



# **Parere 28/2025 sul progetto di decisione di esecuzione della Commissione europea a norma del regolamento (UE) 2016/679 sul livello di protezione adeguato dei dati personali da parte del Brasile**

Versione 1.0

Adottato il 04 November 2025

Translations proofread by EDPB Members.

This language version has not yet been proofread.

# Sintesi

Il 5 settembre 2025 la Commissione europea ha avviato il processo per l'adozione del progetto di decisione di esecuzione ("progetto di decisione") sul livello di protezione adeguato dei dati personali da parte della Repubblica federativa del Brasile ("Brasile").

Il 5 settembre 2025 la Commissione europea ha chiesto il parere del Comitato europeo per la protezione dei dati ("EDPB"). La valutazione dell'EDPB relativa all'adeguatezza del livello di protezione garantito dal Brasile è stata effettuata sulla base dell'esame del progetto di decisione stesso e dell'analisi della documentazione disponibile al pubblico sui siti web ufficiali delle autorità brasiliane.

L'EDPB si è concentrato sulla valutazione sia degli aspetti generali del GDPR contenuti nel progetto di decisione sia sull'accesso da parte delle autorità pubbliche ai dati personali trasferiti dal SEE per finalità di contrasto e di sicurezza nazionale, compresi i mezzi di ricorso a disposizione delle persone fisiche nel SEE. L'EDPB ha inoltre valutato l'esistenza e l'efficacia delle garanzie previste dal quadro giuridico brasiliano.

L'EDPB ha utilizzato come riferimento principale per questo lavoro i criteri di riferimento per l'adeguatezza adottati il 28 novembre 2017 dal gruppo di lavoro "Articolo 29"<sup>2</sup>, nella versione più recente rivista e adottata il 6 febbraio 2018 dall'EDPB ("criteri di riferimento per l'adeguatezza"), e le raccomandazioni 02/2020 dell'EDPB relative alle garanzie essenziali europee per le misure di sorveglianza.

L'EDPB nota con soddisfazione che in Brasile il quadro per la protezione dei dati, in particolare la legge generale sulla protezione dei dati ("LGPD"), unitamente ai decreti presidenziali e ai regolamenti vincolanti emanati dall'autorità per la protezione dei dati del Brasile (*Autoridade Nacional de Proteção de Dados*, ANPD), stabiliscono requisiti (anche in relazione ai principi, ai diritti degli interessati, ai trasferimenti, alla vigilanza e ai mezzi di ricorso) che sono strettamente allineati al GDPR e alla giurisprudenza della Corte di giustizia dell'Unione europea ("CGUE").

L'EDPB ha inoltre concluso che la Commissione europea dovrebbe chiarire nel progetto di decisione alcuni aspetti del quadro giuridico del Brasile e monitorarne attentamente gli sviluppi.

Per quanto riguarda il principio di responsabilizzazione e i requisiti relativi alla valutazione d'impatto sulla protezione dei dati, l'EDPB ritiene importante l'obbligo di effettuarla nei casi in cui il trattamento possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche e che la valutazione d'impatto sulla protezione dei dati comprenda la valutazione della necessità e della proporzionalità del trattamento. L'EDPB invita pertanto la Commissione europea a monitorare l'attuazione pratica di tali requisiti.

<sup>1</sup> Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

<sup>2</sup> Gruppo di lavoro "Articolo 29", WP 254 rev.01, adottato il 28 novembre 2017 e successivamente rivisto e adottato il 6 febbraio 2018, approvato dall'EDPB.

La LGPD prevede, in determinati casi, una limitazione alla fornitura di informazioni agli interessati o all'autorità di controllo sulla base del "segreto commerciale e industriale". Tenendo conto dell'importanza dei requisiti di trasparenza affinché gli interessati possano controllare il modo in cui vengono trattati i loro dati, nonché dell'importanza degli obblighi di cooperazione con l'autorità di controllo, in particolare per fornire le informazioni necessarie alle sue funzioni di controllo, l'EDPB invita la Commissione europea a monitorare l'attuazione di tali limitazioni nella pratica per comprenderne meglio l'impatto sui diritti di informazione e di accesso, nonché sui poteri dell'ANPD, se del caso.

Per quanto riguarda le norme sui trasferimenti successivi, l'EDPB invita la Commissione europea a chiarire nel progetto di decisione se i trasferimenti possono essere effettuati conformemente a condizioni equivalenti a quelle di cui all'articolo 49 GDPR solo in circostanze eccezionali in cui non è possibile ricorrere ad altri strumenti di trasferimento. La Commissione è inoltre invitata a chiarire se gli interessati siano informati in merito a: i possibili rischi del trasferimento quando questo si basa sul loro consenso e sulle circostanze del trasferimento (durata e finalità del trasferimento, paesi di destinazione, responsabilità delle parti coinvolte, diritti degli interessati e mezzi per esercitarli), indipendentemente dallo strumento di trasferimento utilizzato.

L'EDPB invita inoltre la Commissione europea ad approfondire ulteriormente i compiti del consiglio nazionale per la protezione dei dati personali e della vita privata e la sua interazione con l'ANPD.

Per quanto riguarda l'accesso e l'uso da parte di autorità pubbliche brasiliane dei dati personali trasferiti verso titolari e responsabili del trattamento in Brasile per finalità di contrasto penale e di sicurezza nazionale ("accesso da parte di pubbliche amministrazioni"), l'EDPB osserva che la LGPD non si applica al trattamento dei dati effettuato *esclusivamente* a fini di pubblica sicurezza, difesa nazionale, sicurezza dello Stato o indagine e perseguimento di reati. Allo stesso tempo, l'EDPB nota con soddisfazione che la Corte suprema federale del Brasile, nella sua giurisprudenza, ha interpretato la LGPD in modo da estenderne l'applicabilità parziale al trattamento dei dati personali per le indagini penali e il mantenimento dell'ordine pubblico.

Alla luce di ciò, invita la Commissione a valutare ulteriormente e chiarire nel progetto di decisione l'applicabilità della LGPD in caso di trattamento dei dati personali per motivi di contrasto penale, anche per quanto riguarda i poteri di indagine e correttivi dell'ANPD rispetto alle autorità di contrasto, nonché a prendere attentamente in considerazione qualsiasi sviluppo rilevante al riguardo nell'ambito del suo obbligo di monitoraggio.

L'EDPB, consapevole del fatto che agli Stati è concesso un ampio margine di discrezionalità nella definizione delle questioni di sicurezza nazionale, che consente quindi esenzioni per motivi di sicurezza nazionale nel trattamento dei dati personali, invita la Commissione a descrivere e spiegare in modo più preciso nel progetto di decisione i contorni della nozione di sicurezza nazionale ai sensi del diritto brasiliano. A tale proposito, l'EDPB invita la Commissione a chiarire ulteriormente in che modo le esenzioni dalla LGPD per motivi di sicurezza nazionale si rapportano alla raccolta e alla condivisione di dati tra gli enti pubblici nell'ambito del sistema di intelligence brasiliano (SISBIN).

# Indice

|                                                                                                                                          |           |
|------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>1. INTRODUZIONE .....</b>                                                                                                             | <b>5</b>  |
| <b>2. ASPETTI GENERALI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI .....</b>                                                             | <b>6</b>  |
| 2.1 Responsabilizzazione e governance dei dati .....                                                                                     | 6         |
| 2.2 Ambito di applicazione e definizioni.....                                                                                            | 7         |
| 2.2.1 Ambito di applicazione materiale e territoriale della LGPD .....                                                                   | 7         |
| 2.2.2 Definizioni .....                                                                                                                  | 8         |
| 2.3 Principi della protezione dei dati e basi giuridiche .....                                                                           | 8         |
| 2.3.1 Principi del trattamento .....                                                                                                     | 8         |
| 2.3.2 Misure di sicurezza e violazioni .....                                                                                             | 10        |
| 2.3.3 Liceità del trattamento.....                                                                                                       | 10        |
| 2.4 Diritti delle persone fisiche.....                                                                                                   | 11        |
| 2.5 Limitazioni ai trasferimenti successivi.....                                                                                         | 11        |
| 2.6 Meccanismi di procedura e applicazione.....                                                                                          | 13        |
| 2.6.1 Vigilanza indipendente.....                                                                                                        | 14        |
| 2.6.2 Ricorso.....                                                                                                                       | 15        |
| 2.6.3 Sanzioni .....                                                                                                                     | 15        |
| <b>3. ACCESSO E USO DEI DATI PERSONALI TRASFERITI DALL'UNIONE EUROPEA<br/>DA PARTE DI AUTORITÀ PUBBLICHE IN BRASILE .....</b>            | <b>16</b> |
| 3.1 Accesso e uso da parte delle autorità pubbliche brasiliane per motivi di contrasto<br>penale.....                                    | 16        |
| 3.1.1 Quadro giuridico in materia contrasto penale .....                                                                                 | 16        |
| 3.1.2 Necessità e proporzionalità.....                                                                                                   | 18        |
| 3.1.3 Ulteriore utilizzo dei dati e trasferimenti successivi.....                                                                        | 19        |
| 3.1.4 Vigilanza e mezzi di ricorso .....                                                                                                 | 20        |
| 3.2 Accesso e uso da parte delle autorità pubbliche brasiliane per finalità di sicurezza<br>nazionale .....                              | 21        |
| 3.2.1 Ambito dell'esenzione di cui all'articolo 4, punto III, LGPD e sua applicabilità ai<br>reati contro la sicurezza dello Stato ..... | 21        |
| 3.2.2 Quadro giuridico per la sicurezza nazionale .....                                                                                  | 22        |
| 3.2.3 Trasferimenti successivi e accordi internazionali.....                                                                             | 24        |
| 3.2.4 Vigilanza e mezzi di ricorso .....                                                                                                 | 24        |
| <b>4. ATTUAZIONE E MONITORAGGIO DEL PROGETTO DI DECISIONE .....</b>                                                                      | <b>25</b> |

## **Il Comitato europeo per la protezione dei dati**

visto l'articolo 70, paragrafo 1, lettera s), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE ("GDPR"),

visto l'accordo sullo Spazio economico europeo ("SEE"), in particolare l'allegato XI e il protocollo 37, modificato dalla decisione del comitato misto SEE n. 154/2018, del 6 luglio 2018<sup>3</sup>,

visti gli articoli 12 e 22 del proprio regolamento interno,

**HA ADOTTATO IL SEGUENTE PARERE:**

---

<sup>3</sup> Ai fini del presente parere per "Stati membri" si intendono gli "Stati membri del SEE".

