator oferă garanții adecvate, inclusiv drepturi opozabile și căi de atac pentru persoana vizată (articolul 46 din RGPD). În absența unei decizii privind caracterul adecvat al nivelului de protecție sau a unor garanții adecvate, un transfer sau un set de transferuri de date cu caracter personal către o țară terță sau o organizație internațională poate avea loc numai în anumite condiții (articolul 49 din RGPD).
- (2) CEPD reamintește că deciziile privind caracterul adecvat al nivelului de protecție recunosc protecția continuă a datelor cu caracter personal transferate din SEE către țări terțe sau organizații internaționale și reprezintă un instrument solid de transfer pentru a se asigura că drepturile persoanei vizate sunt protejate atunci când datele sunt transferate în afara SEE. Potrivit criteriilor de referință privind caracterul adecvat al nivelului de protecție⁴ și jurisprudenței relevante a CJUE⁵, deși țara terță nu trebuie să asigure un nivel de protecție identic cu cel garantat în ordinea juridică a Uniunii, expresia „nivel de protecție adecvat” de la articolul 45 alineatul (1) din RGPD trebuie înțeleasă în sensul că impune ca țara terță respectivă să asigure efectiv, în temeiul legislației sale interne sau al angajamentelor sale internaționale, un nivel de protecție a drepturilor și libertăților fundamentale în esență echivalent cu cel garantat în cadrul Uniunii, interpretat în lumina Cartei drepturilor fundamentale.
- (3) Brazilia este o republică federativă formată din uniunea celor 26 de state și a Districtului Federal, conform prevederilor Constituției sale federale (denumită în continuare „Constituția”)⁶. Statele braziliene au, de asemenea, constituții proprii, care nu trebuie să contravină Constituției federale. Viața privată și protecția datelor sunt protejate în Constituție ca drepturi fundamentale [articolul 5 alineatul (X), articolul 5 alineatul (XII) și articolul 5 alineatul (LXXIX) din Constituție]⁷ și sunt recunoscute de Curtea Constituțională pentru orice persoană, inclusiv pentru un străin, indiferent dacă persoana respectivă își are reședința sau nu în Brazilia⁸.
- (4) Principalul act legislativ care reglementează protecția datelor este Legea generală privind protecția datelor sau „*Lei Geral de Proteção de Dados (LGPD)*” (nr. 13709 din 14 august 2018,

⁴ Grupul de lucru „articolul 29”, WP 254 rev.01, adoptat la 28 noiembrie 2017 și revizuit ultima dată și adoptat la 6 februarie 2018, aprobat de CEPD, capitolul 3, C.

⁵ CJUE, Hotărârea din 6 octombrie 2015, Maximilian Schrems/Comisarul pentru protecția datelor („Schrems”), C-362/14, și Tribunalul, Hotărârea din 3 septembrie 2025, Philippe Latombe/Comisia Europeană („Latombe”), T-553/23.

⁶ A se vedea considerentul 7 din proiectul de decizie.

⁷ A se vedea considerentul 8 din proiectul de decizie.

⁸ A se vedea considerentul 9 din proiectul de decizie.

modificată ultima dată prin Legea nr. 14460 din 25 octombrie 2022). LGPD este completată prin decrete cu caracter obligatoriu (Decretul prezidențial nr. 10 474 din 26 august 2020 și Decretul prezidențial nr. 11 758 din 30 octombrie 2023), care sunt obligatorii din punct de vedere juridic și executorii⁹.

- (5) Pe lângă LGPD, cadrul brazilian de protecție a datelor include reglementări cu caracter obligatoriu emise de Autoritatea pentru protecția datelor din Brazilia (*Agencia Nacional de Proteção de Dados – „ANPD”*)¹⁰. Aceste reglementări prevăd norme suplimentare privind interpretarea și aplicarea LGPD¹¹. De exemplu, Regulamentul nr. 4 din 24 februarie 2024 privind aplicarea sancțiunilor administrative, Regulamentul nr. 15 din 24 aprilie 2024 privind notificarea incidentelor de securitate („Regulamentul privind notificările incidentelor de securitate”), Regulamentul nr. 19 din 23 august 2024 privind transferul internațional al datelor cu caracter personal („Regulamentul privind transferul de date”), Regulamentul nr. 2 din 27 ianuarie 2022 privind aplicarea LGPD în cazul întreprinderilor mici și mijlocii, Regulamentul nr. 18 din 15 iulie 2024 privind rolul responsabilului cu protecția datelor („Regulamentul RPD”).
- (6) CEPD salută recunoașterea constituțională a dreptului la viață privată și la protecția datelor ca drepturi fundamentale, puse în aplicare în continuare prin intermediul legislației naționale. În plus, CEPD ia act cu satisfacție de angajamentele internaționale asumate de Brazilia¹².
- (7) CEPD ia act de faptul că, în temeiul articolelor 47 și 94 din Regulamentul (UE) 2018/1725, instituțiile¹³, organele, oficiile și agențiile Uniunii Europene pot transfera date cu caracter personal către o țară terță, un teritoriu, un sector sau o organizație internațională recunoscută de Comisia Europeană în temeiul articolului 45 alineatul (3) din Regulamentul (UE) 2016/679 ca asigurând un nivel adecvat de protecție, cu condiția ca transferul să îndeplinească exclusiv sarcini care țin de competența operatorului, fără a fi necesară o autorizație suplimentară. CEPD invită Comisia Europeană să reamintească această posibilitate legală în considerentele proiectului de decizie.

2. ASPECTE GENERALE PRIVIND PROTECȚIA DATELOR

2.1 Răspunderea și guvernanta datelor

⁹ A se vedea considerentele 11 și 12 din proiectul de decizie.

¹⁰ Toate reglementările cu caracter obligatoriu emise de ANPD sunt disponibile aici: https://www.gov.br/anpd/pt-br/aceso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd.

¹¹ A se vedea considerentul 13 din proiectul de decizie.

¹² A se vedea considerentele 8-10 din proiectul de decizie.

¹³ Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (RPDUE), JO L 295, 21.11.2018, p. 39.

- (8) LGPD prevede principiul responsabilității ca unul dintre principiile generale aplicabile prelucrării datelor cu caracter personal. Potrivit acestuia, operatorii și persoanele împuternicite de operatori¹⁴ adoptă măsuri tehnice și organizatorice adecvate pentru a-și îndeplini în mod eficace obligațiile în materie de protecție a datelor și trebuie să fie în măsură să demonstreze această conformitate, printre altele, autorității de supraveghere competente (articolul 46 din LGPD). CEPD ia act de faptul că astfel de măsuri includ desemnarea unui responsabil cu protecția datelor (articolul 41 din LGPD), astfel cum se detaliază în Regulamentul privind RPD al ANPD; evaluarea impactului asupra protecției datelor (articolul 38 din LGPD), precum și păstrarea evidențelor activităților de prelucrare a datelor (articolul 37 din LGPD). În plus, LGPD prevede că operatorii și persoanele împuternicite de operatori pot formula norme interne privind bunele practici și modele de guvernare, inclusiv planuri pentru activități educaționale, mecanisme de supraveghere internă și atenuarea riscurilor (articolul 50 din LGPD). CEPD ia act cu satisfacție de faptul că astfel de instrumente sunt similare celor prevăzute în RGPD pentru a pune în aplicare principiul responsabilității și salută această aliniere strânsă.
- (9) CEPD ia act de faptul că, în ceea ce privește EIPD, LGPD nu include obligația clară de a efectua o EIPD în cazurile în care prelucrarea ar putea genera un risc ridicat pentru drepturile și libertățile persoanelor fizice, atunci când se referă numai la posibila solicitare din partea ANPD. În această privință, CEPD ia act de faptul că ANPD recomandă efectuarea unei EIPD atunci când operațiunea de prelucrare poate genera un risc ridicat în cadrul „întrebărilor frecvente”¹⁵ referitoare la EIPD („Întrebări frecvente privind EIPD”). În plus, LGPD nu include în mod explicit evaluarea necesității și a proporționalității în domeniul de aplicare al EIPD. Cu toate acestea, întrebările frecvente privind EIPD recomandă operatorilor și persoanelor împuternicite de operatori să evalueze în cadrul EIPD-urilor lor necesitatea și proporționalitatea prelucrării.
- (10) În acest context, CEPD invită Comisia Europeană să monitorizeze punerea în aplicare practică a acestor cerințe pentru a verifica dacă EIPD este efectuată atunci când operațiunea de prelucrare este de natură să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice și dacă evaluarea necesității și proporționalității operațiunilor de prelucrare în raport cu scopurile este, de asemenea, inclusă în DPIA.

2.2 Domeniu de aplicare și definiții

- (11) Capitolul 3 din criteriile de referință privind caracterul adecvat al nivelului de protecție este dedicat „principiilor privind conținutul” și se referă la concepte și principii de bază privind protecția datelor. Un sistem al unei țări terțe sau al unei organizații internaționale trebuie să conțină astfel de concepte și principii de bază pentru a asigura un nivel de protecție a datelor cu caracter personal în esență echivalent cu cel garantat de dreptul Uniunii. Acestea nu

¹⁴ Agenți de prelucrare, în conformitate cu articolul 5 alineatul (IX) din LGPD.

¹⁵ https://www.gov.br/anpd/pt-br/canais_atendimento/agentes-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd.

trebuie să corespundă terminologiei RGPD, dar ar trebui să reflecte conceptele consacrate în legislația europeană privind protecția datelor și să fie în concordanță cu acestea. Criteriile de referință privind caracterul adecvat al nivelului de protecție se referă la următoarele concepte importante: „date cu caracter personal”, „prelucrare”, „operatori de date”, „persoană împuternicită de operator”, „destinatar” și „date sensibile”. Acest aspect al legislației braziliene va fi analizat la punctele următoare.