# 1. INTRODUZIONE

- (1) Il capo V GDPR stabilisce le condizioni per i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale. I trasferimenti di dati personali possono avvenire sulla base di una decisione di adeguatezza della Commissione europea (articolo 45 GDPR) o, in mancanza di tale decisione, se il titolare del trattamento o il responsabile del trattamento fornisce garanzie adeguate, compresi diritti azionabili e mezzi di ricorso per l'interessato (articolo 46 GDPR). In mancanza di una decisione di adeguatezza o di garanzie adeguate, il trasferimento o un complesso di trasferimenti verso un paese terzo o un'organizzazione internazionale avviene solo a determinate condizioni (articolo 49 GDPR).
- (2) L'EDPB ricorda che le decisioni di adeguatezza riconoscono la protezione continua dei dati personali trasferiti dal SEE verso paesi terzi o organizzazioni internazionali e costituiscono un solido strumento di trasferimento per garantire la tutela dei diritti dell'interessato quando i dati sono trasferiti al di fuori del SEE. Secondo i criteri di riferimento per l'adeguatezza<sup>4</sup> e la pertinente giurisprudenza della CGUE<sup>5</sup>, sebbene il paese terzo non sia tenuto a garantire un livello di protezione identico a quello garantito nell'ordinamento giuridico dell'UE, l'espressione "livello di protezione adeguato" di cui all'articolo 45, paragrafo 1, GDPR, deve essere intesa nel senso che esige che tale paese assicuri effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione delle libertà e dei diritti fondamentali sostanzialmente equivalente a quello garantito all'interno dell'Unione, letta alla luce della Carta dei diritti fondamentali.
- (3) Il Brasile è una Repubblica federativa composta dall'unione di 26 Stati e un Distretto federale, come stabilito nella sua costituzione federale ("costituzione")<sup>6</sup>. Anche gli Stati brasiliani hanno le proprie costituzioni, che non devono essere in contrasto con la costituzione federale. La vita privata e la protezione dei dati sono tutelate dalla costituzione in quanto diritti fondamentali (articolo 5, punti X, XII, e LXXIX della costituzione)<sup>7</sup> e riconosciute dalla Corte costituzionale per tutte le persone fisiche, compresi gli stranieri, indipendentemente dal fatto che tali persone siano residenti in Brasile<sup>8</sup> o meno.
- (4) Il principale atto normativo che disciplina la protezione dei dati è la legge generale sulla protezione dei dati o *Lei Geral de Proteção de Dados* ("LGPD") (n. 13.709 del 14 agosto 2018, da ultimo modificata dalla legge n. 14.460 del 25 ottobre 2022). La LGPD è integrata dai decreti vincolanti (decreto presidenziale n. 10.474 del 26 agosto 2020 e decreto presidenziale n. 11.758 del 30 ottobre 2023), che sono giuridicamente vincolanti e aventi efficacia esecutiva<sup>9</sup>.
- (5) Oltre alla LGPD, il quadro per la protezione dei dati brasiliano comprende regolamenti vincolanti emanati dall'autorità per la protezione dei dati del Brasile (*Agencia Nacional de Proteção de Dados*, "ANPD")<sup>10</sup>. Tali regolamenti forniscono ulteriori norme sull'interpretazione

<sup>4</sup> Gruppo di lavoro "Articolo 29", WP 254 rev.01, adottato il 28 novembre 2017 e successivamente rivisto e adottato il 6 febbraio 2018, approvato dall'EDPB, capitolo 3, C.

<sup>5</sup> Sentenza della Corte di giustizia del 6 ottobre 2015, *Maximillian Schrems/Data Protection Commissioner* ("Schrems"), C-362/14, e sentenza del Tribunale del 3 settembre 2025, *Philippe Latombe/Commissione europea* ("Latombe"), T-553/23.

<sup>6</sup> Cfr. il considerando 7 del progetto di decisione.

<sup>7</sup> Cfr. il considerando 8 del progetto di decisione.

<sup>8</sup> Cfr. il considerando 9 del progetto di decisione.

<sup>9</sup> Cfr. i considerando 11 e 12 del progetto di decisione.

<sup>10</sup> Tutti i regolamenti vincolanti emanati dall'ANPD sono disponibili all'indirizzo: [https://www.gov.br/anpd/pt-br/aceso-a-informacao/institucional/atos-normativos/regulamentacoes\\_anpd](https://www.gov.br/anpd/pt-br/aceso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd).

e sull'applicazione della LGPD<sup>11</sup>. Ad esempio, il regolamento n. 4 del 24 febbraio 2024 sull'applicazione delle sanzioni amministrative, il regolamento n. 15 del 24 aprile 2024 sulla notifica degli incidenti di sicurezza ("regolamento sulla notifica degli incidenti di sicurezza"), il regolamento n. 19 del 23 agosto 2024 sul trasferimento internazionale dei dati personali ("regolamento sul trasferimento dei dati"), il regolamento n. 2 del 27 gennaio 2022 sull'applicazione della LGPD alle piccole e medie imprese, il regolamento n. 18 del 15 luglio 2024 sul ruolo del responsabile della protezione dei dati ("regolamento RPD").

- (6) L'EDPB accoglie con favore il riconoscimento costituzionale dei diritti alla vita privata e alla protezione dei dati quali diritti fondamentali, ulteriormente attuati tramite la legislazione nazionale. L'EDPB nota inoltre con soddisfazione gli impegni internazionali assunti dal Brasile<sup>12</sup>.
- (7) L'EDPB osserva che, ai sensi degli articoli 47 e 94 del regolamento (UE) 2018/1725<sup>13</sup>, le istituzioni, gli organi e gli organismi dell'Unione europea possono trasferire dati personali a un paese terzo, un territorio, un settore o un'organizzazione internazionale che la Commissione europea ha riconosciuto ai sensi dell'articolo 45, paragrafo 3, del regolamento (UE) 2016/679, quale paese, territorio, settore o organizzazione internazionale che assicura un livello di protezione adeguato, a condizione che il trasferimento serva esclusivamente per lo svolgimento delle attività del titolare del trattamento, senza necessità di un'ulteriore autorizzazione. L'EDPB invita la Commissione europea a richiamare tale possibilità giuridica nei considerando del progetto di decisione.

## **2. ASPETTI GENERALI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI**

### **2.1 Responsabilizzazione e governance dei dati**

- (8) La LGPD prevede il principio di responsabilizzazione come uno dei principi generali applicabili al trattamento dei dati personali. Secondo tale legge, i titolari e i responsabili del trattamento<sup>14</sup> adottano misure tecniche e organizzative adeguate per rispettare efficacemente i loro obblighi in materia di protezione dei dati e devono essere in grado di dimostrare tale rispetto, in particolare all'autorità di controllo competente (articolo 46 LGPD). L'EDPB rileva che tali misure includono la designazione di un responsabile della protezione dei dati (articolo 41 LGPD), come ulteriormente specificato nel regolamento RPD dell'ANPD; la valutazione d'impatto sulla protezione dei dati (articolo 38 LGPD) nonché la tenuta di un registro delle operazioni di trattamento dei dati personali (articolo 37 LGPD). La LGPD stabilisce inoltre che i titolari e i responsabili del trattamento possono formulare norme per buone pratiche e modelli di governance interni, inclusi piani per attività formative, un meccanismo di supervisione interna e l'attenuazione dei rischi (articolo 50 LGPD). L'EDPB nota con soddisfazione che tali strumenti sono analoghi a quelli previsti dal GDPR per attuare il principio di responsabilizzazione e accoglie con favore tale stretto allineamento.

---

<sup>11</sup> Cfr. il considerando 13 del progetto di decisione.

<sup>12</sup> Cfr. i considerando da 8 a 10 del progetto di decisione.

<sup>13</sup> Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE ("EUDPR") (GU L 295 del 21.11.2018, pag. 39).

<sup>14</sup> Soggetti coinvolti nel trattamento dei dati, secondo l'articolo 5, punto IX, LGPD.

- (9) L'EDPB osserva che, per quanto riguarda la valutazione d'impatto sulla protezione dei dati, la LGPD non include un obbligo chiaro di effettuare la valutazione nei casi in cui il trattamento possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche, ma si limita a fare riferimento alla possibile richiesta da parte dell'ANPD. A tale proposito, l'EDPB osserva che l'ANPD raccomanda di effettuare una valutazione d'impatto sulla protezione dei dati quando il trattamento dei dati può comportare un rischio elevato nelle domande frequenti<sup>15</sup> relative alla valutazione d'impatto sulla protezione dei dati ("FAQ sulla valutazione d'impatto sulla protezione dei dati"). Inoltre la LGPD non include esplicitamente la valutazione della necessità e della proporzionalità nell'ambito della valutazione d'impatto sulla protezione dei dati. Tuttavia le FAQ sulla valutazione d'impatto sulla protezione dei dati raccomandano ai titolari e ai responsabili del trattamento di valutare nelle loro valutazioni la necessità e la proporzionalità del trattamento.
- (10) In tale contesto, l'EDPB invita la Commissione europea a monitorare l'attuazione pratica di tali requisiti al fine di verificare che la valutazione d'impatto sulla protezione dei dati sia condotta quando il trattamento può comportare un rischio elevato per i diritti e le libertà delle persone fisiche e che la valutazione della necessità e della proporzionalità dei trattamenti in relazione alle finalità sia inclusa nelle valutazioni d'impatto sulla protezione dei dati.

## **2.2 Ambito di applicazione e definizioni**

- (11) Il capitolo 3 dei criteri di riferimento per l'adeguatezza è dedicato ai "principi sostanziali" e fa riferimento ai concetti e ai principi fondamentali della protezione dei dati. Il sistema di un paese terzo o di un'organizzazione internazionale deve contenere tali concetti e principi fondamentali per garantire un livello di protezione dei dati personali sostanzialmente equivalente a quello garantito dal diritto dell'Unione europea. Essi non devono necessariamente riprendere la terminologia del GDPR, ma dovrebbero rispecchiare ed essere coerenti con le nozioni sancite nel diritto dell'UE in materia di protezione dei dati. I criteri di riferimento per l'adeguatezza fanno riferimento agli importanti concetti seguenti: "dati personali", "trattamento", "titolare del trattamento", "responsabile del trattamento", "destinatario" e "dati sensibili". Tale aspetto del diritto brasiliano sarà trattato nei paragrafi successivi.

### **2.2.1 Ambito di applicazione materiale e territoriale della LGPD**

- (12) L'EDPB accoglie con favore il fatto che l'ambito di applicazione della LGPD, sia materiale che territoriale, sia molto simile a quello previsto dal quadro dell'UE in materia di protezione dei dati.
- (13) L'articolo 4 LGPD esclude dal suo ambito di applicazione il trattamento per finalità esclusivamente personali e non economiche e tali eccezioni sono previste anche nel GDPR (articolo 2, paragrafo 2, lettera c), GDPR). Vi sono inoltre altri trattamenti che esulano parzialmente dall'ambito di applicazione della LGPD, in particolare il trattamento per: motivi di sicurezza pubblica, difesa nazionale, sicurezza dello Stato o indagine e perseguimento di reati; scopi giornalistici e artistici; ricerca accademica; ricerca medica (articolo 3, punto III, LGPD). Questo aspetto è approfondito nella sezione 3.1 del presente parere.
- (14) Per quanto riguarda in particolare l'applicazione parziale della LGPD al trattamento dei dati personali effettuato per scopi giornalistici e artistici, l'EDPB osserva che l'ambito di

---

<sup>15</sup> [https://www.gov.br/anpd/pt-br/canais\\_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd](https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd).

applicazione dell'eccezione è equivalente a quello previsto dall'articolo 85, paragrafo 2, GDPR<sup>16</sup>, vale a dire che tale eccezione si applica solo quando i dati personali sono trattati esclusivamente per tali finalità, mentre tutti gli altri trattamenti effettuati dalla stampa, dai media e dagli organismi artistici rientrano nell'ambito di applicazione della LGPD. Rimangono inoltre applicabili alcune eccezioni previste per il trattamento dei dati personali esclusivamente a scopi accademici, ossia gli articoli 7 (requisiti della base giuridica) e 11 (norme sul trattamento dei dati sensibili) LGPD<sup>17</sup>. L'ambito di applicazione di tali eccezioni è inoltre in linea con quello stabilito dall'articolo 85, paragrafo 2, GDPR.

## 2.2.2 Definizioni

- (15) L'EDPB nota con soddisfazione l'allineamento con il quadro dell'UE in materia di protezione dei dati per quanto riguarda le definizioni utilizzate nella LGPD, che sono coerenti con quelle previste nel GDPR. In particolare, le definizioni fornite dalla LGPD dei termini "dati personali", "informazioni pseudonimizzate", "dati anonimi"<sup>18</sup>, "trattamento dei dati", "titolare del trattamento", "responsabile del trattamento" e "dati sensibili" (articolo 5 LGPD) sono analoghe a quelle contenute nel GDPR, in particolare nel considerando 26, nell'articolo 4 e nell'articolo 9, paragrafo 1. Anche altre definizioni, quali "interessato", "responsabile della protezione dei dati", "consenso", "valutazione d'impatto sulla protezione dei dati" e il concetto di "contitolarietà del trattamento"<sup>19</sup>, sono sostanzialmente equivalenti ai concetti previsti dal GDPR.

## 2.3 Principi della protezione dei dati e basi giuridiche

### 2.3.1 Principi del trattamento

- (16) I criteri di riferimento per l'adeguatezza, conformemente al GDPR, stabiliscono che i dati devono essere trattati in modo lecito, corretto e legittimo. A norma dell'articolo 6 LGPD, i trattamenti di dati personali sono effettuati in buona fede e sono soggetti ai principi seguenti: finalità, adeguatezza, necessità, libero accesso<sup>20</sup>, qualità dei dati, trasparenza, sicurezza, prevenzione, non discriminazione, responsabilità e responsabilizzazione.
- (17) Tenendo conto dei concetti alla base di tali principi, l'ordinamento giuridico brasiliano sancisce gli stessi principi in materia di trattamento dei dati stabiliti dall'articolo 5 GDPR. Ad esempio, in relazione alla limitazione delle finalità, l'articolo 7, settimo comma, LGPD prevede che "il successivo trattamento dei dati personali di cui al terzo comma (dati personali accessibili al pubblico) e quarto comma (dati resi manifestamente pubblici dall'interessato) del presente articolo può essere effettuato per nuove finalità, purché si rispettino le finalità legittime e specifiche del nuovo trattamento e la tutela dei diritti dell'interessato, nonché i motivi e i principi stabiliti nella presente legge".
- (18) Il GDPR prevede chiaramente che tale trattamento successivo possa avvenire solo se la nuova finalità è compatibile con quella iniziale. L'obbligo di garantire la compatibilità delle finalità (nonché il rispetto delle norme etiche e delle garanzie tecniche e giuridiche applicabili)

---

<sup>16</sup> Cfr. anche il considerando 35 del progetto di decisione.

<sup>17</sup> Cfr. anche i considerando 32 e 33 del progetto di decisione.

<sup>18</sup> L'articolo 12 LGPD precisa ulteriormente che i dati anonimizzati non sono considerati dati personali, tranne quando l'anonimizzazione è stata annullata oppure può essere annullata mediante sforzi ragionevoli. Tale articolo spiega che il termine "ragionevole" deve essere considerato tenendo conto di fattori oggettivi quali: 1) il costo e il tempo necessari per il processo di annullamento; 2) la tecnologia disponibile; e 3) l'uso esclusivo dei mezzi propri del titolare del trattamento.

<sup>19</sup> Cfr. articolo 42, primo comma, punto I, LGPD.

<sup>20</sup> "Libero accesso: garantire agli interessati la possibilità di consultare gratuitamente e facilmente le modalità e la durata del trattamento, nonché l'integrità dei propri dati personali" (articolo 6, punto IV, LGPD).

è evidenziato nella guida orientativa sul trattamento dei dati personali a scopi accademici e di ricerca pubblicata dall'ANPD, nonché nelle linee guida sul legittimo interesse. L'ANPD, nelle linee guida sul legittimo interesse, spiega come il titolare del trattamento debba dimostrare un legame effettivo tra le due finalità del trattamento e tener conto delle "legittime aspettative" dell'interessato. Dette linee guida precisano inoltre che "l'analisi delle legittime aspettative può basarsi su diversi fattori, tra cui si possono evidenziare i seguenti: d) la finalità prevista della raccolta dei dati e la sua compatibilità con il trattamento basato su un legittimo interesse". L'EDPB accoglie con favore tale chiarimento da parte dell'ANPD, che contribuisce ad allineare meglio i requisiti della limitazione delle finalità.

- (19) Il principio della limitazione della conservazione previsto dal GDPR stabilisce che i dati sono conservati solo per l'arco di tempo necessario al conseguimento delle finalità per le quali sono trattati (articolo 5, paragrafo 1, lettera e), GDPR). Sebbene non includa esplicitamente il principio di limitazione della conservazione, l'articolo 6 LGPD dovrebbe essere letto in combinato disposto con l'articolo 15 LGPD che specifica i requisiti in caso di cessazione del trattamento dei dati. In tale articolo il principio di limitazione della conservazione è chiaramente collegato ai principi di "adeguatezza" e "necessità" che rientrano nei principi generali di cui all'articolo 6 LGPD. Per maggiore chiarezza, l'EDPB incoraggia la Commissione europea a chiarire nel progetto di decisione l'interazione tra gli articoli 6 e 15 LGPD in relazione al principio di limitazione della conservazione.
- (20) Inoltre, per quanto riguarda i requisiti relativi alla limitazione della conservazione, l'articolo 16 LGPD stabilisce le condizioni per la conservazione e la cancellazione dei dati personali dopo la fine del trattamento. Tale articolo prevede inoltre quattro finalità per le quali i dati possono essere conservati dopo la fine del trattamento: 1) per il rispetto di obblighi giuridici o normativi; 2) per finalità di ricerca, garantendo, ove possibile, l'anonimizzazione dei dati; 3) in caso di trasferimento a terzi nel rispetto degli obblighi imposti dalla LGPD; oppure 4) se utilizzati esclusivamente dal titolare del trattamento, purché i dati siano anonimizzati e sia vietato l'accesso agli stessi da parte di terzi. L'EDPB osserva che tali situazioni di trattamento sono conformi al principio di limitazione della conservazione sancito dal GDPR.
- (21) Il principio di trasparenza e correttezza mira a garantire che gli interessati abbiano il controllo sui propri dati personali e, a tal fine, le informazioni devono di norma essere fornite all'interessato in modo proattivo<sup>21</sup>. Nel contempo, la LGPD stabilisce una limitazione a tale principio in caso di "segreto commerciale e industriale", che può incidere sulla possibilità per gli interessati di ricevere informazioni sul trattamento dei propri dati al fine di poter esercitare il proprio controllo su di esso (ad esempio, tramite la presentazione di un reclamo all'ANPD). Tuttavia nel progetto di decisione la Commissione europea spiega che tale limitazione dovrebbe essere interpretata alla luce della legge brasiliana sull'accesso alle informazioni e del decreto presidenziale n. 7.721 del 16 maggio 2012 e deve pertanto essere interpretata "in modo da garantire che il trattamento e comunque la divulgazione di informazioni non rivelino segreti commerciali e non determinino un vantaggio competitivo per altri soggetti, nel rispetto degli obiettivi di protezione dei dati personali. Ciò significa che, per quanto riguarda il principio di trasparenza, e in tutto il testo della LGPD, la limitazione riguardante il "segreto commerciale e industriale" non deve essere intesa come un motivo generale per rifiutarsi di adempiere alla legge; piuttosto, devono essere predisposte garanzie specifiche per assicurare la divulgazione delle informazioni in modo da tutelare tali interessi"<sup>22</sup>.

<sup>21</sup> Ciò è sottolineato anche dai criteri di riferimento per l'adeguatezza, cfr. capitolo 3, A(7).

<sup>22</sup> Cfr. il considerando 81 del progetto di decisione.

- (22) Alla luce dell'importanza del principio di trasparenza, l'EDPB invita la Commissione europea a monitorare l'attuazione di tale disposizione nella pratica al fine di comprenderne meglio l'impatto sul diritto di informazione e di accesso.

### **2.3.2 Misure di sicurezza e violazioni**

- (23) La LGPD include i principi di sicurezza e prevenzione che prevedono l'applicazione di misure per la protezione dei dati personali e la prevenzione dei danni connessi al loro trattamento (articolo 6, punti VII e VII, LGPD); inoltre la LGPD stabilisce esplicitamente che, qualora le misure di sicurezza non siano attuate in modo adeguato, il trattamento dei dati è considerato illecito. La legge impone l'attuazione delle misure necessarie per dimostrare la conformità a tale principio mediante un approccio basato sul rischio (articoli 44, 46 e 47 LGPD) e il rispetto dei requisiti relativi alla valutazione delle violazioni e alla notifica delle stesse (articoli 48 e 49 LGPD). L'EDPB nota con soddisfazione che tali principi e obblighi sono strettamente allineati a quelli stabiliti nel GDPR.
- (24) L'EDPB accoglie con favore l'adozione da parte dell'ANPD di un ulteriore regolamento vincolante relativo alla notifica degli incidenti di sicurezza, che definisce il concetto di incidente e fornisce dettagli per la valutazione della sua gravità (ad esempio, quando si ritiene che l'incidente crei rischi per gli interessati o incida in modo significativo sui loro interessi e diritti fondamentali e debba quindi essere comunicato all'ANPD e all'interessato), nonché i requisiti di notifica degli incidenti<sup>23</sup>. A tale riguardo, l'EDPB osserva che, secondo il regolamento sulla notifica degli incidenti di sicurezza, come norma generale, "la comunicazione di un incidente di sicurezza all'ANPD deve essere effettuata dal titolare del trattamento entro tre giorni lavorativi"<sup>24</sup> e invita la Commissione europea ad allineare di conseguenza il suo progetto di decisione (considerando 75)<sup>25</sup>.
- (25) Per quanto riguarda la notifica delle violazioni dei dati, l'EDPB osserva che la LGPD stabilisce che tale notifica (sia all'ANPD che all'interessato) deve includere, tra l'altro, informazioni sulle misure tecniche e di sicurezza utilizzate per la protezione dei dati personali, adottate prima e dopo l'incidente, nel rispetto dei segreti commerciali e industriali (articolo 6, punto III, e articolo 9, punto II, LGPD). L'EDPB comprende la necessità di garantire efficacemente che il diritto al rispetto della vita privata e alla protezione dei dati non pregiudichi la tutela di altri diritti e invita la Commissione a monitorare l'attuazione di tale limitazione nei casi in cui le informazioni sull'incidente siano state fornite in modo parziale (tenendo conto dei segreti commerciali e industriali) e il suo impatto sui poteri dell'ANPD, se del caso.

### **2.3.3 Liceità del trattamento**

- (26) L'EDPB rileva che il principio di liceità e la sua attuazione, come previsto dalla LGPD (articolo 5, punto XII, e articoli 7, 8 e 10), sono strettamente allineati a quelli sanciti dal GDPR (articolo 4, paragrafo 11, e articoli 6, 7 e 9) e accoglie con favore tale allineamento.

#### **2.3.3.1 Legittimo interesse**

- (27) Le prescrizioni relative al legittimo interesse da utilizzare come base giuridica per il trattamento ai sensi della LGPD (articolo 7, punto IX) sono in linea con il GDPR (articolo 6, paragrafo 1,

---

<sup>23</sup> Cfr. i considerando da 73 a 77 del progetto di decisione.

<sup>24</sup> Cfr. gli articoli 6 e 9 del regolamento sulla notifica degli incidenti di sicurezza.

<sup>25</sup> Cfr. il considerando 75 del progetto di decisione secondo cui "[l]a notifica di un incidente di sicurezza all'ANPD e agli interessati deve avvenire entro tre giorni (72 ore) dal momento in cui il titolare del trattamento ne è venuto a conoscenza".

lettera f). La LGPD sottolinea inoltre che i diritti e le libertà fondamentali (tra cui il diritto alla protezione dei dati<sup>26</sup>) dovrebbero prevalere nella maggior parte dei casi.

- (28) L'EDPB rileva che l'articolo 10 LGPD elenca le finalità legittime per le quali tale base giuridica potrebbe essere utilizzata. Una di tali finalità legittime è quella di sostenere e promuovere l'attività del titolare del trattamento (articolo 10, punto I, LGPD).
- (29) Sebbene tale espressione sembri essere generica, l'EDPB osserva che le condizioni per l'utilizzo del "legittimo interesse" sono ulteriormente specificate nella guida "Basi giuridiche per il trattamento dei dati personali - Legittimo interesse" ("guida sul legittimo interesse") adottata dall'ANPD. Tale guida chiarisce che, affinché un interesse possa essere considerato "legittimo", devono essere soddisfatte tre condizioni: 1) compatibilità con l'ordinamento giuridico brasiliano; 2) riferimento a una situazione specifica; e 3) trattamento effettuato per finalità legittime, specifiche ed esplicite<sup>27</sup>. Tali condizioni sono analoghe alle tre condizioni cumulative per il trattamento legittimo dei dati personali ai sensi di tale base giuridica, specificate dalla CGUE<sup>28</sup>, e alla loro ulteriore spiegazione fornita dalla Corte. Inoltre le condizioni per il "legittimo interesse" specificate nella guida sul legittimo interesse sono simili a quelle delle linee guida adottate dall'EDPB<sup>29</sup>. L'EDPB accoglie con favore l'approccio adottato dall'ANPD in merito al legittimo interesse e al suo utilizzo per il trattamento.