2.2.1 Domeniul de aplicare material și teritorial al LGPD

- (12) CEPD salută faptul că domeniul de aplicare al LGPD, atât material, cât și teritorial, este foarte similar cu cel prevăzut de cadrul UE privind protecția datelor.
- (13) Articolul 4 din LGPD exclude din domeniul său de aplicare prelucrarea în scopuri pur personale și neeconomice, iar astfel de excepții sunt avute în vedere și în RGPD [articolul 2 alineatul (2) litera (c) din RGPD]. În plus, alte operațiuni de prelucrare se află parțial în afara domeniului de aplicare al LGPD, în special în scopuri legate de: siguranța publică, apărarea națională, legile adoptate la nivelul unui stat sau investigarea și urmărirea penală a infracțiunilor; scopuri jurnalistice și artistice; cercetarea academică; cercetarea în domeniul sănătății [articolul 3 alineatul (III) din LGPD]. Acest aspect este detaliat în secțiunea 3.1 din prezentul avis.
- (14) În special în ceea ce privește aplicarea parțială a LGPD pentru prelucrarea datelor cu caracter personal în scopuri jurnalistice și artistice, CEPD observă că domeniul de aplicare al excepției este echivalent cu cel prevăzut la articolul 85 alineatul (2) din RGPD¹⁶, și anume o astfel de excepție se aplică numai atunci când datele cu caracter personal sunt prelucrate exclusiv în acest scop, toate celelalte prelucrări de către presă, mass-media și organismele artistice intrând în domeniul de aplicare al LGPD. De asemenea, rămân aplicabile unele excepții prevăzute pentru prelucrarea datelor cu caracter personal exclusiv în scopuri academice, și anume articolele 7 (cerințe privind temeiul juridic) și 11 (norme privind prelucrarea datelor sensibile) din LGPD¹⁷. Domeniul de aplicare al acestor excepții este, de asemenea, în conformitate cu cel stabilit la articolul 85 alineatul (2) din RGPD.

2.2.2. Definiții

- (15) CEPD ia act cu satisfacție de alinierea la cadrul UE de protecție a datelor în ceea ce privește definițiile utilizate în LGPD, care sunt în concordanță cu cele prevăzute în RGPD. În special, LGPD definește „datele cu caracter personal”, „informațiile pseudonimizate”, „datele anonime”¹⁸, „prelucrarea datelor”, „operatorul de date”, „persoana împuternicită de operator”

¹⁶ A se vedea, de asemenea, considerentul 35 din proiectul de decizie.

¹⁷ A se vedea, de asemenea, considerentele 32 și 33 din proiectul de decizie.

¹⁸ Articolul 12 din LGPD prevede, de asemenea, că datele anonimizate nu sunt considerate date cu caracter personal, cu excepția cazului în care anonimizarea a fost sau poate fi inversată prin eforturi rezonabile. Acest articol explică faptul că termenul „rezonabil” ar trebui luat în considerare ținând seama de factori obiectivi precum: 1) costul și timpul necesare pentru inversare; 2) tehnologia disponibilă; și (3) utilizarea exclusivă a mijloacelor proprii ale operatorului.

și „datele sensibile” (articolul 5 din LGPD) în mod similar celor definite în RGPD, și anume considerentul 26, articolul 4 și articolul 9 alineatul (1). Alte definiții, de exemplu „persoană vizată”, „responsabil cu protecția datelor”, „consimțământ”, „evaluare a impactului asupra protecției datelor” și conceptul de „exercitare în comun a competenței de operator”¹⁹ sunt, de asemenea, echivalente în esență cu conceptele prevăzute în RGPD.

2.3 Principii de protecție a datelor și temeuri juridice

2.3.1 Principiile prelucrării

- (16) Criteriile de referință privind caracterul adecvat al nivelului de protecție, în conformitate cu RGPD, stabilesc că datele trebuie prelucrate în mod legal, echitabil și legitim. În conformitate cu articolul 6 din LGPD, activitățile de prelucrare a datelor cu caracter personal se desfășoară cu bună-credință și se supun următoarelor principii privind: scopul, caracterul adecvat, necesitatea, accesul liber²⁰, calitatea datelor, transparența, securitatea, prevenirea, nediscriminarea, răspunderea și responsabilitatea.
- (17) Luând în considerare conceptele acestor principii, sistemul juridic brazilian consacră aceleași principii de prelucrare a datelor prevăzute la articolul 5 din RGPD. De exemplu, în ceea ce privește limitarea scopului, LGPD prevede la articolul 7 alineatul (7) că „prelucrarea ulterioară a datelor cu caracter personal menționate la alineatele 3 (date cu caracter personal accesibile publicului) și 4 (date făcute publice în mod manifest de persoana vizată) din prezentul articol poate fi efectuată în scopuri noi, cu condiția respectării unor scopuri legitime și specifice pentru noua prelucrare și pentru păstrarea drepturilor persoanei vizate, precum și a motivelor și principiilor prevăzute de prezenta lege”.
- (18) RGPD prevede în mod clar că o astfel de prelucrare ulterioară ar avea loc numai dacă un astfel de scop nou este compatibil cu scopul inițial. Cerința de a asigura compatibilitatea scopurilor (precum și respectarea standardelor etice și a garanțiilor tehnice și juridice aplicabile) este evidențiată în Ghidul pentru prelucrarea datelor cu caracter personal în scopuri academice și pentru efectuarea de studii și cercetări emis de ANPD, precum și în Orientările privind interesul legitim. În Orientările privind interesul legitim, ANPD explică modul în care operatorul de date trebuie să demonstreze o legătură efectivă între cele două scopuri ale prelucrării și să ia în considerare „așteptările legitime” ale persoanei vizate. Orientările clarifică în continuare faptul că „[a]naliza așteptărilor legitime se poate baza pe mai mulți factori, printre care următorii: d) scopul preconizat al colectării datelor și compatibilitatea acestuia cu prelucrarea bazată pe un interes legitim”. CEPD salută această clarificare din partea ANPD, care contribuie la o mai bună aliniere a cerințelor limitării scopului.

¹⁹ A se vedea articolul 42 alineatul (1) punctul (l) din LGPD.

²⁰ „Accesul liber: garantarea pentru persoanele vizate a unei consultări facilitate și gratuite cu privire la forma și durata prelucrării, precum și cu privire la integritatea datelor lor cu caracter personal” (articolul 6 partea IV din LGPD).

- (19) Principiul limitării legate de stocare prevăzut în RGPD prevede că datele se stochează numai pe perioada necesară pentru a se asigura îndeplinirea scopurilor în care sunt prelucrate [articolul 5 alineatul (1) litera (e) din RGPD]. Chiar dacă articolul 6 din LGPD nu include în mod explicit principiul limitării legate de stocare, acest articol ar trebui coroborat cu articolul 15 din LGPD, care precizează cerința în cazul încetării prelucrării datelor. În acest articol, principiul limitării legate de stocare este în mod clar legat de principiile „caracterului adecvat” și „necesității” care se încadrează în principiile generale enumerate la articolul 6 din LGPD. Pentru mai multă claritate, CEPD încurajează Comisia Europeană să clarifice în proiectul de decizie interacțiunea dintre articolele 6 și 15 din LGPD în raport cu principiul limitării legate de stocare.
- (20) În plus, în ceea ce privește cerințele de limitare a stocării, articolul 16 din LGPD stabilește condițiile de stocare și de ștergere a datelor cu caracter personal după încheierea prelucrării. Acest articol prevede, de asemenea, patru scopuri în care datele pot fi păstrate după încetarea prelucrării datelor: (1) pentru respectarea obligațiilor legale sau de reglementare; (2) în scopuri de cercetare, asigurând, ori de câte ori este posibil, anonimizarea datelor; (3) atunci când sunt transferate unor terți în conformitate cu cerințele LGPD; sau (4) atunci când sunt utilizate exclusiv de operator, atât timp cât datele sunt anonimizate, iar accesul terților la datele respective este interzis. CEPD ia act de faptul că aceste situații de prelucrare sunt în conformitate cu principiul limitării legate de stocare consacrat în RGPD.
- (21) Principiul transparenței și al echității urmărește să asigure controlul persoanelor vizate asupra datelor lor cu caracter personal și, în acest scop, informațiile sunt furnizate persoanei vizate într-un mod proactiv, ca regulă generală²¹. În același timp, LGPD stabilește o limitare a acestui principiu legată de „secretul comercial și industrial”, care poate avea un impact asupra persoanelor vizate care urmează să primească informații cu privire la prelucrarea datelor lor pentru a-și putea exercita controlul asupra acestora (de exemplu, prin depunerea plângerii la ANPD). Cu toate acestea, în proiectul de decizie, Comisia Europeană explică faptul că această limitare ar trebui interpretată din perspectiva Legii Braziliei privind accesul la informații și a Decretului prezidențial nr. 7721 din 16 mai 2012 și „prin urmare, trebuie interpretată astfel încât prelucrarea și divulgarea în alt mod a informațiilor să nu dezvăluie secrete comerciale sau să creeze avantaje concurențiale pentru alți actori, îndeplinind în același timp obiectivele de protecție a datelor cu caracter personal. Aceasta înseamnă că, în ceea ce privește principiul transparenței și în întregul text al LGPD, limitarea pe motivul «secretului comercial și industrial» nu trebuie înțeleasă ca un motiv general de refuz al respectării legii, ci în sensul că trebuie instituite garanții specifice pentru a se asigura divulgarea informațiilor într-un mod care să protejeze interesele respective”²².

²¹ Acest lucru este subliniat și de criteriile de referință privind caracterul adecvat al nivelului de protecție; a se vedea capitolul 3 secțiunea A alineatul (7).

²² A se vedea considerentul 81 din proiectul de decizie.

- (22) Având în vedere importanța principiului transparenței, CEPD invită Comisia Europeană să monitorizeze punerea în aplicare a acestei dispoziții în practică pentru a înțelege mai bine impactul acesteia asupra dreptului la informare și acces.

2.3.2 Măsurile de securitate și încălcări ale securității

- (23) LGPD include principiile de securitate și prevenire care impun aplicarea unor măsuri de protecție a datelor cu caracter personal și de prevenire a prejudiciilor legate de o astfel de prelucrare [articolul 6 alineatele (VII) și (VII) din LGPD]; în plus, LGPD prevede în mod explicit că, în cazul în care măsurile de securitate nu sunt puse în aplicare în mod corespunzător, prelucrarea datelor este considerată ilegală. Legea impune punerea în aplicare a măsurilor necesare pentru demonstrarea conformității cu acest principiu prin abordarea bazată pe riscuri (articolele 44, 46 și 47 din LGPD) și respectarea cerințelor pentru evaluarea încălcării și notificarea încălcării (articolele 48 și 49 din LGPD). CEPD ia act cu satisfacție de faptul că aceste principii și obligații sunt strâns aliniate la cele prevăzute în RGPD.
- (24) CEPD salută adoptarea de către ANPD a unui regulament suplimentar cu caracter obligatoriu privind notificările incidentelor de securitate a informațiilor, care explică conceptul incidentului și detalii pentru evaluarea gravității acestuia (de exemplu, atunci când se consideră că incidentul creează riscuri pentru persoanele vizate sau afectează în mod semnificativ interesele și drepturile fundamentale ale persoanelor vizate și, prin urmare, se comunică ANPD și persoanei vizate), precum și privind cerințele de notificare a incidentelor²³. În acest sens, CEPD ia act de faptul că, în conformitate cu Regulamentul privind notificările incidentelor de securitate a informațiilor, ca regulă generală, „comunicarea unui incident de securitate a informațiilor către ANPD trebuie efectuată de operator în termen de trei zile lucrătoare”²⁴ și invită Comisia Europeană să își alinieze proiectul de decizie (considerentul 75) în consecință²⁵.
- (25) În ceea ce privește notificarea încălcărilor securității datelor, CEPD ia act de faptul că LGPD prevede că o astfel de notificare (atât către ANPD, cât și către persoana vizată) include, printre altele, informații privind măsurile tehnice și de securitate utilizate pentru protecția datelor cu caracter personal, adoptate înainte și după incident, cu respectarea secretelor comerciale și industriale [articolul 6 alineatul (III) și articolul 9 alineatul (II) din LGPD]. CEPD înțelege necesitatea de a se asigura în mod eficace că dreptul la viață privată și la protecția datelor nu afectează în mod negativ protecția altor drepturi și invită Comisia să monitorizeze punerea în aplicare a unei astfel de limitări în cazul în care informațiile privind incidentul au fost furnizate parțial (luând în considerare secretele comerciale și industriale) și eventualul impact al acesteia asupra competențelor ANPD.

²³ A se vedea considerentele 73-77 din proiectul de decizie.

²⁴ A se vedea articolele 6 și 9 din Regulamentul privind notificările incidentelor de securitate a informațiilor.

²⁵ A se vedea considerentul 75 din proiectul de decizie, conform căruia „[n]otificarea unui incident de securitate a informațiilor către ANPD și persoanele vizate are loc în termen de trei zile (72 de ore) de la momentul la care operatorul a luat cunoștință de acesta”.

2.3.3 Legalitatea prelucrării

- (26) CEPD ia act de faptul că principiul legalității și punerea sa în aplicare, astfel cum se prevede în LGPD [articolul 5 alineatul (XII), articolele 7, 8 și 10], este strâns aliniat la cel consacrat în RGPD [articolul 4 alineatul (11), articolele 6, 7 și 9] și salută această aliniere.

2.3.3.1 Interesul legitim

- (27) Cerințele privind interesul legitim care trebuie utilizate ca temei juridic pentru prelucrarea în LGPD [articolul 7 alineatul (IX)] sunt aliniate la RGPD [articolul 6 alineatul (1) litera (f)]. LGPD subliniază, de asemenea, că drepturile și libertățile fundamentale (care includ dreptul la protecția datelor²⁶) ar trebui să prevaleze de obicei.
- (28) CEPD ia act de faptul că articolul 10 din LGPD enumeră scopurile legitime pentru care ar putea fi utilizat un astfel de temei juridic. Unul dintre aceste scopuri legitime este sprijinirea și promovarea activității operatorului [articolul 10 alineatul (I) din LGPD].
- (29) Deși această expresie pare să fie cuprinzătoare, CEPD ia act de faptul că condițiile de utilizare a „interesului legitim” sunt detaliate în Ghidul privind „Temeiul juridic pentru prelucrarea datelor cu caracter personal – Interesul legitim” („Ghidul privind interesul legitim”) adoptat de ANPD. Acest ghid clarifică faptul că, pentru ca un interes să fie considerat „legitim”, trebuie îndeplinite trei condiții: (1) compatibilitatea cu sistemul juridic brazilian; (2) referirea la o situație specifică; și (3) prelucrarea să fie legată de scopuri legitime, specifice și explicite²⁷. Aceste condiții sunt similare cu trei condiții cumulative pentru ca prelucrarea datelor cu caracter personal să fie legală în baza acestui temei juridic, specificat de CJUE²⁸, și cu explicațiile suplimentare furnizate de Curte. În plus, condițiile privind „interesul legitim” specificate în Ghidul privind interesul legitim sunt apropiate de cele din orientările adoptate de CEPD²⁹. CEPD salută abordarea adoptată de ANPD în ceea ce privește interesul legitim și utilizarea sa pentru prelucrare.

2.4 Drepturi individuale

- (30) CEPD salută faptul că LGPD oferă persoanelor fizice drepturi similare celor prevăzute în RGPD (ambele în capitolul III). În special, LGPD are în vedere dreptul de acces, dreptul la rectificare, dreptul la portabilitatea datelor, dreptul la restricționarea prelucrării, dreptul la ștergerea datelor, dreptul la informare, dreptul de a refuza sau de a retrage consimțământul,

²⁶ A se vedea punctul 3 din prezentul aviz.

²⁷ A se vedea considerentul 52 din proiectul de decizie.

²⁸ De exemplu, CJUE, Hotărârea din 7 decembrie 2023, cauzele conexate C-26/22 și C-64/22, SCHUFA Holding AG, punctele 75-80.

²⁹ Orientările nr. 1/2024 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (f) din RGPD (versiunea 1.0), adoptate la 8 octombrie 2024.

precum și dreptul de a se opune prelucrării și dreptul de a adresa petiții (articolele 9 și 18 din LGPD).

- (31) LGPD prevede, de asemenea, dreptul persoanelor vizate de a solicita reexaminarea deciziilor luate exclusiv pe baza prelucrării automate a datelor cu caracter personal care le afectează interesele (articolul 20 din LGPD). Conținutul articolului 20 din LGPD reflectă în esență articolul 22 din RGPD.
- (32) CEPD ia act de faptul că, în ceea ce privește drepturile persoanelor vizate, Legea braziliană privind „habeas data” stabilește dispoziții specifice pentru a acorda dreptul de acces și dreptul de rectificare într-un termen scurt (10 și, respectiv, 15 zile) de la cererea unei persoane și salută acest aspect.
- (33) CEPD consideră că LGPD stabilește cerințe în esență echivalente cu cele asigurate în RGPD pentru drepturile persoanelor vizate.

2.5 Restricții privind transferurile ulterioare de date

- (34) Criteriile de referință privind caracterul adecvat al nivelului de protecție 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 să fie permis numai în cazul în care destinatarul ulterior (adică destinatarul transferului ulterior) face, de asemenea, obiectul unor norme (inclusiv norme contractuale) care oferă un nivel adecvat de protecție și urmează instrucțiunile relevante atunci când prelucrează date în numele operatorului de date”.
- (35) În ceea ce privește evaluarea caracterului adecvat al cadrului juridic și al practicii Braziliei, transferul ulterior înseamnă transferul de date cu caracter personal de la entitatea care acționează în calitate de operator în cadrul domeniului de aplicare teritorial al LGPD a Braziliei către entitatea din afara acestui domeniu de aplicare.
- (36) Cerințele privind transferul ulterior sunt prevăzute în capitolul V din LGPD și completate ulterior de ANPD prin adoptarea „Regulamentului privind transferul de date”, care prevede definiții ale noțiunilor de „transfer”, „transfer internațional de date”, „importator”, „exportator” și includ cerințe detaliate pentru transferuri.
- (37) CEPD ia act cu satisfacție de faptul că definițiile noțiunilor de „transfer” și de „transfer internațional de date” sunt aliniate la cele din Orientările CEPD nr. 05/2021³⁰.
- (38) În conformitate cu LGPD și cu Regulamentul privind transferul de date, transferurile ulterioare pot avea loc numai în scopuri legitime, specifice și explicite și atunci când există instrumente

³⁰ Punctul 9, Orientările nr. 05/2021 privind interacțiunea dintre aplicarea articolului 3 și dispozițiile privind transferurile internaționale în conformitate cu capitolul V din RGPD, adoptate la 14 februarie 2023.

sau condiții specifice (articolul 33 din LGPD și articolele 9-33 din Regulamentul privind transferul de date)³¹. CEPD apreciază că aceste instrumente sunt foarte similare instrumentelor de transfer prevăzute în capitolul V din RGPD. Cu toate acestea, CEPD invită Comisia Europeană să clarifice în proiectul de decizie dacă transferurile pot fi efectuate în conformitate cu articolul 33 alineatele (III)-(IX) din LGPD numai în circumstanțele excepționale, în care condițiile prevăzute la articolul 33 alineatele (I)-(II) din LGPD nu sunt îndeplinite³².

- (39) Cu toate acestea, Regulamentul privind transferul de date precizează că transferurile de date cu caracter personal sunt permise „atunci când persoana vizată și-a dat consimțământul specific și distinct pentru un astfel de transfer, fiind informată în prealabil cu privire la caracterul internațional al operațiunii preconizate, care se distinge în mod clar de alte scopuri”. Nu este clar dacă o astfel de cerință implică obligația de a informa persoanele vizate cu privire la posibilele riscuri ale transferurilor internaționale care decurg din lipsa unei protecții adecvate în țara terță și din absența unor garanții adecvate (de exemplu, informații privind faptul că este posibil să nu existe o autoritate de supraveghere și/sau principii de prelucrare a datelor și/sau drepturi ale persoanelor vizate în țara terță), care este o cerință în temeiul articolului 49 alineatul (1) litera (a) din RGPD. Pentru CEPD și în conformitate cu RGPD, furnizarea acestor informații este esențială pentru a permite persoanei vizate să își dea consimțământul în cunoștință de cauză, având cunoștință deplină despre aceste aspecte specifice ale transferului. Prin urmare, CEPD invită Comisia Europeană să clarifice în proiectul de decizie dacă persoana vizată este informată cu privire la posibilele riscuri ale unui astfel de transfer care decurg din absența unei protecții adecvate în țara terță și cu privire la garanțiile adecvate.
- (40) În plus, Regulamentul privind transferul de date prevede că „[a]tât operatorul, cât și persoana împuternicită de operator trebuie să adopte măsuri eficiente care să demonstreze respectarea și conformitatea cu normele privind protecția datelor cu caracter personal, precum și eficacitatea acestor măsuri, într-un mod compatibil cu nivelul de risc al prelucrării și cu modalitatea de transfer internațional utilizată” [articolul 4 alineatul (2) din Regulamentul privind transferul de date]. CEPD salută includerea acestei obligații. În același timp, ar fi benefic să se clarifice faptul că eficacitatea acestor măsuri ar trebui evaluată astfel încât să se asigure, de asemenea, că legislația locală a țărilor terțe relevante nu ar submina continuitatea protecției persoanelor vizate ale căror date sunt transferate³³. CEPD invită Comisia Europeană să clarifice faptul că acest element va fi luat în considerare și în scenariile de transfer.
- (41) CEPD salută includerea unei cerințe explicite de transparență în ceea ce privește persoana vizată, și anume că persoanele vizate au dreptul de a primi instrumentul contractual utilizat pentru transferul ulterior, precum și descrierea unui astfel de transfer, de exemplu durata și

³¹ A se vedea, de asemenea, considerentele 101-109 din proiectul de decizie.