## 2.4 Diritti delle persone fisiche

- (30) L'EDPB accoglie con favore il fatto che la LGPD conferisca alle persone fisiche diritti analoghi a quelli previsti dal GDPR (entrambi al capo III). In particolare, la LGPD prevede il diritto di accesso, il diritto di rettifica, il diritto alla portabilità dei dati, il diritto di limitazione del trattamento, il diritto di cancellazione, il diritto di informazione, il diritto di negare o revocare il consenso, il diritto di opporsi al trattamento e il diritto di presentare ricorso (articoli 9 e 18 LGPD).
- (31) La LGPD conferisce inoltre agli interessati il diritto di richiedere il riesame delle decisioni adottate unicamente sulla base del trattamento automatizzato di dati personali che incidono sui loro interessi (articolo 20 LGPD). Il contenuto dell'articolo 20 LGPD rispecchia sostanzialmente l'articolo 22 GDPR.
- (32) L'EDPB osserva che, in relazione ai diritti degli interessati, la legge brasiliana sull'*habeas data* stabilisce disposizioni specifiche per garantire il diritto di accesso e il diritto di rettifica entro un breve lasso di tempo (rispettivamente 10 e 15 giorni) dalla richiesta di una persona fisica, e accoglie con favore tale aspetto.
- (33) L'EDPB ritiene che la LGPD stabilisca requisiti sostanzialmente equivalenti a quelli garantiti dal GDPR per quanto riguarda i diritti degli interessati.

## 2.5 Limitazioni ai trasferimenti successivi

- (34) I criteri di riferimento per l'adeguatezza chiariscono che il livello di protezione delle persone fisiche i cui dati personali sono trasferiti in base a una decisione di adeguatezza non deve

---

<sup>26</sup> Cfr. il paragrafo 3 del presente parere.

<sup>27</sup> Cfr. il considerando 52 del progetto di decisione.

<sup>28</sup> Ad esempio, sentenza della CGUE del 7 dicembre 2023, *SCHUFA Holding AG*, cause riunite C-26/22 e C-64/22, punti da 75 a 80.

<sup>29</sup> Linee guida 1/2024 sul trattamento dei dati personali sulla base dell'articolo 6, paragrafo 1, lettera f), GDPR (versione 1.0), adottate l'8 ottobre 2024.

essere compromesso dal trasferimento successivo e che pertanto qualsiasi trasferimento successivo "dovrebbe essere consentito soltanto quando il destinatario successivo (ossia il destinatario del trasferimento successivo) è anch'esso soggetto a norme (comprese norme contrattuali) che garantiscano un livello di protezione adeguato e segue le pertinenti istruzioni quando tratta i dati per conto del titolare del trattamento".

- (35) In relazione alla valutazione dell'adeguatezza del quadro giuridico e delle prassi del Brasile, per trasferimento successivo si intende il trasferimento di dati personali dall'entità, che agisce quale titolare del trattamento, nell'ambito di applicazione territoriale della LGPD brasiliana, all'entità al di fuori di tale ambito.
- (36) I requisiti relativi al trasferimento successivo sono stabiliti nel capo V LGPD e ulteriormente integrati dall'ANPD attraverso l'adozione del regolamento sul trasferimento dei dati, che fornisce le definizioni di "trasferimento", "trasferimento internazionale di dati", "importatore", "esportatore" e include requisiti dettagliati per i trasferimenti.
- (37) L'EDPB nota con soddisfazione che la definizione di "trasferimento" e di "trasferimento internazionale di dati" è in linea con quella contenuta nelle linee guida 05/2021 dell'EDPB<sup>30</sup>.
- (38) Secondo la LGPD e il regolamento sul trasferimento dei dati, i trasferimenti successivi possono aver luogo solo per finalità legittime, specifiche ed esplicite e quando sono in vigore condizioni o strumenti specifici (articolo 33 LGPD, e articoli da 9 a 33 del regolamento sul trasferimento dei dati)<sup>31</sup>. L'EDPB riconosce che tali strumenti sono simili agli strumenti di trasferimento previsti nel capo V GDPR. L'EDPB invita tuttavia la Commissione europea a chiarire nel progetto di decisione se i trasferimenti possano essere effettuati in conformità dell'articolo 33, punti da III a IX, LGPD solo in circostanze eccezionali, qualora non siano soddisfatte le condizioni di cui all'articolo 33, punti da I a II, LGPD<sup>32</sup>.
- (39) Tuttavia il regolamento sul trasferimento dei dati specifica che i trasferimenti internazionali di dati personali sono consentiti "quando l'interessato ha fornito il consenso specifico e distinguibile per tale trasferimento, con previa informazione sulla natura internazionale dell'operazione prevista, distinguendola chiaramente da altre finalità". Non è chiaro se tale requisito comporti l'obbligo di informare gli interessati dei possibili rischi dei trasferimenti internazionali derivanti dalla mancanza di una protezione adeguata nel paese terzo e dalla mancanza di garanzie adeguate (ad esempio, informazioni relative al fatto che nel paese terzo potrebbero non esistere un'autorità di controllo e/o principi in materia di trattamento dei dati e/o diritti degli interessati), come previsto dall'articolo 49, paragrafo 1, lettera a), GDPR. Per l'EDPB, e ai sensi del GDPR, la fornitura di tali informazioni è essenziale per consentire all'interessato di fornire un consenso informato con piena conoscenza di tali fatti specifici relativi al trasferimento. L'EDPB invita pertanto la Commissione europea a chiarire nel progetto di decisione se l'interessato sia informato dei possibili rischi di tale trasferimento derivanti dalla mancanza di una protezione adeguata nel paese terzo e di garanzie adeguate.
- (40) Inoltre, secondo il regolamento sul trasferimento dei dati, "sia il titolare del trattamento che il responsabile del trattamento adottano misure efficaci in grado di dimostrare il rispetto e la conformità alle norme in materia di protezione dei dati personali e l'efficacia di tali misure, in modo compatibile con il livello di rischio del trattamento e con le modalità di trasferimento

---

<sup>30</sup> Paragrafo 9, linee guida 05/2021 sull'interazione tra l'applicazione dell'articolo 3 e le disposizioni sui trasferimenti internazionali a norma del capo V GDPR, adottate il 14 febbraio 2023.

<sup>31</sup> Cfr. i considerando da 101 a 109 del progetto di decisione.

<sup>32</sup> L'articolo 49 GDPR specifica che le deroghe previste da tale articolo possono essere applicate solo in mancanza di una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 3, GDPR, o di garanzie adeguate ai sensi dell'articolo 46 GDPR.

internazionale utilizzate" (articolo 4, secondo comma, del regolamento sul trasferimento dei dati). L'EDPB accoglie con favore l'inserimento di tale obbligo. Allo stesso tempo, sarebbe utile chiarire che l'efficacia di tali misure dovrebbe essere valutata in modo da garantire anche che la legislazione locale del paese terzo in questione non comprometta la continuità della protezione degli interessati i cui dati sono trasferiti<sup>33</sup>. L'EDPB invita la Commissione europea a chiarire che negli scenari di trasferimento sarà preso in considerazione anche tale elemento.

- (41) L'EDPB accoglie con favore l'inclusione di un requisito esplicito in materia di trasparenza nei confronti dell'interessato, ossia che l'interessato ha il diritto di ricevere lo strumento contrattuale utilizzato per il trasferimento successivo, nonché la descrizione di tale trasferimento, ad esempio la durata e la finalità del trasferimento, i paesi di destinazione, le responsabilità delle parti coinvolte, i diritti dell'interessato e i mezzi per esercitarli (articolo 16 del regolamento sul trasferimento dei dati).
- (42) Tuttavia sembra che tale ambito di applicazione dell'obbligo di trasparenza sia pertinente solo quando i trasferimenti sono effettuati sulla base di clausole contrattuali tipo e non quando sono utilizzati altri strumenti<sup>34</sup>. L'EDPB invita pertanto la Commissione europea a chiarire che gli stessi obblighi di trasparenza si applicano indipendentemente dallo strumento di trasferimento utilizzato.
- (43) L'EDPB rileva inoltre che i requisiti relativi al contenuto delle norme vincolanti d'impresa ("BCR") non sono pienamente in linea con quelli previsti dal GDPR, in particolare dall'articolo 47, paragrafo 2, lettere f) e l), GDPR. Al fine di garantire che il livello di protezione offerto dal GDPR non venga compromesso, l'EDPB invita la Commissione europea a chiarire nel progetto di decisione che anche tali elementi<sup>35</sup> saranno presi in considerazione quando detto strumento di trasferimento dovrà essere utilizzato per i trasferimenti successivi di dati personali verso il Brasile in base alla decisione di adeguatezza.

## 2.6 Meccanismi di procedura e applicazione

- (44) Secondo i criteri di riferimento per l'adeguatezza<sup>36</sup> e la pertinente giurisprudenza della CGUE<sup>37</sup>, un sistema di protezione dei dati sostanzialmente equivalente al modello dell'Unione europea deve prevedere: i) un'autorità indipendente, che dovrebbe vigilare e far rispettare le norme in materia di protezione dei dati, con il potere di indagare e intervenire senza pressioni esterne. I sistemi di protezione dei dati devono garantire ii) che i titolari e i responsabili del trattamento siano responsabilizzati e consapevoli delle loro responsabilità, mentre gli interessati siano informati dei loro diritti. Dovrebbero essere previsti processi di verifica e sanzioni efficaci per garantire il rispetto delle norme; iii) che i titolari e i responsabili del trattamento dei dati dimostrino la conformità attraverso misure quali valutazioni d'impatto sulla protezione dei dati, registri delle attività di trattamento e la designazione di responsabili della protezione dei dati. Inoltre iv) il sistema di protezione dei dati deve fornire supporto e assistenza ai singoli interessati nell'esercizio dei loro diritti e meccanismi di ricorso adeguati.

<sup>33</sup> Cfr. sentenza Latombe. Cfr. anche CGUE, 16 luglio 2020, sentenza nella causa C-311/18 ("Schrems II").

<sup>34</sup> Ad esempio, il regolamento sul trasferimento dei dati include requisiti generali in materia di trasparenza quando si intende ricorrere alle norme vincolanti d'impresa, in particolare "l'istituzione e l'attuazione di un programma di governance della vita privata che miri a instaurare un rapporto di fiducia con l'interessato, mediante azioni trasparenti che garantiscano meccanismi di partecipazione dell'interessato" (articolo 25, punto V, del regolamento sul trasferimento dei dati) e trasparenza in relazione all'esercizio dei diritti dell'interessato e al diritto di reclamo (articolo 26, punto VI, del regolamento sul trasferimento dei dati).

<sup>35</sup> Responsabilità e cooperazione con l'autorità di controllo (articolo 47, paragrafo 2, lettere f) e l), GDPR).

<sup>36</sup> Cfr. il capitolo 3, sezione C), dei criteri di riferimento per l'adeguatezza.

<sup>37</sup> CGUE, 6 ottobre 2015, sentenza nella causa C-362/14, *Schrems*.

- (45) Nella presente sezione, l'EDPB ha concentrato la propria valutazione sull'esistenza di un'autorità indipendente, di un meccanismo di ricorso adeguato e di sanzioni efficaci.