³² Articolul 49 din RGPD precizează că derogările prevăzute la acest articol pot fi utilizate numai în absența unei decizii privind caracterul adecvat al nivelului de protecție în temeiul articolului 45 alineatul (3) din RGPD sau a unor garanții adecvate în temeiul articolului 46 din RGPD.

³³ A se vedea hotărârea în cauza Latombe. A se vedea, de asemenea, CJUE, Hotărârea din 16 iulie 2020 în cauza C-311/18 („Schrems II”).

scopul transferului, țările de destinație, responsabilitățile părților implicate, drepturile persoanelor vizate și mijloacele de exercitare a acestora (articolul 16 din Regulamentul privind transferul de date).

- (42) Cu toate acestea, se pare că un astfel de domeniu de aplicare al obligației de transparență este relevant numai atunci când transferurile sunt efectuate pe baza unor clauze contractuale standard, și nu atunci când sunt utilizate alte instrumente³⁴. Prin urmare, CEPD invită Comisia Europeană să clarifice faptul că aceleași obligații de transparență se aplică indiferent de instrumentul de transfer utilizat.
- (43) CEPD ia act, de asemenea, de faptul că cerințele privind conținutul BCR nu sunt pe deplin conforme cu cele din RGPD, în special cu articolul 47 alineatul (2) litera (f) și litera (l) din RGPD. Pentru a se asigura că nivelul de protecție oferit de RGPD nu va fi subminat, CEPD invită Comisia Europeană să clarifice în proiectul de decizie că și aceste elemente³⁵ vor fi luate în considerare atunci când acest instrument de transfer trebuie utilizat pentru transferurile ulterioare de date cu caracter personal către Brazilia în temeiul deciziei privind caracterul adecvat al nivelului de protecție.

2.6 Mecanisme procedurale și de asigurare a respectării legii

- (44) În conformitate cu criteriile de referință privind caracterul adecvat al nivelului de protecție³⁶ și cu jurisprudența relevantă a CJUE³⁷, un sistem de protecție a datelor echivalent în esență cu modelul Uniunii Europene trebuie să prevadă: (i) o autoritate independentă, care ar trebui să supravegheze și să asigure respectarea legislației privind protecția datelor, având competența de a investiga și de a lua măsuri fără influență externă. Sistemele de protecție a datelor trebuie să asigure (ii) că operatorii și persoanele împuternicite de operatori sunt responsabili și își cunosc responsabilitățile, în timp ce persoanele vizate sunt informate cu privire la drepturile lor. Ar trebui instituite sancțiuni și procese de verificare eficace pentru a asigura respectarea normelor; (iii) faptul că operatorii de date și persoanele împuternicite de operatori demonstrează conformitatea, prin măsuri precum evaluări ale impactului asupra protecției datelor, evidențe ale activităților de prelucrare și numirea responsabililor cu protecția datelor. În plus, (iv) sistemul de protecție a datelor trebuie să furnizeze asistență și sprijin fiecărei persoane vizate în exercitarea drepturilor sale și mecanisme adecvate de recurs.

³⁴ De exemplu, Regulamentul privind transferul de date include cerințe generale privind transparența atunci când se intenționează utilizarea regulilor corporatiste obligatorii (*binding corporate rules* – BCR), în special „instituirea și punerea în aplicare a unui program de guvernanță în materie de confidențialitate care vizează stabilirea unei relații de încredere cu persoana vizată, prin intermediul unor acțiuni transparente care să asigure mecanisme pentru participarea persoanei vizate” [articolul 25 alineatul (V) din Regulamentul privind transferul de date] și transparența în ceea ce privește exercitarea drepturilor persoanei vizate și a dreptului de a depune o plângere [articolul 26 alineatul (VI) din Regulamentul privind transferul de date].

³⁵ Răspunderea și cooperarea cu autoritatea de supraveghere [articolul 47 alineatul (2) litera (f) și litera (l) din RGPD].

³⁶ A se vedea capitolul 3 secțiunea (C) din Criteriile de referință privind caracterul adecvat al nivelului de protecție.

³⁷ CJUE, Hotărârea din 6 octombrie 2015, Schrems, C-362/14.

- (45) În această secțiune, evaluarea CEPD se concentrează asupra existenței unei autorități independente, a unui mecanism de recurs adecvat și a unor sancțiuni eficace.

2.6.1 Supraveghere independentă

- (46) LGPD instituie *Agencia Nacional de Proteção de Dados* (ANPD) ca autoritate națională de supraveghere responsabilă cu monitorizarea și punerea în aplicare a dispozițiilor sale.
- (47) CEPD salută faptul că ANPD a primit statutul de „autoritate cu caracter special”, o desemnare menită să asigure autonomia necesară pentru exercitarea deplină a funcțiilor și competențelor juridice care îi sunt conferite de LGPD, în special prin revocarea dispozițiilor care condiționau funcționarea și operațiunile financiare ale ANPD de autorizațiile care urmau să fie acordate de executiv.
- (48) De asemenea, CEPD salută modificările aduse la 15 septembrie 2025 cadrului juridic brazilian, conform cărora ANPD este recunoscută în prezent ca **agenție de reglementare**³⁸. Prin urmare, CEPD înțelege că una dintre principalele modificări este că ANPD își va transmite bugetul direct Ministerului Planificării și Bugetului, în loc să îl transmită prin intermediul Ministerului Justiției. Bugetul ANPD rămâne o linie separată în bugetul de stat federal. CEPD înțelege că ANPD avea deja independență și în ceea ce privește bugetul și finanțele sale, dar, devenind o agenție de reglementare, procesul său administrativ este simplificat.
- (49) CEPD salută, de asemenea, noua competență a ANPD, care a fost desemnată recent drept autoritate responsabilă cu protecția copiilor în mediul online³⁹. CEPD ia act de faptul că, în conformitate cu capitolul IX din LGPD, ANPD dispune de competențele și misiunile necesare și disponibile pentru a asigura respectarea drepturilor privind protecția datelor și pentru a promova conștientizarea, cum ar fi competențele de investigare și sancționare (articolul 55-J LGPD).
- (50) În ceea ce privește personalul și bugetul ANPD, care joacă un rol important în independența acesteia, CEPD ia act cu satisfacție de decizia recentă de majorare a numărului de angajați prin crearea a peste 200 de posturi noi⁴⁰.
- (51) CEPD ia act de faptul că, în conformitate cu articolul 55-C din LGPD, (actuala) ANPD este compusă dintr-o serie de organisme⁴¹, inclusiv Consiliul național pentru protecția datelor cu caracter personal și a vieții private (denumit în continuare „Consiliul”). CEPD ia act de

³⁸ Măsura provizorie nr. 1.317/2025 este disponibilă la adresa <https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314>.

³⁹ Legea nr. 15.211/2025 privind protecția copiilor și a minorilor în mediul digital, disponibilă la adresa <https://www.in.gov.br/web/dou/-/lei-n-15.211-de-17-de-setembro-de-2025-656579619>.

⁴⁰ <https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314>.

⁴¹ Potrivit articolului 55-C din LGPD, ANPD se compune din: Consiliul de administrație, cel mai înalt organ de conducere; Consiliul național pentru protecția datelor cu caracter personal și a vieții private; Biroul Comisiei de disciplină; IV – Biroul Ombudsmanului; VI – Biroul pentru afaceri juridice și VI – Unități administrative și unități specializate necesare pentru punerea în aplicare a dispozițiilor LGPD. A se vedea, de asemenea, considerentele 126-130 din proiectul de decizie.

componența acestuia, care include, de asemenea, reprezentanți ai ramurii executive federale, ai ramurii legislative și ai sistemului judiciar⁴². CEPD ia act, de asemenea, de faptul că, în conformitate cu articolul 58-B din LGPD, Consiliul este responsabil, printre altele, de (i) „propunerea de orientări strategice și furnizarea de informații generale pentru pregătirea politicii naționale privind protecția datelor cu caracter personal și a vieții private și pentru activitățile ANPD”; și (ii) „recomandarea acțiunilor care urmează să fie întreprinse de ANPD”.

- (52) În special în ceea ce privește aceste sarcini, CEPD consideră că este important să se înțeleagă mai clar modul în care acestea sunt puse în aplicare și măsura în care propunerile și recomandările Consiliului influențează activitatea ANPD. Prin urmare, invită Comisia Europeană să aprofundeze aceste sarcini și interacțiunea dintre Consiliu și ANPD, pentru a evalua mai bine influența Consiliului asupra activităților ANPD.

2.6.2 Căi de atac

- (53) CEPD salută mecanismul de recurs prevăzut de LGPD, care oferă, de asemenea, persoanelor vizate dreptul de a formula o plângere la ANPD și de a contesta decizia sa prin prezentarea unui recurs în fața consiliului său de administrație. Ulterior, persoanele fizice pot să conteste în instanță deciziile consiliului, precum și să introducă orice recurs împotriva ANPD pentru nerespectarea obligațiilor care îi revin în temeiul LGPD. Diferența dintre instrumentul de apel și instrumentul de recurs nu reiese în mod clar din proiectul de decizie. CEPD invită Comisia să clarifice suplimentar funcționarea acestor două căi, inclusiv dacă recurgerea la recurs se limitează doar la refuzul de a trata o plângere sau la respingerea pe fond a unei plângeri.
- (54) De asemenea, CEPD salută acordarea dreptului la despăgubiri pentru daunele materiale și morale, precum și acțiunile colective în despăgubire (articolul 22 din LGPD).

2.6.3 Sancțiuni

- (55) CEPD reamintește că existența unor sancțiuni eficace și disuasive poate juca un rol important în asigurarea respectării normelor de protecție a datelor, deoarece este un semn al gradului ridicat de responsabilitate și de conștientizare pe care sistemul îl asigură. CEPD salută competențele corective conferite ANPD, care au fost exercitate în mai multe rânduri⁴³ și includ o serie de măsuri, cum ar fi avertismente, amenzi de până la două procente (2 %) din veniturile brute ale entității juridice private implicate, amenzi zilnice, blocarea datelor cu caracter personal legate de încălcare până la regularizarea situației, suspendarea temporară a activităților relevante de prelucrare a datelor și ștergerea datelor cu caracter personal în cauză

⁴² A se vedea, de asemenea, considerentul 132 din proiectul de decizie și articolul 55-C din LGPD.

⁴³ A se vedea ANPD, Registrul sancțiunilor. https://www.gov.br/anpd/pt-br/centrais-de-conteudo/deciso-es-em-processos-sancionadores-1/deciso-es-em-processos-sancionadores?_authenticator=7951f0a70d3d125fd05e11a1e544b72d2c61f304.

(articolul 52 din LGPD)⁴⁴. CEPD invită Comisia să monitorizeze aplicarea consecventă a acestora, în special în ceea ce privește sancțiunile.

- (56) CEPD ia act cu satisfacție de faptul că ANPD a emis un regulament (cu caracter obligatoriu) privind sancțiunile. Acest regulament clasifică sancțiunile la diferite niveluri, utilizând factori obiectivi, cum ar fi tipul și volumul datelor prelucrate sau impactul drepturilor persoanelor vizate și prevede o metodologie de calculare a amenzilor, care este în conformitate cu cerințele de la articolul 83 din RGPD.

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

- (57) În temeiul articolului 45 alineatul (2) din RGPD, evaluarea limitărilor și a garanțiilor prevăzute în legislația braziliană în ceea ce privește accesul și utilizarea ulterioară de către autoritățile publice braziliene a datelor cu caracter personal transferate operatorilor și persoanelor împuternicite de operatori din Brazilia în scopuri de asigurare a respectării dreptului penal și de securitate națională („accesul autorităților publice”) este un element important al testului „echivalenței esențiale”, astfel cum a fost interpretat de CJUE.
- (58) CEPD ia act cu satisfacție de atenția specială acordată acestui aspect și informațiile concrete furnizate de Comisie în proiectul de decizie⁴⁵. Prin urmare, CEPD se abține de la reproducerea majorității constatărilor și evaluărilor factuale în prezentul avis. În schimb, evaluează interferența sistemului brazilian în ceea ce privește accesul guvernului în scopuri de asigurare a respectării legii și de securitate națională pe baza celor 4 elemente identificate de CEPD în Garanțiile esențiale europene pentru măsurile de supraveghere., adoptate la 10 noiembrie 2020⁴⁶:
- Garanția A – Norme clare, precise și accesibile;
 - Garanția B – Necesitatea și proporționalitatea în raport cu obiectivele legitime urmărite;
 - Garanția C – Mecanism independent de supraveghere;
 - Garanția D – Căi de atac eficiente la dispoziția persoanelor fizice.

⁴⁴ „Aceste sancțiuni pot fi impuse entităților publice sau private, cu excepția amenzilor și a amenzilor zilnice, care nu pot fi impuse entităților publice” (considerentul 135 din proiectul de decizie).

⁴⁵ A se vedea considerentele 152-217 din proiectul de decizie.

⁴⁶ [Recomandările 02/2020 privind garanțiile esențiale europene pentru măsurile de supraveghere.](#)

3.1 Accesarea și utilizarea datelor de către autoritățile publice braziliene în scopul aplicării dreptului penal

3.1.1 Cadrul juridic în domeniul asigurării respectării dreptului penal

- (59) CEPD ia act de faptul că accesarea și utilizarea ulterioară a datelor cu caracter personal de către autoritățile braziliene de aplicare a legii⁴⁷ sunt reglementate de un sistem de acte juridice de natură juridică diferită. Protecția datelor și a vieții private, inclusiv secretul corespondenței și al comunicațiilor, sunt consacrate la articolul 5 din Constituție ca drepturi fundamentale. CEPD salută în special faptul că domeniul de aplicare al protecției acestor drepturi, la fel ca în UE, nu se limitează doar la cetățenii brazilieni, ci include și străinii care locuiesc sau nu în Brazilia⁴⁸.
- (60) În continuare, există mai multe legi sectoriale specializate care reglementează eventualul acces la datele cu caracter personal în scopul asigurării respectării legii. În ceea ce privește accesul la datele transferate din UE către Brazilia, sunt relevante în special Codul penal, Legea privind interceptarea convorbirilor telefonice, Cadrul civil pentru internet, Legea privind confidențialitatea instituțiilor financiare, Legea privind organizațiile criminale și anchetele penale și altele. CEPD ia act de faptul că aceste acte juridice sunt accesibile publicului și ar putea fi considerate suficient de clare pentru a oferi persoanelor vizate o indicație cu privire la circumstanțele și condițiile în care autoritățile publice sunt împuternicite să își acceseze datele⁴⁹.
- (61) O altă sursă importantă de drept în Brazilia este jurisprudența Curții Supreme Federale a Braziliei, care pare să aplice o interpretare largă a domeniului de aplicare al drepturilor la viață privată și la protecția datelor⁵⁰, precum și jurisprudența Curții Interamericane a Drepturilor Omului responsabilă cu interpretarea și aplicarea Convenției americane privind drepturile omului, ratificată de Brazilia în 1992⁵¹.
- (62) CEPD ia act de faptul că domeniul de aplicare al LGPD în cazul prelucrării datelor cu caracter personal pentru asigurarea respectării dreptului penal este parțial, ceea ce poate conduce la insecuritate juridică.
- (63) Astfel cum a recunoscut Comisia în proiectul de decizie, LGPD nu se aplică prelucrării datelor efectuate *exclusiv* în scopul siguranței publice, al apărării naționale, al securității statului sau al investigării și urmăririi penale a infracțiunilor⁵². În conformitate cu articolul 4 litera alineatele

⁴⁷ A se vedea lista autorităților de la considerentul 165 din proiectul de decizie.

⁴⁸ A se vedea considerentele 8 și 9 din proiectul de decizie.

⁴⁹ A se vedea Hotărârea CEDO în cauza Zakharov, punctul 229.

⁵⁰ Curtea Supremă Federală, Hotărârea privind ADI 6649, septembrie 2022.

⁵¹ A se vedea considerentul 10 din proiectul de decizie.

⁵² A se vedea considerentele 30 și 31 din proiectul de decizie.

(I) și (III) din LGPD, prelucrarea datelor în aceste domenii va fi reglementată de o legislație specifică, care trebuie să cuprindă principiile și drepturile persoanelor vizate menționate în LGPD. Din cunoștințele CEPD, confirmate de Comisie, Brazilia nu a adoptat încă o legislație specifică privind prelucrarea datelor cu caracter personal în domeniul justiției penale și al asigurării respectării legii (de exemplu, similară Directivei UE privind protecția datelor în materie de asigurare a respectării legii⁵³).

- (64) CEPD ia act cu satisfacție de faptul că Curtea Supremă Federală a Braziliei a interpretat LGPD în jurisprudența⁵⁴ sa într-un mod care a extins aplicabilitatea sa parțială la prelucrarea datelor cu caracter personal pentru anchetele penale și menținerea ordinii publice.
- (65) CEPD salută faptul că autoritatea de supraveghere din Brazilia, ANPD, sprijină pe deplin această interpretare și susține că *„absența unei legislații specifice nu acordă agențiilor de securitate o autorizație largă și nelimitată de a prelucra datele cu caracter personal ale cetățenilor în scopuri exclusive de securitate publică și de investigare și urmărire penală a infracțiunilor, fără nicio limită”*⁵⁵. În același timp, CEPD ia act de faptul că, în temeiul articolului 4 alineatul (III) punctul (3) din LGPD, pentru unele prelucrări specifice ale datelor efectuate exclusiv în scopul asigurării respectării legii, ANPD pare să aibă în prezent în principal un rol consultativ în raport cu autoritățile de aplicare a legii.
- (66) CEPD invită Comisia să evalueze suplimentar și să clarifice în proiectul de decizie aplicabilitatea LGPD în cazul prelucrării datelor cu caracter personal în scopul asigurării respectării dreptului penal, inclusiv competențele ANPD, precum și să ia în considerare cu atenție orice evoluție relevantă în acest sens în cadrul monitorizării sale viitoare (a se vedea, de asemenea, secțiunea privind supravegherea și căile de atac).

3.1.2 Necesitatea și proporționalitatea

- (67) CEPD ia act cu satisfacție de faptul că, în general, accesul la datele privind comunicațiile, atât conținutul, cât și metadatele, precum și la alte categorii de informații confidențiale protejate, cum ar fi datele bancare și fiscale, necesită o autorizație judiciară prealabilă.
- (68) În ceea ce privește accesul la datele privind comunicațiile, CEPD salută faptul că, în temeiul Legii privind interceptarea convorbirilor telefonice și al jurisprudenței Curții Supreme Federale, o astfel de măsură este considerată excepțională și face obiectul unor condiții stricte menite să asigure necesitatea și proporționalitatea acesteia⁵⁶. În plus, ca măsură preventivă împotriva eventualelor abuzuri, legislația braziliană prevede că interceptarea comunicațiilor fără

⁵³ Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului (JO L 119, 4.5.2016, p. 89).

⁵⁴ Curtea Supremă Federală, Hotărârea privind ADI 6649, septembrie 2022.

⁵⁵ A se vedea Nota tehnică ANPD nr. 29/2024/FIS/CGF/ANPD adresată Ministerului Justiției și Securității Publice, punctul 5.4.1.29, disponibilă la adresa: [SEI/ANPD - 0132350 - Nota Técnica](#).

⁵⁶ A se vedea considerentele 169 și 170 din proiectul de decizie.

autorizație judiciară sau în scopuri neautorizate de lege constituie o infracțiune pasibilă de o pedeapsă cu închisoarea de până la patru ani⁵⁷.