## 2.6.1 Vigilanza indipendente

- (46) La LGPD istituisce l'*Agencia Nacional de Proteção de Dados* (ANPD) quale autorità nazionale di controllo responsabile di monitorare e applicare le sue disposizioni.
- (47) L'EDPB accoglie con favore il fatto che all'ANPD sia stato concesso lo status di "autorità di natura speciale", una designazione intesa a garantire l'autonomia necessaria per svolgere pienamente le funzioni giuridiche ed esercitare i poteri ad essa conferiti dalla LGPD, in particolare revocando le disposizioni che subordinavano il funzionamento e le operazioni finanziarie dell'ANPD alle autorizzazioni che dovevano essere rilasciate dall'esecutivo.
- (48) Allo stesso modo, l'EDPB accoglie con favore le modifiche apportate il 15 settembre 2025 al quadro giuridico brasiliano, in base alle quali l'ANPD è ora riconosciuta come **agenzia di regolamentazione**<sup>38</sup>. L'EDPB ritiene pertanto che uno dei principali cambiamenti sia che l'ANPD presenterà il proprio bilancio direttamente al ministero della Pianificazione e del bilancio, anziché doverlo presentare tramite il ministero della Giustizia. Il bilancio dell'ANPD rimane una voce separata nel bilancio degli Stati federali. L'EDPB è consapevole che l'ANPD godeva già di indipendenza anche in materia di bilancio e finanze ma, diventando un'agenzia di regolamentazione, il suo processo amministrativo è stato semplificato.
- (49) L'EDPB accoglie inoltre con favore la nuova competenza dell'ANPD, che è stata recentemente designata come autorità responsabile della protezione dei minori online<sup>39</sup>. L'EDPB prende atto del fatto che, ai sensi del capo IX LGPD, l'ANPD è dotata dei necessari poteri e incarichi disponibili per garantire la conformità ai diritti in materia di protezione dei dati e per sensibilizzare l'opinione pubblica al riguardo, quali i poteri di indagine e sanzionatori (articolo 55-J LGPD).
- (50) Per quanto riguarda il personale e il bilancio dell'ANPD, che svolgono un ruolo importante per la sua indipendenza, l'EDPB nota con soddisfazione la recente decisione di aumentare il personale con oltre 200 nuove posizioni<sup>40</sup>.
- (51) L'EDPB osserva che, ai sensi dell'articolo 55-C LGPD, l'ANPD è (ora) composta da una serie di organi<sup>41</sup>, tra cui il consiglio nazionale per la protezione dei dati personali e della vita privata ("consiglio"). L'EDPB prende atto della sua composizione, che comprende anche rappresentanti dell'organo esecutivo federale, dell'organo legislativo e del sistema giudiziario<sup>42</sup>. L'EDPB rileva inoltre che, ai sensi dell'articolo 58-B LGPD, il consiglio è responsabile, tra l'altro, di i) "proporre linee guida strategiche e fornire informazioni di base per l'elaborazione della politica nazionale per la protezione dei dati personali e della vita

<sup>38</sup> Misura provvisoria n. 1.317/2025 disponibile all'indirizzo: <https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314>.

<sup>39</sup> Legge n. 15.211/2025, relativa alla protezione dei bambini e dei minori nell'ambiente digitale, disponibile all'indirizzo: <https://www.in.gov.br/web/dou/-/lei-n-15.211-de-17-de-setembro-de-2025-656579619>.

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

<sup>41</sup> Ai sensi dell'articolo 55-C LGPD, l'ANPD è composta da: il consiglio di amministrazione, l'organo direttivo più alto; un consiglio nazionale per la protezione dei dati personali e della vita privata; l'ufficio della commissione di disciplina; IV - l'ufficio del Mediatore; VI - l'ufficio per gli affari legali, e VI - le unità amministrative e le unità specializzate necessarie per l'applicazione delle disposizioni della LGPD. Cfr. i considerando da 126 a 130 del progetto di decisione.

<sup>42</sup> Cfr. anche il considerando 132 del progetto di decisione e l'articolo 55-C LGPD.

privata e per le attività dell'ANPD"; e ii) "raccomandare le azioni che l'ANPD deve intraprendere".

- (52) Con particolare riferimento a tali compiti, l'EDPB ritiene importante acquisire una comprensione più chiara delle modalità di attuazione degli stessi e della misura in cui le proposte e le raccomandazioni del consiglio influenzano il lavoro dell'ANPD. Invita pertanto la Commissione europea ad approfondire ulteriormente tali compiti e l'interazione tra il consiglio e l'ANPD, al fine di valutare meglio l'influenza del consiglio sulle attività dell'ANPD.

## **2.6.2 Ricorso**

- (53) L'EDPB accoglie con favore il meccanismo di ricorso previsto dalla LGPD, che conferisce inoltre agli interessati il diritto di presentare un reclamo all'ANPD e di impugnare le sue decisioni presentando ricorso al suo consiglio di amministrazione. Le persone fisiche possono poi impugnare le decisioni del consiglio dinanzi agli organi giurisdizionali nonché presentare ricorso contro l'ANPD per il mancato rispetto degli obblighi che le incombono ai sensi della LGPD. Poiché la differenza tra lo strumento di impugnazione e lo strumento di ricorso non emerge chiaramente dal progetto di decisione, l'EDPB invita la Commissione a chiarire ulteriormente il funzionamento di queste due vie e a specificare anche se il ricorso sia limitato solo al rifiuto di trattare un reclamo o al rigetto nel merito di un reclamo.
- (54) Analogamente, l'EDPB accoglie con favore la disposizione relativa al diritto al risarcimento dei danni materiali e immateriali, nonché al ricorso collettivo (articolo 22 LGPD).

## **2.6.3 Sanzioni**

- (55) L'EDPB ricorda che l'esistenza di sanzioni efficaci e dissuasive può svolgere un ruolo importante nel garantire il rispetto delle norme in materia di protezione dei dati, in quanto è un segno dell'elevato grado di responsabilizzazione e consapevolezza che il sistema garantisce. L'EDPB accoglie con favore i poteri correttivi conferiti all'ANPD, che sono stati esercitati in diverse occasioni<sup>43</sup> e comprendono una serie di misure quali ammonimenti, ammende fino al due per cento (2 %) dei ricavi lordi dei soggetti giuridici privati coinvolti, ammende giornaliere, il blocco dei dati personali relativi alla violazione fino alla sua regolarizzazione, la cessazione temporanea delle attività di trattamento dei dati in questione e la cancellazione dei dati personali interessati (articolo 52 LGPD)<sup>44</sup>. L'EDPB invita la Commissione a monitorarne l'applicazione coerente, con particolare attenzione alle sanzioni.
- (56) L'EDPB nota con soddisfazione che l'ANPD ha emanato un regolamento (vincolante) sulle sanzioni. Tale regolamento classifica le sanzioni in diversi livelli utilizzando fattori oggettivi quali il tipo e il volume dei dati trattati o l'impatto sui diritti degli interessati e prevede una metodologia di calcolo delle ammende in linea con i requisiti di cui all'articolo 83 GDPR.

<sup>43</sup> Cfr. il registro delle sanzioni dell'ANPD: [https://www.gov.br/anpd/pt-br/centrais-de-conteudo/deciso-es-em-processos-sancionadores-1/deciso-es-em-processos-sancionadores?\\_authenticator=7951f0a70d3d125fd05e11a1e544b72d2c61f304](https://www.gov.br/anpd/pt-br/centrais-de-conteudo/deciso-es-em-processos-sancionadores-1/deciso-es-em-processos-sancionadores?_authenticator=7951f0a70d3d125fd05e11a1e544b72d2c61f304).

<sup>44</sup> "Tali sanzioni possono essere imposte nei confronti di soggetti pubblici o privati, ad eccezione delle ammende, comprese quelle giornaliere, che non possono essere inflitte nei confronti degli enti pubblici" (considerando 135 del progetto di decisione).

### 3. ACCESSO E USO DEI DATI PERSONALI TRASFERITI DALL'UNIONE EUROPEA DA PARTE DI AUTORITÀ PUBBLICHE IN BRASILE

- (57) Conformemente all'articolo 45, paragrafo 2, GDPR, la valutazione delle limitazioni e delle garanzie previste dalla legislazione brasiliana in materia di accesso e successivo utilizzo da parte delle autorità pubbliche brasiliane dei dati personali trasferiti ai titolari del trattamento e ai responsabili del trattamento in Brasile per finalità di contrasto penale e di sicurezza nazionale ("accesso da parte di pubbliche amministrazioni") è un elemento importante della verifica dell'"equivalenza sostanziale", secondo l'interpretazione della CGUE.
- (58) L'EDPB nota con soddisfazione la particolare attenzione e le informazioni fattuali fornite dalla Commissione su questo aspetto nel progetto di decisione<sup>45</sup>. Pertanto l'EDPB si astiene dal riprodurre la maggior parte delle constatazioni e delle analisi fattuali nel presente parere. Valuta invece l'ingerenza del sistema brasiliano per l'accesso da parte di pubbliche amministrazioni per motivi di contrasto penale e di sicurezza nazionale sulla base dei 4 elementi individuati dall'EDPB nelle raccomandazioni relative alle garanzie essenziali europee per le misure di sorveglianza, adottate il 10 novembre 2020<sup>46</sup>:
- Garanzia A — Norme giuridiche chiare, precise e accessibili;
  - Garanzia B — Necessità e proporzionalità rispetto agli obiettivi legittimi perseguiti;
  - Garanzia C — Meccanismo di controllo indipendente;
  - Garanzia D — La persona deve poter accedere a mezzi di ricorso efficaci.

#### 3.1 Accesso e uso da parte delle autorità pubbliche brasiliane per motivi di contrasto penale

##### 3.1.1 Quadro giuridico in materia contrasto penale

- (59) L'EDPB osserva che l'accesso e il successivo utilizzo dei dati personali da parte delle autorità di contrasto brasiliane<sup>47</sup> sono disciplinati da un sistema di atti giuridici di diversa natura giuridica. La protezione dei dati e la vita privata, compresa la segretezza della corrispondenza e delle comunicazioni, sono sancite dall'articolo 5 della costituzione come diritti fondamentali. L'EDPB accoglie con particolare favore il fatto che l'ambito di applicazione della protezione di tali diritti, analogamente all'UE, non sia limitato ai soli cittadini brasiliani, ma comprenda anche gli stranieri residenti in Brasile o meno<sup>48</sup>.
- (60) Esistono inoltre diverse leggi settoriali specializzate che disciplinano il possibile accesso ai dati personali per motivi di contrasto penale. Per quanto riguarda l'accesso ai dati trasferiti dall'UE al Brasile, sono particolarmente rilevanti il codice penale, la legge sulle intercettazioni telefoniche, il quadro civile di Internet, la legge sulla riservatezza degli istituti finanziari,

<sup>45</sup> Cfr. i considerando da 152 a 217 del progetto di decisione.

<sup>46</sup> [Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza.](#)

<sup>47</sup> Cfr. l'elenco delle autorità al considerando 165 del progetto di decisione.

<sup>48</sup> Cfr. i considerando 8 e 9 del progetto di decisione.

la legge sulle associazioni a delinquere e sulle indagini penali e altre. L'EDPB osserva che tali atti giuridici sono accessibili al pubblico e potrebbero essere considerati sufficientemente chiari da fornire agli interessati un'indicazione delle circostanze e delle condizioni in cui le autorità pubbliche sono autorizzate ad accedere ai loro dati<sup>49</sup>.