- (69) Punerea în aplicare strictă a garanțiilor pentru accesul la datele privind comunicațiile este deosebit de relevantă, având în vedere existența în Brazilia a unei obligații generale de păstrare a datelor pentru furnizorii de servicii de conectare la internet și de aplicații online, care trebuie să păstreze jurnalele de conectare timp de un an⁵⁸. Deși ia act cu satisfacție de faptul că accesul la datele păstrate este posibil numai sub rezerva unei autorizații judiciare⁵⁹, CEPD reamintește abordarea strictă și restricțiile privind păstrarea generalizată și nediferențiată a metadatelor privind comunicațiile în UE⁶⁰ și ia act cu satisfacție de informațiile suplimentare furnizate de Comisie în legătură cu absența păstrării în masă a datelor în țară. Prin urmare, CEPD încurajează Comisia să acorde o atenție deosebită regimului juridic și practicii din Brazilia în ceea ce privește accesul la datele privind comunicațiile în timpul monitorizării și revizuirii proiectului de decizie.
- (70) CEPD ia act cu satisfacție de faptul că se aplică garanții similare și în ceea ce privește accesul autorităților de aplicare a legii la datele fiscale și bancare, și anume cerința unei autorizații judiciare prealabile, permisă numai pentru infracțiuni grave, existența unor sancțiuni penale în caz de abuz etc.
- (71) În conformitate cu proiectul de decizie, există o excepție de la cerința generală privind autorizarea judiciară prealabilă pentru accesul autorităților de aplicare a legii la anumite categorii de date cu caracter personal⁶¹. În temeiul articolelor 15 și 16 din Legea privind organizațiile criminale și anchetele penale, un șef de poliție și Parchetul pot accesa fără autorizație judiciară datele de înregistrare ale unei persoane anchetate cu privire la: „*datele privind calificarea personală, afilierea și adresa deținute de Tribunalul Electoral, societăți de telefonie, instituții financiare, furnizori de internet și administratori de cărți de credit*”⁶². În aceeași ordine de idei, societățile de transport vor permite, pentru o perioadă de cinci ani, accesul direct și permanent al unui judecător, al Parchetului sau al șefului poliției la bazele de date cu rezervări și evidențe de călătorie⁶³.
- (72) CEPD ia act de faptul că domeniul de aplicare al Legii privind organizațiile criminale și anchetele penale se limitează la investigarea și sancționarea grupurilor infracționale organizate și a organizațiilor teroriste care prezintă un risc semnificativ pentru cetățeni și societate și, prin urmare, pot justifica o ingerință mai gravă în drepturile fundamentale la viață

⁵⁷ Ibidem.

⁵⁸ A se vedea considerentul 173 din proiectul de decizie.

⁵⁹ Ibidem.

⁶⁰ Pentru mai multe informații privind păstrarea datelor, a se vedea Declarația CEPD 5/2024 privind recomandările Grupului la nivel înalt referitoare la accesul la date pentru o aplicare eficace a legii, disponibilă la adresa https://www.edpb.europa.eu/system/files/2024-11/edpb_statement_20241104_ontherecommendationsofthehlg_en.pdf.

⁶¹ A se vedea considerentul 164 din proiectul de decizie.

⁶² A se vedea articolul 15 din Legea privind organizațiile criminale și anchetele penale.

⁶³ A se vedea articolul 16 din Legea privind organizațiile criminale și anchetele penale.

privată și la protecția datelor⁶⁴. În același timp, CEPD consideră că informațiile cu privire la aceste excepții furnizate în considerentul 164 din proiectul de decizie sunt foarte generale și incomplete. În special, din informațiile din proiectul de decizie nu reiese în mod clar dacă, într-un astfel de caz, accesul la datele cu caracter personal face obiectul unui control jurisdicțional *ex post* al necesității și proporționalității.

- (73) Având în vedere cele de mai sus, CEPD invită Comisia să clarifice și să explice în proiectul de decizie domeniul de aplicare și natura cazurilor în care accesul la date al autorităților de aplicare a legii nu necesită autorizare judiciară, precum și garanțiile aplicabile din legislația braziliană. CEPD consideră, de asemenea, că, în cursul monitorizării proiectului de decizie, Comisia ar trebui să acorde o atenție deosebită aplicării acestor excepții în temeiul legislației braziliene.

3.1.3 Utilizarea ulterioară a datelor și transferurile ulterioare

- (74) CEPD reamintește că nivelul de protecție acordat datelor cu caracter personal transferate din UE/SEE în Brazilia nu trebuie să fie subminat de utilizarea ulterioară sau de schimbul de date cu destinatarii din Brazilia sau dintr-o țară terță, și anume transferurile ulterioare ar trebui să fie permise numai în cazul în care se asigură un nivel continuu de protecție în esență echivalent cu cel prevăzut în dreptul UE.
- (75) În acest sens, CEPD ia act cu satisfacție de faptul că Curtea Supremă Federală a Braziliei a hotărât că schimbul de date cu caracter personal între organismele publice (inclusiv atunci când sunt partajate între autoritățile de aplicare a legii și serviciile de informații) presupune: (1) definirea unui scop legitim, specific și explicit pentru prelucrarea datelor; (2) compatibilitatea prelucrării cu scopurile comunicate; (3) limitarea partajării la minimul necesar pentru îndeplinirea scopului comunicat; precum și respectarea deplină a cerințelor, a garanțiilor și a procedurilor prevăzute în LGPD, în măsura în care acest lucru este compatibil cu sectorul public⁶⁵.
- (76) În pofida acestei hotărâri importante a celei mai înalte instanțe din Brazilia, având în vedere complexitatea deja menționată, domeniul de aplicare exact și modalitățile de aplicare a LGPD în cazul autorităților de aplicare a legii, CEPD invită Comisia să monitorizeze atent evoluțiile și practica în acest domeniu.
- (77) În ceea ce privește transferul ulterior de date cu caracter personal către autoritățile de aplicare a dreptului penal din țări terțe, proiectul de decizie face trimitere la articolul 33 alineatul (III) din LGPD, care stabilește că transferurile internaționale de date pot avea loc atunci când „sunt necesare pentru cooperarea juridică internațională între organismele publice de informații,

⁶⁴ A se vedea Hotărârea CJUE din 6 octombrie 2020, cauzele conexate La Quadrature du Net și alții, C-511/18 și C-512/18, EU:C:2020:791, punctele 95-98, Hotărârea din 2 octombrie 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punctele 54, 57 și 60 [Hotărârea din 2 martie 2021, Prokuratuur (Condițiile de acces la datele privind comunicațiile electronice), C-746/18, EU:C:2021:152, punctul 35].

⁶⁵ A se vedea considerentul 187 din proiectul de decizie.

anchetă și urmărire penală, în conformitate cu instrumentele juridice internaționale⁶⁶. CEPD consideră că această explicație este prea generală și invită Comisia să detalieze în proiectul de decizie condițiile și garanțiile care reglementează transferurile ulterioare.

3.1.4 Supraveghere și căi de atac

- (78) CEPD reamintește că orice ingerință în dreptul la viață privată și la protecția datelor ar trebui să facă obiectul unui sistem de supraveghere eficace, independent și imparțial, care trebuie să fie asigurat fie de un judecător, fie de un alt organism independent (de exemplu, o autoritate administrativă sau un organ parlamentar)⁶⁷.
- (79) De asemenea, ia act de faptul că, în cadrul brazilian, astfel cum este descris de Comisie, activitățile autorităților de aplicare a dreptului penal sunt supravegheate de diferite organisme: (i) sistemul judiciar; (ii) ANPD și (iii) Parchetul.
- (80) Controlul judiciar, astfel cum s-a explicat mai sus în secțiunea privind necesitatea și proporționalitatea⁶⁸, se aplică în ceea ce privește colectarea și accesul la datele cu caracter personal, în special sub forma unei revizui și autorizări *ex ante*.
- (81) În privința rolului ANPD, astfel cum s-a explicat deja în secțiunea 3.1.1 din prezentul aviz, proiectul de decizie privind caracterul adecvat al nivelului de protecție reamintește că, în conformitate cu articolul 4 alineatul (III) din LGPD, această lege nu se aplică prelucrării datelor cu caracter personal efectuate *exclusiv* în scopuri privind (i) siguranța publică; (ii) apărarea națională; (iii) securitatea statului și (iv) investigarea și urmărirea penală a infracțiunilor. În plus, articolul 4 alineatul (I) prevede că o astfel de prelucrare va fi reglementată de o legislație specifică, care, printre altele, trebuie să cuprindă principiile generale de protecție și drepturile persoanelor vizate, astfel cum sunt prevăzute în LGPD. Punctul (3) din același articol recunoaște că ANPD are un rol consultativ în ceea ce privește excepțiile prevăzute la alineatul (III) atunci când se desfășoară exclusiv în aceste scopuri, în special competențele ANPD de a emite avize și recomandări tehnice, precum și de a solicita DPIA din partea operatorilor relevanți.
- (82) În proiectul său de decizie⁶⁹, Comisia face trimitere la o decizie importantă din 15 septembrie 2022 a Curții Supreme Federale, care indică aplicabilitatea principiilor generale de protecție a datelor și a drepturilor persoanelor vizate în ceea ce privește prelucrarea datelor cu caracter personal de către stat pentru furnizarea de servicii publice. Această decizie se axează pe „schimbul de date cu caracter personal” între organismele și entitățile administrației publice și în activitățile de informații, precum și pe „accesul agenților și entităților

⁶⁶ Ibidem.

⁶⁷ Recomandările 02/2020 privind garanțiile esențiale europene pentru măsurile de supraveghere, adoptate la 10 noiembrie 2020; a se vedea pagina 12

https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_ro.pdf.

⁶⁸ A se vedea secțiunea 3.1.2 de mai sus.

⁶⁹ A se vedea considerentul 187 din proiectul de decizie.

guvernamentale” la registrul de bază al cetățenilor. În ceea ce privește rolul ANPD de asigurare a respectării legislației, CEPD înțelege din informațiile suplimentare furnizate de Comisie că ANPD a exercitat deja un astfel de rol în raport cu poliția, precum și cu Ministerul Justiției și Securității Publice. Acest lucru s-a realizat pe baza jurisprudenței potrivit căreia, prin extinderea aplicabilității parțiale a principiilor generale și a drepturilor persoanelor vizate la prelucrarea efectuată în scopul asigurării respectării legii, ANPD este responsabilă și de supravegherea și aplicarea legii în acest domeniu.

- (83) Având în vedere cele de mai sus, CEPD invită Comisia să detalieze în continuare rolul ANPD în materie de asigurare a respectării legii, în special în ceea ce privește temeiurile juridice relevante și competențele sale de investigare și corective față de autoritățile de aplicare a legii, și să monitorizeze atent evoluțiile din acest domeniu.
- (84) În sfârșit, CEPD observă că Parchetul are o competență mai amplă decât supravegherea normelor privind protecția datelor și a vieții private și impunerea de sancțiuni pentru încălcarea drepturilor fundamentale. De exemplu, astfel cum s-a explicat deja în secțiunea 3.1 din prezentul aviz, în temeiul Legii privind organizațiile criminale și anchetele penale, Parchetul este una dintre autoritățile care pot accesa fără autorizație judiciară datele de înregistrare ale unei persoane anchetate. Prin urmare, CEPD invită Comisia să detalieze și să explice în proiectul de decizie rolul și competențele Parchetului în ceea ce privește supravegherea prelucrării datelor cu caracter personal de către autoritățile braziliene de aplicare a legii.
- (85) În ceea ce privește căile de atac, CEPD ia act cu satisfacție de faptul că mecanismele juridice descrise în prima parte a prezentului aviz și, în special, căile de atac judiciare aflate la dispoziția persoanelor fizice pentru a-și exercita drepturile la protecția datelor și la viață privată se aplică și în ceea ce privește activitățile organismelor de asigurare a respectării dreptului penal.

3.2 Accesarea și utilizarea datelor de către autoritățile publice din Brazilia în scopuri legate de securitatea națională

3.2.1 Domeniul de aplicare al derogării de la articolul 4 alineatul (III) din LGPD și aplicabilitatea acesteia în cazul infracțiunilor împotriva securității statului

- (86) Astfel cum a fost introdus de Comisie, articolul 4 alineatul (III) din LGPD exceptează „securitatea statului” de la aplicarea LGPD în cazul prelucrării datelor cu caracter personal, alături de securitatea publică, apărarea națională și activitățile de investigare și urmărire penală a infracțiunilor.

- (87) CEPD ia act de faptul că legislația braziliană privind „*Seguranca Nacional*” (securitatea națională), astfel cum este prevăzută în Legea nr. 14197 din 1 septembrie 2021 de modificare a Codului penal și de revocare a Legii din 1983 privind securitatea națională⁷⁰, exprimă conceptul brazilian de „securitate națională” pe baza unei liste exhaustive de infracțiuni⁷¹, care abordează diferite amenințări la adresa integrității statului brazilian ca instituție [suveranitatea națională, spionajul (articolul 350-K), infracțiunile împotriva instituțiilor democratice (articolul 359-L) et al.]. Normele Legii nr. 14197 au fost stabilite ca parte integrantă a Codului penal brazilian.
- (88) Acestea fiind spuse, CEPD se așteaptă ca prelucrarea datelor de către autoritățile braziliene pentru urmărirea penală a infracțiunilor prevăzute în Legea nr. 14197 să fie reglementată de regimul aplicabil accesului și utilizării autorităților braziliene în scopul asigurării respectării dreptului penal, astfel cum se descrie în capitolul 3.2 din proiectul de decizie, fiind astfel supusă aceluiași considerente privind protecția datelor ca cele menționate în capitolul 3.1 din prezentul aviz. Prin urmare, CEPD solicită Comisiei să clarifice în proiectul de decizie dacă prelucrarea datelor referitoare la urmărirea penală a infracțiunilor enumerate în Legea nr. 14197 este într-adevăr reglementată de regimul de protecție a datelor aplicabil activităților de asigurare a respectării legii sau de un alt regim. În acest din urmă caz, CEPD invită Comisia să explice în continuare normele de protecție a datelor aplicabile urmării penale a acestor infracțiuni în scopul securității naționale.

3.2.2 Cadrul juridic pentru securitatea națională

- (89) Cadrul juridic codificat pe care se bazează proiectul de decizie în capitolul său privind accesul guvernului în „scopuri de securitate națională” constă în Legea nr. 14197 din 2021, Legea nr. 9883 din 7 decembrie 1999 de instituire a sistemului brazilian de informații și Decretul conex nr. 4376 din 2002. Ultimele două acte legislative menționate au instituit sistemul brazilian de informații [*Sistema Brasileiro des Inteligência* (SISBIN)] și funcționarea acestuia. Acestea sunt urmate de Decretul prezidențial cu caracter obligatoriu nr. 8793⁷² din 2016, care definește politica națională de informații [așa-numita *Política Nacional de Inteligência* (PNI)], precum și LGPD în 2018.
- (90) Decretul prezidențial nr. 8793 din 2016 descrie subiectul, obiectivele și limitele PNI. Activitățile prevăzute în acest decret au ca scop producerea și diseminarea către autoritățile competente a informațiilor referitoare la fapte și situații care au loc pe teritoriul național sau în afara acestuia, cu o influență imediată sau potențială asupra procesului decizional, a acțiunii guvernamentale și a siguranței societății și a informațiilor de stat. În aceste condiții, „informațiile” se referă la toate informațiile – și datele – necesare și prelucrate pentru a sprijini procesul decizional al ramurii executive în acest domeniu.

⁷⁰ Legea nr. 14197 din 1 septembrie 2021, disponibilă la adresa https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14197.htm (02.10.2026).

⁷¹ A se vedea considerentul 200 din proiectul de decizie.

⁷² A se vedea considerentul 199 din proiectul de decizie.

- (91) În conformitate cu temeiul juridic al SISBIN, astfel cum a fost prezentat de Comisie, SISBIN și entitățile sale au fost instituite ca mecanism de bază pentru punerea în aplicare a PNI și, ca atare, au sarcina de a desfășura activități legate de domeniul securității naționale, precum și de siguranța și securitatea publică și de protecția instituțiilor democratice. În acest scop, SISBIN prevede schimbul de cunoștințe și planificarea integrată a activităților⁷³. În consecință, conceptul de securitate națională în Brazilia, având în vedere activitățile SISBIN, pare să nu se limiteze doar la infracțiunile codificate în Legea nr. 14197, ci ar putea fi considerat parte integrantă a unui concept mai larg de informații naționale.
- (92) SISBIN, astfel cum a fost înființat inițial, era compus din optsprezece entități federale, printre care treisprezece ministere, și ulterior extins la 48 de așa-numite agenții în temeiul Decretului nr. 11693 din 6 septembrie 2023 privind organizarea și funcționarea SISBIN⁷⁴. CEPD ia act de faptul că cooperarea în cadrul SISBIN integrează și alte entități decât instituțiile tradiționale de securitate, cum ar fi Ministerul Științei [articolul 4 alineatul (IV)], Ministerul Agriculturii [articolul 4 alineatul (XV)] și Ministerul Energiei [articolul 4 alineatul (XVIII)] și Procurorul general federal [articolul 4 alineatul (XIX)].
- (93) Întrucât prin Decretul nr. 4376 din 2002 s-a solicitat Consiliului consultativ al sistemului brazilian de informații să propună standarde și proceduri generale pentru schimbul de „cunoștințe și comunicații” în cadrul SISBIN⁷⁵, prin Decretul nr. 11693 din 2023 se desemnează organul central al SISBIN pentru producerea de instrumente tehnice⁷⁶ destinate schimbului de informații și cunoștințe și se descrie schimbul și utilizarea datelor obținute de entitățile SISBIN. Cu toate acestea, proiectul de decizie al Comisiei nu furnizează informații suplimentare cu privire la astfel de norme sau standarde juridice emise de organul central, de exemplu atunci când entitățile SISBIN fac schimb de date cu caracter personal între acestea.
- (94) În plus, par să existe diferențe în ceea ce privește conceptele de sensibilitate a informațiilor, având în vedere că, în temeiul legislației relevante care reglementează activitățile SISBIN, sensibilitatea este legată de gradul de confidențialitate acordat unor informații⁷⁷ și de limitarea scopului în raport cu principiile generale ale RGPD⁷⁸.
- (95) Astfel cum s-a explicat deja mai sus, articolul 4 alineatul (III) literele (a)-(c) din LGPD, care a fost codificat numai după instituirea SISBIN și stabilirea unei politici naționale privind informațiile, exceptează de la aplicarea LGPD activitățile de prelucrare a datelor desfășurate exclusiv în scopul siguranței publice, al apărării naționale și al securității statului, cu excepția principiilor generale stabilite în materie de protecție a datelor.

⁷³ Decretul prezidențial nr. 8793, secțiunea 5, denumirile SISBIN și organele integrate în acesta, schimbul de cunoștințe în cadrul SISBIN și planificarea integrată a cooperării dintre membrii SISBIN ca instrumente pentru realizarea PNI.

⁷⁴ A se vedea considerentul 202 din proiectul de decizie.

⁷⁵ A se vedea articolul 7 alineatul (II) din Decretul nr. 4.376.

⁷⁶ A se vedea articolul 10 alineatul (XI), disponibil la adresa https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11693.htm (26.9.2025).

⁷⁷ A se vedea Decretul nr. 8793 din 2016, Decretul nr. 11693, considerentul 204 din proiectul de decizie.

⁷⁸ A se vedea articolul 6 alineatul (I) din LGPD, care se referă la scopuri legitime și specifice, în timp ce RGPD prevede scopuri legale și specifice.