- (61) Un'altra importante fonte normativa in Brasile è la giurisprudenza della Corte suprema federale del Brasile, che sembra applicare un'interpretazione ampia della portata dei diritti alla vita privata e alla protezione dei dati<sup>50</sup>, nonché la giurisprudenza della Corte interamericana dei diritti umani responsabile dell'interpretazione e dell'applicazione della Convenzione americana sui diritti dell'uomo, ratificata dal Brasile nel 1992<sup>51</sup>.
- (62) L'EDPB osserva che l'ambito di applicabilità della LGPD in caso di trattamento dei dati personali per motivi di contrasto penale è parziale, il che può comportare incertezza giuridica.
- (63) Come riconosciuto dalla Commissione nel progetto di decisione, la LGPD non si applica al trattamento dei dati effettuato *esclusivamente* a fini di pubblica sicurezza, difesa nazionale, sicurezza dello Stato o indagine e perseguimento di reati<sup>52</sup>. Ai sensi dell'articolo 4, punti I) e III), LGPD, il trattamento dei dati in questi ambiti sarà disciplinato da una normativa specifica, che dovrà comprendere i principi e i diritti degli interessati delineati nella LGPD. Per quanto a conoscenza dell'EDPB e confermato dalla Commissione, il Brasile non ha ancora adottato una legislazione specifica in materia di trattamento dei dati personali nel settore della giustizia penale e dell'applicazione della legge (ad esempio, analoga alla direttiva dell'UE sulla protezione dei dati nelle attività di polizia e giudiziarie<sup>53</sup>).
- (64) L'EDPB nota con soddisfazione che la Corte suprema federale del Brasile, nella sua giurisprudenza<sup>54</sup>, ha interpretato la LGPD in modo da estenderne l'applicabilità parziale al trattamento dei dati personali per le indagini penali e il mantenimento dell'ordine pubblico.
- (65) L'EDPB accoglie con favore il fatto che l'autorità di controllo brasiliana, l'ANPD, sostenga pienamente tale interpretazione e ritenga che *"l'assenza di una legislazione specifica non conferisca alle agenzie di sicurezza un'autorizzazione ampia e illimitata a trattare i dati personali dei cittadini esclusivamente per motivi di sicurezza pubblica e di indagine e perseguimento di reati senza alcuna restrizione"*<sup>55</sup>. Allo stesso tempo, l'EDPB osserva che, ai sensi dell'articolo 4, punto III), terzo comma, LGPD, per alcuni specifici trattamenti di dati effettuati esclusivamente per motivi di contrasto penale, l'ANPD sembra avere attualmente un ruolo principalmente consultivo rispetto alle autorità di contrasto.
- (66) L'EDPB invita la Commissione a valutare ulteriormente e chiarire nel progetto di decisione l'applicabilità della LGPD in caso di trattamento dei dati personali per motivi di contrasto penale, anche per quanto riguarda i poteri dell'ANPD, nonché a prendere attentamente in considerazione qualsiasi sviluppo rilevante al riguardo nell'ambito del futuro monitoraggio (cfr. anche la sezione relativa alla vigilanza e ai mezzi di ricorso).

<sup>49</sup> Cfr. la sentenza della Corte CEDU in *Zakharov*, punto 229.

<sup>50</sup> Cfr. Corte suprema federale, decisione sul ricorso diretto di incostituzionalità n. 6649, settembre 2022.

<sup>51</sup> Cfr. il considerando 10 del progetto di decisione.

<sup>52</sup> Cfr. i considerando 30 e 31 del progetto di decisione.

<sup>53</sup> Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU L 119 del 4.5.2016, pag. 89).

<sup>54</sup> Cfr. Corte suprema federale, decisione sul ricorso diretto di incostituzionalità n. 6649, settembre 2022.

<sup>55</sup> Cfr. la nota tecnica ANPD n. 29/2024/FIS/CGF/ANPD, indirizzata al ministero della Giustizia e della pubblica sicurezza, punto 5.4.1.29, disponibile all'indirizzo: [SEI/ANPD - 0132350 - Nota Técnica](#).

### 3.1.2 Necessità e proporzionalità

- (67) L'EDPB nota con soddisfazione che, come norma generale, l'accesso ai dati relativi alle comunicazioni, sia al contenuto che ai metadati, nonché ad altre categorie di informazioni riservate protette, quali i dati bancari e fiscali, necessita di un'autorizzazione giudiziaria preventiva.
- (68) Per quanto riguarda l'accesso ai dati relativi alle comunicazioni, l'EDPB accoglie con favore il fatto che, ai sensi della legge sulle intercettazioni telefoniche e della giurisprudenza della Corte suprema federale, tale misura sia considerata eccezionale e sia soggetta a condizioni rigorose volte a garantirne la necessità e la proporzionalità<sup>56</sup>. Inoltre, quale misura preventiva contro possibili abusi, il diritto brasiliano prevede che l'intercettazione delle comunicazioni senza autorizzazione giudiziaria o per fini non autorizzati dalla legge costituisca un reato punibile con una pena detentiva fino a quattro anni<sup>57</sup>.
- (69) La rigorosa attuazione delle misure di garanzia per l'accesso ai dati relativi alle comunicazioni è particolarmente importante, data l'esistenza in Brasile di un obbligo generale di conservazione dei dati che impone ai fornitori di servizi di connessione internet e di applicazioni online di conservare i registri delle connessioni per un anno<sup>58</sup>. Pur notando con soddisfazione che l'accesso ai dati conservati è possibile solo previa autorizzazione giudiziaria<sup>59</sup>, l'EDPB ricorda l'approccio rigoroso e le restrizioni alla conservazione generale e indiscriminata dei metadati delle comunicazioni nell'UE<sup>60</sup> e prende atto con soddisfazione delle ulteriori informazioni fornite dalla Commissione in merito all'assenza di conservazione di massa dei dati nel paese. L'EDPB incoraggia pertanto la Commissione a prestare particolare attenzione alle prassi e al regime giuridici in vigore in Brasile in materia di accesso ai dati delle comunicazioni durante il monitoraggio e il riesame del progetto di decisione.
- (70) L'EDPB nota con soddisfazione che garanzie analoghe si applicano anche per quanto riguarda l'accesso da parte delle autorità di contrasto ai dati fiscali e bancari, ovvero l'obbligo di autorizzazione giudiziaria preventiva, consentito solo per reati gravi, l'esistenza di sanzioni penali in caso di abuso ecc.
- (71) Secondo il progetto di decisione, è prevista un'eccezione all'obbligo generale dell'autorizzazione giudiziaria preventiva per l'accesso da parte delle autorità di contrasto a determinate categorie di dati personali<sup>61</sup>. A norma degli articoli 15 e 16 della legge sulle associazioni a delinquere e sulle indagini penali, un capo della polizia e la procura possono accedere senza autorizzazione giudiziaria ai dati di registrazione di una persona indagata relativi a: *"qualifiche personali, affiliazioni e indirizzi conservati dalla Corte elettorale, dalle compagnie telefoniche, dagli istituti finanziari, dai fornitori di servizi internet e dagli amministratori di carte di credito"*<sup>62</sup>. Analogamente, le società di trasporto consentiranno, per un periodo di cinque anni, l'accesso diretto e permanente da parte di un giudice, della procura o di un capo della polizia alle banche dati relative alle prenotazioni e ai registri di viaggio<sup>63</sup>.

<sup>56</sup> Cfr. i considerando 169 e 170 del progetto di decisione.

<sup>57</sup> Ibidem.

<sup>58</sup> Cfr. il considerando 173 del progetto di decisione.

<sup>59</sup> Ibidem.

<sup>60</sup> Per ulteriori informazioni sulla conservazione dei dati, cfr. il documento dell'EDPB *Statement 5/2024 on the recommendations of the high level group on access to data for effective law enforcement*, disponibile all'indirizzo: [https://www.edpb.europa.eu/system/files/2024-11/edpb\\_statement\\_20241104\\_ontherecommendationsofthehlq\\_en.pdf](https://www.edpb.europa.eu/system/files/2024-11/edpb_statement_20241104_ontherecommendationsofthehlq_en.pdf).

<sup>61</sup> Cfr. il considerando 164 del progetto di decisione.

<sup>62</sup> Cfr. l'articolo 15 della legge sulle associazioni a delinquere e sulle indagini penali.

<sup>63</sup> Cfr. l'articolo 16 della legge sulle associazioni a delinquere e sulle indagini penali.

- (72) L'EDPB rileva che l'ambito di applicazione della legge sulle associazioni a delinquere e sulle indagini penali è limitato alle indagini e alle sanzioni nei confronti dei gruppi criminali organizzati e delle organizzazioni terroristiche, che rappresentano un rischio significativo per i cittadini e la società e possono quindi giustificare una più grave ingerenza nei diritti fondamentali alla vita privata e alla protezione dei dati<sup>64</sup>. Allo stesso tempo l'EDPB ritiene che le informazioni relative a tali eccezioni fornite nel considerando 164 del progetto di decisione siano molto generiche e non complete. In particolare, dalle informazioni contenute nel progetto di decisione non risulta chiaro se, in tal caso, l'accesso ai dati personali sia soggetto a un controllo giurisdizionale ex post della necessità e della proporzionalità.
- (73) In considerazione di quanto sopra, l'EDPB invita la Commissione a chiarire e spiegare ulteriormente nel progetto di decisione l'ambito e la natura dei casi in cui l'accesso ai dati da parte delle autorità di contrasto non necessita di autorizzazione giudiziaria, nonché le garanzie applicabili nella legislazione brasiliana. L'EDPB ritiene inoltre che la Commissione dovrebbe prestare particolare attenzione all'applicazione di tali eccezioni ai sensi del diritto brasiliano durante il monitoraggio del progetto di decisione.

### 3.1.3 Ulteriore utilizzo dei dati e trasferimenti successivi

- (74) L'EDPB ricorda che il livello di protezione offerto ai dati personali trasferiti dall'UE/SEE verso il Brasile non deve essere compromesso dall'ulteriore utilizzo o condivisione dei dati con destinatari in Brasile o in un paese terzo, vale a dire che i trasferimenti successivi dovrebbero essere consentiti soltanto se è garantito un continuo livello di protezione sostanzialmente equivalente a quello previsto dal diritto dell'UE.
- (75) A tale proposito, l'EDPB rileva con soddisfazione che la Corte suprema federale del Brasile ha stabilito che la condivisione di dati personali tra enti pubblici (anche quando sono condivisi tra autorità di contrasto e agenzie di intelligence) presuppone: 1) la definizione di una finalità legittima, specifica ed esplicita per il trattamento dei dati; 2) la compatibilità del trattamento con le finalità comunicate; 3) la limitazione della condivisione al minimo necessario per conseguire la finalità comunicata; nonché il pieno rispetto degli obblighi, delle garanzie e delle procedure previsti dalla LGPD, nella misura in cui ciò sia compatibile con il settore pubblico<sup>65</sup>.
- (76) Nonostante questa importante sentenza dell'organo giurisdizionale di grado più elevato del Brasile, data la complessità di cui si è già fatta menzione, l'ambito e le modalità di applicazione esatti della LGPD alle autorità di contrasto, l'EDPB invita la Commissione a monitorare attentamente gli sviluppi e la prassi in tale ambito.
- (77) Per quanto riguarda il trasferimento successivo di dati personali verso autorità di contrasto in materia penale di paesi terzi, il progetto di decisione fa riferimento all'articolo 33, punto III, LGPD che stabilisce che i trasferimenti internazionali di dati possono aver luogo quando sono "necessari per la cooperazione giuridica internazionale tra enti pubblici di intelligence, indagine e azione penale, conformemente agli strumenti giuridici internazionali"<sup>66</sup>. L'EDPB ritiene che tale spiegazione sia troppo generica e invita la Commissione ad approfondire

---

<sup>64</sup> Cfr. la sentenza della CGUE del 6 ottobre 2020, cause riunite *La Quadrature du Net e altri*, C-511/18 e C-512/18, ECLI:EU:C:2020:791, punti da 95 a 98, sentenza del 2 ottobre 2018, *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788, punti 54, 57 e 60, (sentenza del 2 marzo 2021, *Prokuratuur* (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche), C-746/18, ECLI:EU:C:2021:152, punto 35.

<sup>65</sup> Cfr. il considerando 187 del progetto di decisione.

<sup>66</sup> Ibidem.

ulteriormente nel progetto di decisione le condizioni e le garanzie che disciplinano i trasferimenti successivi.