- (96) Astfel cum a subliniat Comisia în proiectul de decizie, cadrul general al Constituției Braziliei, precum și participarea Braziliei la Curtea Interamericană a Drepturilor Omului se referă la cadrul juridic pentru accesul guvernului la serviciile de informații naționale. CEPD recunoaște, de asemenea, că și hotărârile Curții Supreme Federale din Brazilia au jucat un rol important în definirea peisajului juridic⁷⁹. Până în prezent, hotărârile Curții Supreme au reprezentat un sprijin concis și relevant pentru dezvoltarea suplimentară a protecției datelor cu caracter personal în conformitate cu Constituția Braziliei. În același timp, trebuie remarcat faptul că hotărârile Curții Supreme nu precizează și nici nu stabilesc norme generale abstracte de protecție a datelor pentru prelucrarea datelor cu caracter personal, ci interpretează dispozițiile și principiile Constituției și ale LGPD.
- (97) CEPD este conștient de faptul că statelor li se acordă o marjă largă de apreciere în definirea aspectelor de securitate națională, ceea ce permite apoi derogări în materie de securitate națională în ceea ce privește prelucrarea datelor cu caracter personal. În acest context, reamintește definiția dată de Curtea Europeană a Drepturilor Omului, potrivit căreia amenințările la adresa securității naționale trebuie să se distingă prin natura lor, gravitatea lor și circumstanțele specifice de riscurile generale pentru siguranța publică sau de infracțiunile grave⁸⁰.
- (98) CEPD înțelege că datele prelucrate de entitățile SISBIN beneficiază de derogarea prevăzută la articolul 4 alineatul (III) din LGPD numai atunci când prelucrarea este efectuată *exclusiv* în scopuri legate de siguranța publică, apărarea națională și securitatea statului. Acest lucru pare să se aplice în mod specific activităților organismului central al SISBIN, Agenția braziliană de informații (ABIN). În consecință, cu excepția cazului în care o entitate a SISBIN acționează în numele ABIN în unul dintre aceste scopuri, LGPD se aplică integral.
- (99) CEPD invită Comisia să confirme această înțelegere și să descrie și să explice mai precis în proiectul de decizie prezentarea conceptului de securitate națională în temeiul legislației braziliene, în special în ceea ce privește colectarea și schimbul de date între și de către entități în numele activităților SISBIN, precum și în ceea ce privește punerea în aplicare a PNI. În acest sens, CEPD invită Comisia să clarifice, de asemenea, modul în care derogările de la LGPD în scopuri de securitate națională se referă la derogarea pentru securitatea națională în temeiul RGPD.

3.2.3 Transferuri ulterioare și acorduri internaționale

- (100) Articolul 33 din LGPD definește condițiile prealabile pentru transferul internațional de date. Articolul 33 alineatele (I) și (II) din LGPD stabilește cerințe similare unei decizii privind caracterul adecvat al nivelului de protecție sau cerințe pentru garanții suplimentare în temeiul RGPD. Aceste cerințe sunt eliminate în articolul 33 alineatele (III), (VI) și (VII) din LGPD, care abordează cazurile de „cooperare juridică între serviciile de informații”, transferurile care

⁷⁹ A se vedea considerentul 203 din proiectul de decizie.

⁸⁰ CEDO, Big Brother Watch și alții/Regatul Unit, 25 mai 2021, punctul 350.

răspund „unui angajament asumat în cadrul acordurilor de cooperare internațională” și transferurile „necesare pentru aplicarea unei politici publice sau a unei atribuții juridice a serviciului public”, și anume securitatea națională și serviciile de informații naționale. Această decizie pare să fie în conformitate cu conceptul de la articolul 4 alineatul (III) din LGPD, care limitează aplicarea LGPD numai la principiile sale în materie de siguranță publică, apărare națională și siguranță de stat. Astfel, s-ar putea considera că transferurile ulterioare în scopuri legate de informațiile naționale ar trebui efectuate în conformitate cu principiile generale ale protecției datelor prevăzute în LGPD, fiind în același timp supuse dispozițiilor privind cooperarea internațională prevăzute în actele juridice de instituire a PNI și SISBIN.

- (101) Acestea fiind spuse, CEPD recunoaște că Brazilia poate avea nevoie și chiar transmite date cu caracter personal serviciilor externe de informații în scopul cooperării sau al punerii în aplicare a PNI în conformitate cu obiectivul de a preveni și de a identifica amenințările pe baza conceptului integrat de securitate menționat mai sus.
- (102) Astfel cum s-a menționat anterior, Comisia subliniază aplicabilitatea cadrului general al Constituției Braziliei și garantarea „habeas data” pentru protecția datelor cu caracter personal în cadrul SISBIN, care se aplică și transferurilor ulterioare în scopul securității naționale. CEPD invită Comisia să clarifice în continuare temeiul juridic și garanțiile și condițiile în materie de protecție a datelor pe care ABIN și ceilalți membri ai SISBIN sunt obligați să le ia în considerare înainte de a divulga date cu caracter personal partenerilor străini în scopuri legate de serviciile de informații naționale.
- (103) CEPD ia act, de asemenea, de faptul că Comisia nu a integrat considerații privind existența acordurilor internaționale încheiate între Brazilia și țări terțe sau organizații internaționale în evaluarea sa privind caracterul adecvat al nivelului de protecție. Întrucât LGPD nu prevede o legislație obligatorie dincolo de principiile generale de protecție a datelor, astfel de acorduri ar putea conține dispoziții specifice pentru transferul internațional de date cu caracter personal deținute de ABIN sau de ceilalți membri ai SISBIN către țări terțe. CEPD consideră că încheierea de acorduri bilaterale sau multilaterale cu țări terțe în scopul cooperării în materie de informații ar putea afecta cadrul juridic privind protecția datelor, astfel cum a fost evaluat.
- (104) Prin urmare, CEPD invită Comisia să clarifice dacă există astfel de acorduri internaționale în scopuri legate de serviciile naționale de informații și să evalueze impactul potențial al acestora asupra nivelului de protecție acordat datelor cu caracter personal transferate din SEE către Brazilia în ceea ce privește cadrul juridic evaluat în principal pentru prelucrarea datelor în scopuri legate de informațiile naționale.

3.2.4 Supraveghere și căi de atac

- (105) Proiectul de decizie privind caracterul adecvat al nivelului de protecție prezintă diferite organisme care supraveghează activitățile autorităților braziliene responsabile cu securitatea națională, în special (i) ramura executivă, (ii) ramura legislativă; (iii) ANPD; și (iv) sistemul

judiciar. În ceea ce privește ANPD, CEPD reamintește examinarea și concluziile formulate în secțiunea 3.1.4 din prezentul aviz, care rămân valabile și în acest caz.

- (106) Conform proiectului de decizie, Camera pentru Relații Externe și Apărare Națională a Consiliului Guvernului este responsabilă de supravegherea punerii în aplicare a Poliției Naționale a Informațiilor, iar Oficiul pentru Securitate Instituțională este responsabil de coordonarea activității serviciilor federale de informații. CEPD ia act de faptul că acest control se referă numai la asigurarea faptului că obiectivele care trebuie atinse de sistemul de informații și la punerea lor în aplicare, dar nu include nicio competență de investigare sau de sancționare și nu acoperă prelucrarea efectivă a datelor cu caracter personal.
- (107) De fapt, Comisia mixtă pentru controlul activităților de informații (CCAI) (ramura legislativă) este cea care exercită controlul asupra activităților de informații, incluzând legitimitatea și eficacitatea acestora. CEPD salută faptul că structura și competențele CCAI au fost consolidate, sporind transparența activităților sale și permițând organismului să exercite un control adecvat, cum ar fi efectuarea de analize post-hoc, audituri și controale ale operațiunilor în curs. De asemenea, CEPD ia act cu satisfacție de faptul că CCAI poate trata plângerile persoanelor vizate ca parte a competenței sale de a investiga plângerile cu privire la încălcări ale drepturilor fundamentale și ale garanțiilor fundamentale.
- (108) Competența sistemului judiciar de a soluționa cauzele introduse de cetățeni împotriva autorităților publice este un aspect pozitiv, în special deoarece permite supravegherea judiciară a activităților desfășurate în numele securității naționale, asigurând respectarea, printre altele, a drepturilor constituționale (inclusiv a dreptului la protecția datelor) și a LGPD. CEPD ia act cu satisfacție de faptul că este prevăzută posibilitatea de a introduce o cale de atac prin intermediul Curții Supreme Federale și, în cele din urmă, prin intermediul Curții Interamericane a Drepturilor Omului.
- (109) CEPD înțelege că, în contextul activităților naționale de informații, persoanelor vizate li se oferă (i) drepturile consacrate în LGPD (ca urmare a hotărârii Curții Supreme Federale din 15 septembrie 2022); (ii) dreptul de a obține acces la datele cu caracter personal și de a le rectifica prin calea de atac constituțională „habeas data”; precum și (iii) dreptul la despăgubiri pentru daune materiale și morale.
- (110) CEPD salută existența unor astfel de drepturi și faptul că acestea pot fi invocate prin mecanisme judiciare și administrative, în special CCAI, precum și faptul că aceste căi de atac sunt accesibile tuturor persoanelor, indiferent de cetățenie.

4. PUNEREA ÎN APLICARE ȘI MONITORIZAREA PROIECTULUI DE DECIZIE

- (111) În ceea ce privește monitorizarea și revizuirea proiectului de decizie, CEPD ia act de faptul că, în conformitate cu jurisprudența CJUE, „având în vedere că nivelul de protecție asigurat de o țară terță este susceptibil să evolueze, revine Comisiei, după adoptarea unei decizii [privind caracterul adecvat al nivelului de protecție în temeiul articolului 45 din RGPD] sarcina de a verifica în mod periodic dacă constatarea referitoare la nivelul de protecție adecvat asigurat de țara terță în cauză este în continuare justificată în fapt și în drept. O astfel de verificare se impune, în orice caz, atunci când există indicii care dau naștere unei îndoieli în această privință”⁸¹.
- (112) CEPD ia act de faptul că revizuirea constatării privind caracterul adecvat al nivelului de protecție va avea loc cel puțin o dată la patru ani, în conformitate cu articolul 45 alineatul (3) din RGPD⁸².
- (113) CEPD salută faptul că proiectul de decizie prevede, la considerentul 230, participarea CEPD la reuniunea organizată între Comisie și autoritățile braziliene și dedicată revizuirii funcționării deciziei privind caracterul adecvat al nivelului de protecție. În ceea ce privește implicarea practică a CEPD și a reprezentanților săi în pregătirea și desfășurarea revizuirilor periodice viitoare, CEPD reiterează că orice documentație relevantă, inclusiv corespondența, ar trebui comunicată în scris CEPD cu suficient timp înainte de desfășurarea revizuirilor.

Pentru Comitetul European pentru Protecția Datelor,
Președinte

(Anu Talus)

⁸¹ Hotărârea Schrems I a CJUE, punctul 76. A se vedea, de asemenea, articolul 3 alineatul (4) din proiectul de decizie.

⁸² A se vedea considerentul 229 și articolul 3 alineatul (4) din proiectul de decizie.