### 3.1.4 Vigilanza e mezzi di ricorso

- (78) L'EDPB ricorda che qualsiasi ingerenza nel diritto al rispetto della vita privata e alla protezione dei dati deve essere soggetta a un sistema di vigilanza efficace, indipendente e imparziale che deve essere previsto da un giudice o da un altro organo indipendente (ad esempio un'autorità amministrativa o un organo parlamentare)<sup>67</sup>.
- (79) L'EDPB rileva inoltre che nel quadro brasiliano, come descritto dalla Commissione, le attività delle autorità di contrasto in materia penale sono soggette a vigilanza da parte di diversi organismi: i) il sistema giudiziario; ii) l'ANPD; e iii) la procura.
- (80) Il controllo giurisdizionale, come spiegato sopra nella sezione dedicata alla necessità e alla proporzionalità<sup>68</sup>, si applica in relazione alla raccolta di dati personali e all'accesso agli stessi, in particolare sotto forma di riesame e autorizzazione ex ante.
- (81) Per quanto riguarda il ruolo dell'ANPD, come già spiegato nella sezione 3.1.1. del presente parere, il progetto di decisione di adeguatezza ricorda che, ai sensi dell'articolo 4, punto III, LGPD, tale legge non si applica al trattamento dei dati personali effettuato *esclusivamente* a fini di i) pubblica sicurezza; ii) difesa nazionale; iii) sicurezza dello Stato e iv) indagine e perseguimento di reati. Inoltre l'articolo 4, punto I, stabilisce che tale trattamento sarà disciplinato da una normativa specifica che, tra le altre cose, dovrà comprendere i principi generali di protezione e i diritti degli interessati, quali delineati nella LGPD. Il terzo comma dello stesso articolo riconosce all'ANPD un ruolo consultivo in relazione alle eccezioni previste al punto III quando il trattamento è effettuato esclusivamente per tali finalità; in particolare riconosce i poteri dell'ANPD di emettere raccomandazioni e pareri tecnici, nonché di richiedere valutazioni d'impatto sulla protezione dei dati ai relativi titolari del trattamento.
- (82) Nel suo progetto di decisione<sup>69</sup>, la Commissione fa riferimento a un'importante decisione del 15 settembre 2022 della Corte suprema federale, che indica l'applicabilità dei principi generali di protezione dei dati e dei diritti degli interessati al trattamento dei dati personali da parte dello Stato per la fornitura di servizi pubblici. Tale decisione si concentra sulla "condivisione dei dati personali" tra organismi ed enti della pubblica amministrazione e nelle attività di intelligence, nonché sull'"accesso delle agenzie e degli enti pubblici" al registro di base dei cittadini. Per quanto riguarda il ruolo esecutivo dell'ANPD, l'EDPB apprende dalle informazioni aggiuntive fornite dalla Commissione che l'ANPD ha già esercitato tale ruolo rispetto alla polizia e al ministero della Giustizia e della pubblica sicurezza. Ciò è avvenuto sulla base della giurisprudenza che, estendendo l'applicabilità parziale dei principi generali e dei diritti degli interessati al trattamento effettuato per motivi di contrasto penale, attribuisce all'ANPD la responsabilità di vigilare e applicare la legislazione anche in tale ambito.
- (83) Alla luce di quanto sopra, l'EDPB invita la Commissione ad approfondire ulteriormente il ruolo esecutivo dell'ANPD, in particolare per quanto riguarda le basi giuridiche pertinenti e i suoi

<sup>67</sup> Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza adottate il 10 novembre 2020, cfr. pagina 12:

[https://www.edpb.europa.eu/sites/default/files/files/file1/edpb\\_recommendations\\_202002\\_europeanessentialquaranteessurveillance\\_it.pdf](https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialquaranteessurveillance_it.pdf).

<sup>68</sup> Cfr. la sezione 3.1.2.

<sup>69</sup> Cfr. il considerando 187 del progetto di decisione.

poteri di indagine e correttivi rispetto alle autorità di contrasto, e a monitorare attentamente gli sviluppi in tale ambito.

- (84) L'EDPB osserva infine che la procura ha una competenza che va al di là della vigilanza delle norme in materia di protezione dei dati e vita privata e dell'imposizione di sanzioni per le violazioni dei diritti fondamentali. Ad esempio, come già spiegato nella sezione 3.1 del presente parere, ai sensi della legge sulle associazioni a delinquere e sulle indagini penali, la procura è una delle autorità che può accedere senza autorizzazione giudiziaria ai dati di registrazione di una persona indagata. L'EDPB invita pertanto la Commissione ad approfondire e chiarire ulteriormente nel progetto di decisione il ruolo e i poteri della procura in relazione alla vigilanza sul trattamento dei dati personali da parte delle autorità di contrasto brasiliane.
- (85) Per quanto riguarda il ricorso, l'EDPB rileva con soddisfazione che i meccanismi giuridici descritti nella prima parte del presente parere, e in particolare i rimedi giurisdizionali a disposizione delle persone fisiche per far valere i loro diritti alla protezione dei dati e alla vita privata, si applicano anche in relazione alle attività degli organismi di contrasto in materia penale.

## **3.2 Accesso e uso da parte delle autorità pubbliche brasiliane per finalità di sicurezza nazionale**

### **3.2.1 Ambito dell'esenzione di cui all'articolo 4, punto III, LGPD e sua applicabilità ai reati contro la sicurezza dello Stato**

- (86) Come introdotto dalla Commissione, l'articolo 4, punto III, LGPD esenta la "sicurezza dello Stato" dall'applicazione della LGPD al trattamento dei dati personali, insieme alla sicurezza pubblica, alla difesa nazionale e alle attività di indagine e perseguimento di reati.
- (87) L'EDPB rileva che la legislazione brasiliana in materia di "*Seguranca Nacional*" (sicurezza nazionale), come stabilito dalla legge n. 14.197 del 1° settembre 2021 che modifica il codice penale e revoca la legge del 1983 sulla sicurezza nazionale<sup>70</sup>, esprime il concetto brasiliano di sicurezza nazionale sulla base di un elenco esaustivo di reati<sup>71</sup> che riguardano diverse minacce all'integrità dello Stato brasiliano come istituzione (sovranità nazionale, spionaggio (art. 350-K), reati contro le istituzioni democratiche (art. 359-L) et al.). Le norme della legge n. 14.197 sono state inserite come parte integrante del codice penale brasiliano.
- (88) Ciò detto, l'EDPB si aspetterebbe che il trattamento dei dati da parte delle autorità brasiliane per il perseguimento di reati di cui alla legge n. 14.197 sia disciplinato dal regime applicabile all'accesso e all'uso da parte delle autorità brasiliane per motivi di contrasto penale, come descritto alla sezione 3.2 del progetto di decisione, e che sia quindi soggetto alle stesse considerazioni in materia di protezione dei dati di cui alla sezione 3.1 del presente parere. L'EDPB chiede pertanto alla Commissione di chiarire nel progetto di decisione se il trattamento dei dati relativo al perseguimento di reati di cui alla legge n. 14.197 sia effettivamente disciplinato dal regime di protezione dei dati applicabile alle attività di contrasto o da un altro regime. In quest'ultimo caso, l'EDPB invita la Commissione a fornire ulteriori

<sup>70</sup> Legge n. 14.197 del 1° settembre 2021, disponibile all'indirizzo: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2021/lei/l14197.htm](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14197.htm) (02.10.2026).

<sup>71</sup> Cfr. il considerando 200 del progetto di decisione.

chiarimenti sulle norme in materia di protezione dei dati applicabili al perseguimento di tali reati per motivi di sicurezza nazionale.

### 3.2.2 Quadro giuridico per la sicurezza nazionale

- (89) Il quadro giuridico codificato su cui si basa il progetto di decisione nella sezione dedicata all'accesso da parte di pubbliche amministrazioni per "finalità di sicurezza nazionale" è costituito dalla legge n. 14.197 del 2021, dalla legge n. 9.883 del 7 dicembre 1999 che istituisce il sistema di intelligence brasiliano e dal relativo decreto n. 4.376 del 2002. Gli ultimi due atti legislativi citati istituiscono il sistema di intelligence brasiliano (*Sistema Brasileiro des Inteligência*, SISBIN) e ne regolano il funzionamento. A questi seguono il decreto presidenziale n. 8.793<sup>72</sup> del 2016, vincolante, che definisce la politica di intelligence nazionale (la cosiddetta *Política Nacional de Inteligência*, PNI), nonché la LGPD del 2018.
- (90) Il decreto presidenziale n. 8.793 del 2016 descrive l'oggetto, gli obiettivi e i limiti della PNI. Le attività previste da tale decreto mirano a produrre e diffondere tra le autorità competenti conoscenze relative a fatti e situazioni che si verificano all'interno o all'esterno del territorio nazionale e che hanno un'influenza immediata o potenziale sul processo decisionale, sull'azione governativa, sulla sicurezza della società e sui servizi di intelligence dello Stato. In tali circostanze, per intelligence si intende l'insieme delle informazioni (e dei dati) necessarie e trattate al fine di sostenere il processo decisionale del ramo esecutivo in tale ambito.
- (91) Secondo la base giuridica del SISBIN presentata dalla Commissione, il SISBIN e le sue entità sono stati istituiti come meccanismo centrale per l'attuazione della PNI e, in quanto tali, sono incaricati di svolgere attività relative alla sicurezza nazionale, alla pubblica sicurezza, all'incolumità pubblica e alla protezione delle istituzioni democratiche. A tal fine, il SISBIN prevede lo scambio di conoscenze e la pianificazione integrata delle attività<sup>73</sup>. Di conseguenza, alla luce delle attività del SISBIN, il concetto di sicurezza nazionale in Brasile non sembra limitarsi esclusivamente ai reati codificati nella legge n. 14.197 ma potrebbe essere considerato parte integrante di un concetto più ampio di intelligence nazionale.
- (92) Il SISBIN è stato inizialmente istituito con diciotto entità federali, tra cui tredici ministeri, e successivamente esteso a 48 cosiddette agenzie con il decreto n. 11.693, del 6 settembre 2023, sull'organizzazione e sul funzionamento del SISBIN<sup>74</sup>. L'EDPB rileva che la cooperazione nell'ambito del SISBIN integra entità che vanno oltre le classiche istituzioni di sicurezza, quali il ministero della Scienza (art. 4, punto IV), dell'Agricoltura (art. 4, punto XV) e dell'Energia (art. 4, punto XVIII) e il Procuratore generale federale (art. 4, punto XIX).
- (93) Mentre il decreto n. 4.376 del 2002 ha incaricato il consiglio consultivo del sistema di intelligence brasiliano di proporre norme e procedure generali per lo scambio di "conoscenze e comunicazioni" all'interno del SISBIN<sup>75</sup>, il decreto n. 11.693 del 2023 affida all'organo centrale del SISBIN il compito di produrre strumenti tecnici<sup>76</sup> per la condivisione di dati e conoscenze e descrive la condivisione e l'utilizzo dei dati ottenuti dalle entità del SISBIN. Il progetto di decisione della Commissione non fornisce tuttavia ulteriori informazioni su tali

<sup>72</sup> Cfr. il considerando 199 del progetto di decisione.

<sup>73</sup> La sezione 5 del decreto presidenziale n. 8.793 indica il SISBIN e gli organi che ne fanno parte, lo scambio di conoscenze all'interno del SISBIN e la pianificazione integrata della cooperazione tra i membri del SISBIN come strumenti per l'attuazione della PNI.

<sup>74</sup> Cfr. il considerando 202 del progetto di decisione.

<sup>75</sup> Cfr. l'articolo 7, punto II, del decreto n. 4.376.

<sup>76</sup> Cfr. l'articolo 10, punto XI, disponibile all'indirizzo: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2023-2026/2023/decreto/d11693.htm](https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11693.htm) (26.09.2025).

norme o standard giuridici emanati dall'organo centrale, ad esempio quando le entità del SISBIN condividono tra loro dati personali.

- (94) Inoltre sembrano esistere differenze nei concetti di sensibilità delle informazioni, dato che, ai sensi della legge che disciplina le attività del SISBIN, la sensibilità è correlata al grado di riservatezza attribuito a un'informazione<sup>77</sup>, e di limitazione delle finalità rispetto ai principi generali del GDPR<sup>78</sup>.
- (95) Come già spiegato sopra, l'articolo 4, punto III, lettere da a) a c), LGPD, codificato solo dopo l'istituzione del SISBIN e la definizione di una politica nazionale in materia di intelligence, esenta dall'applicazione della LGPD i trattamenti di dati effettuati esclusivamente a fini di pubblica sicurezza, difesa nazionale e sicurezza dello Stato, fatta eccezione per i principi generali stabiliti in materia di protezione dei dati.
- (96) Come sottolineato dalla Commissione nel progetto di decisione, il quadro costituzionale globale del Brasile nonché la partecipazione del Brasile alla Corte interamericana dei diritti umani rientrano nel quadro giuridico per l'accesso delle pubbliche amministrazioni a fini di intelligence nazionale. L'EDPB riconosce inoltre che anche le sentenze della Corte suprema federale brasiliana hanno svolto un ruolo importante nella definizione del panorama giuridico<sup>79</sup>. Le sentenze della Corte suprema finora hanno rappresentato un sostegno conciso e pertinente per l'ulteriore sviluppo della protezione dei dati personali in conformità della costituzione brasiliana. Allo stesso tempo, occorre ricordare che le sentenze della Corte suprema non specificano né stabiliscono norme generali astratte in materia di protezione dei dati per il trattamento dei dati personali ma interpretano le disposizioni e i principi della costituzione e della LGPD.
- (97) L'EDPB è consapevole del fatto che agli Stati è concesso un ampio margine di discrezionalità nella definizione delle questioni di sicurezza nazionale, il che consente poi di applicare esenzioni per motivi di sicurezza nazionale al trattamento dei dati personali. In tale contesto, l'EDPB ricorda la definizione data dalla Corte europea dei diritti dell'uomo, secondo cui le minacce alla sicurezza nazionale devono distinguersi, per loro natura, gravità e specificità delle circostanze, dai rischi generali per la sicurezza pubblica o dai reati gravi<sup>80</sup>.
- (98) È opinione dell'EDPB che i dati trattati dalle entità del SISBIN beneficino dell'esenzione di cui all'articolo 4, punto III, LGPD solo quando il trattamento è effettuato *esclusivamente* a fini di pubblica sicurezza, difesa nazionale e sicurezza dello Stato. Ciò sembra applicarsi in modo specifico alle attività dell'organo centrale del SISBIN, l'Agenzia brasiliana di intelligence (ABIN). Di conseguenza, a meno che un'entità del SISBIN non agisca per conto dell'ABIN per una di queste finalità, la LGPD si applica integralmente.
- (99) L'EDPB invita la Commissione a confermare tale interpretazione e a descrivere e spiegare in modo più preciso nel progetto di decisione i contorni del concetto di sicurezza nazionale ai sensi del diritto brasiliano, in particolare per quanto riguarda la raccolta e la condivisione di dati tra e da parte di entità per conto delle attività del SISBIN e per quanto riguarda l'attuazione della PNI. A questo proposito, l'EDPB invita la Commissione a chiarire anche in che modo le esenzioni dalla LGPD per motivi di sicurezza nazionale si rapportano all'esenzione per motivi di sicurezza nazionale prevista dal GDPR.

<sup>77</sup> Cfr. il decreto n. 8.793 del 2016, decreto n. 11.693, considerando 204 del progetto di decisione.

<sup>78</sup> Cfr. l'articolo 6, punto I, LGPD, relativo a finalità legittime e specifiche, mentre il GDPR richiede finalità lecite e specifiche.

<sup>79</sup> Cfr. il considerando 203 del progetto di decisione.

<sup>80</sup> Corte EDU, *Big Brother Watch e altri/Regno Unito*, 25 maggio 2021, punto 350.

### 3.2.3 Trasferimenti successivi e accordi internazionali

- (100) L'articolo 33 LGPD definisce le condizioni preliminari per il trasferimento internazionale di dati. L'articolo 33, punti I e II, LGPD stabilisce requisiti simili a una decisione di adeguatezza o ai requisiti per garanzie supplementari ai sensi del GDPR. Una deroga a tali requisiti è prevista all'articolo 33, punti III, VI e VII, LGPD, che disciplina i casi di "cooperazione giuridica tra enti di intelligence", i trasferimenti effettuati in ottemperanza a "un impegno assunto nell'ambito di accordi di cooperazione internazionale" e i trasferimenti "necessari per l'applicazione di una politica pubblica o di un'attribuzione giuridica al servizio pubblico", vale a dire la sicurezza nazionale e l'intelligence nazionale. Tale decisione sembra essere in linea con il concetto di cui all'articolo 4, punto III, LGPD, che limita l'applicazione della LGPD esclusivamente ai suoi principi per quanto riguarda le questioni di pubblica sicurezza, difesa nazionale e sicurezza dello Stato. Si potrebbe quindi ritenere che i trasferimenti successivi a fini di intelligence nazionale debbano essere effettuati nel rispetto dei principi generali in materia di protezione dei dati della LGPD, pur essendo soggetti alle disposizioni in materia di cooperazione internazionale previste dagli atti giuridici che istituiscono la PNI e il SISBIN.
- (101) Ciò premesso, l'EDPB riconosce che il Brasile può avere la necessità di trasmettere e di fatto trasmette dati personali a servizi di intelligence stranieri a fini di cooperazione o al fine di attuare la PNI in linea con l'obiettivo di prevenire e individuare minacce sulla base del suddetto concetto integrato di sicurezza.
- (102) Come esposto in precedenza, la Commissione sottolinea l'applicabilità del quadro costituzionale globale del Brasile e la garanzia dell'*habeas data* per la protezione dei dati personali all'interno del SISBIN, che si applicano anche ai trasferimenti successivi a fini di sicurezza nazionale. L'EDPB invita la Commissione a chiarire ulteriormente la base giuridica nonché le garanzie e le condizioni in materia di protezione dei dati che l'ABIN e gli altri membri del SISBIN sono tenuti a prendere in considerazione prima di divulgare a partner stranieri dati personali a fini di intelligence nazionale.
- (103) L'EDPB rileva inoltre che la Commissione non ha integrato nella sua valutazione dell'adeguatezza considerazioni relative all'esistenza di accordi internazionali conclusi tra il Brasile e paesi terzi o organizzazioni internazionali. Poiché la LGPD non prevede una normativa vincolante al di là dei principi generali di protezione dei dati, tali accordi potrebbero contenere disposizioni specifiche per il trasferimento internazionale dei dati personali detenuti dall'ABIN o dagli altri membri del SISBIN verso paesi terzi. L'EDPB ritiene che la conclusione di accordi bilaterali o multilaterali con paesi terzi per finalità di intelligence nazionale possa incidere sul quadro giuridico in materia di protezione dei dati applicabile.
- (104) L'EDPB invita pertanto la Commissione a chiarire se esistono simili accordi internazionali per finalità di intelligence nazionale e a valutare il loro potenziale impatto sul livello di protezione garantito ai dati personali trasferiti dal SEE al Brasile in relazione al quadro giuridico valutato in via preliminare per il trattamento dei dati a fini di intelligence nazionale.

### 3.2.4 Vigilanza e mezzi di ricorso

- (105) Il progetto di decisione di adeguatezza presenta diversi organismi incaricati di vigilare sulle attività condotte dalle autorità brasiliane di sicurezza nazionale, in particolare i) l'organo esecutivo; ii) l'organo legislativo; iii) l'ANPD; e iv) il sistema giudiziario. Per quanto riguarda l'ANPD, l'EDPB ricorda le considerazioni e le conclusioni formulate nella sezione 3.1.4 del presente parere, che rimangono valide anche in questo caso.

- (106) Secondo il progetto di decisione, la Camera delle relazioni esterne e della difesa nazionale del Consiglio del governo è responsabile della vigilanza dell'attuazione delle attività condotte dalla polizia nazionale di intelligence mentre l'Ufficio per la sicurezza istituzionale è responsabile del coordinamento dell'attività di intelligence federale. L'EDPB osserva che tale controllo si limita a garantire il raggiungimento degli obiettivi del sistema di intelligence e la loro attuazione, ma non include alcun potere di indagine o sanzionatorio e non riguarda il trattamento effettivo dei dati personali.
- (107) Spetta infatti alla commissione mista di vigilanza delle attività di intelligence (CCAI) (organo legislativo) esercitare il controllo in relazione alle attività di intelligence, anche per quanto riguarda la legittimità e l'efficacia. L'EDPB accoglie con favore il rafforzamento della struttura e dei poteri della CCAI, che ha determinato una maggiore trasparenza delle sue attività e consentito all'organo di esercitare un controllo adeguato, ad esempio effettuando revisioni a posteriori, audit e controlli delle operazioni in corso. L'EDPB rileva inoltre con soddisfazione che la CCAI è in grado di gestire i reclami degli interessati nell'ambito della sua competenza di indagare sui reclami relativi a violazioni dei diritti e delle garanzie fondamentali.
- (108) La competenza del sistema giudiziario a giudicare le cause intentate dai cittadini contro le autorità pubbliche è un aspetto positivo, in particolare perché consente il controllo giurisdizionale delle attività svolte in nome della sicurezza nazionale, garantendo il rispetto, tra l'altro, dei diritti costituzionali (compreso il diritto alla protezione dei dati) e della LGPD. L'EDPB rileva con soddisfazione che è prevista la possibilità di ricorso dinanzi alla Corte suprema federale e, in ultima istanza, dinanzi alla Corte interamericana dei diritti umani.
- (109) È opinione dell'EDPB che, nel contesto delle attività di intelligence nazionale, agli interessati siano garantiti i) i diritti sanciti dalla LGPD (in seguito alla sentenza della Corte suprema federale del 15 settembre 2022); ii) il diritto di ottenere l'accesso e la rettifica dei dati personali attraverso il mezzo di ricorso costituzionale dell'*habeas data*; nonché iii) il diritto al risarcimento dei danni materiali e immateriali.
- (110) L'EDPB accoglie con favore l'esistenza di tali diritti e il fatto che essi possano essere invocati attraverso meccanismi giudiziari e amministrativi, in particolare la CCAI, nonché il fatto che tali vie di ricorso siano accessibili a tutte le persone fisiche, indipendentemente dalla cittadinanza.

## 4. ATTUAZIONE E MONITORAGGIO DEL PROGETTO DI DECISIONE

- (111) Per quanto riguarda il monitoraggio e il riesame del progetto di decisione, l'EDPB osserva che, secondo la giurisprudenza della CGUE, "alla luce del fatto che il livello di protezione assicurato da un paese terzo può evolversi, incombe alla Commissione, successivamente all'adozione di una decisione [di adeguatezza] in forza [dell'articolo 45 GDPR], verificare periodicamente se la constatazione relativa al livello di protezione adeguato assicurato dal paese terzo in questione continui ad essere giustificata in fatto e in diritto. Una siffatta verifica è in ogni caso obbligatoria quando taluni indizi facciano sorgere un dubbio al riguardo"<sup>81</sup>.

---

<sup>81</sup> Sentenza *Schrems I* della CGUE, punto 76. Cfr. anche l'articolo 3, paragrafo 4, del progetto di decisione.

- (112) L'EDPB rileva che la revisione della constatazione di adeguatezza avrà luogo almeno ogni quattro anni, conformemente all'articolo 45, paragrafo 3, GDPR<sup>82</sup>.
- (113) L'EDPB accoglie con favore il fatto che il progetto di decisione, al considerando 230, preveda la partecipazione dell'EDPB all'incontro organizzato tra la Commissione e le autorità brasiliane e dedicato al riesame del funzionamento della decisione di adeguatezza. Per quanto concerne il coinvolgimento pratico dell'EDPB e dei suoi rappresentanti nella preparazione e nello svolgimento dei futuri riesami periodici, l'EDPB ribadisce che qualsiasi documentazione pertinente, compresa la corrispondenza, dovrebbe essere condivisa per iscritto con l'EDPB con sufficiente anticipo rispetto ai riesami.

Per il Comitato europeo per la protezione dei dati

La presidente

(Anu Talus)

---

<sup>82</sup> Cfr. il considerando 229 e l'articolo 3, paragrafo 4, del progetto di decisione.