DECISIONE DI ESECUZIONE (UE) 2026/179 DELLA COMMISSIONE

del 26 gennaio 2026

a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio sul livello di protezione adeguato dei dati personali da parte del Brasile

[notificata con il numero C(2026) 373]

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il 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 (regolamento generale sulla protezione dei dati) ([1]), in particolare l'articolo 45, paragrafo 3,

considerando quanto segue:

1. INTRODUZIONE

(1) Il regolamento (UE) 2016/679 stabilisce le norme per il trasferimento di dati personali da titolari del trattamento o responsabili del trattamento nell'Unione verso paesi terzi e organizzazioni internazionali nella misura in cui tale trasferimento rientri nel suo ambito di applicazione. Le norme sui trasferimenti internazionali di dati sono stabilite nel capo V (articoli da 44 a 50) di tale regolamento. Sebbene la circolazione di dati personali verso e da paesi al di fuori dell'Unione europea sia essenziale per l'espansione degli scambi transfrontalieri e della cooperazione internazionale, occorre garantire che il livello di protezione offerto ai dati personali nell'Unione europea non sia compromesso da trasferimenti verso paesi terzi ([2]).

(2) Ai sensi dell'articolo 45, paragrafo 3, del regolamento (UE) 2016/679 la Commissione può decidere, mediante atti di esecuzione, che un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo, o un'organizzazione internazionale garantiscono un livello di protezione adeguato. Nel rispetto di tale condizione, i trasferimenti di dati personali verso un paese terzo possono avvenire senza la necessità di ottenere ulteriori autorizzazioni, come previsto dall'articolo 45, paragrafo 1, e dal considerando 103 di tale regolamento.

(3) Come specificato all'articolo 45, paragrafo 2, del regolamento (UE) 2016/679, l'adozione della decisione di adeguatezza deve basarsi su un'analisi completa dell'ordinamento giuridico del paese terzo, per quanto riguarda tanto le norme applicabili agli importatori di dati quanto le limitazioni e le garanzie relative all'accesso ai dati personali da parte delle autorità pubbliche. Nella propria valutazione la Commissione deve stabilire se il paese terzo in questione assicura un livello di protezione «sostanzialmente equivalente» a quello garantito all'interno dell'Unione europea ([3]). Il criterio rispetto al quale viene valutata l'«equivalenza sostanziale» è quello stabilito dalla legislazione dell'Unione europea, in particolare il regolamento (UE) 2016/679, nonché dalla giurisprudenza della Corte di giustizia dell'Unione europea ([4]). Anche i «criteri di riferimento per l'adeguatezza» del comitato europeo per la protezione dei dati (EDPB) sono importanti al riguardo, al fine di chiarire ulteriormente tale criterio e fornire orientamenti ([5]).

([1]) GU L 119 del 4.5.2016, pag. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj.
([2]) Considerando 101 del regolamento (UE) 2016/679.
([3]) Considerando 104 del regolamento (UE) 2016/679.
([4]) Cfr. sentenza della Corte di giustizia del 16 luglio 2020, Facebook Ireland e Schrems («Schrems II»), C-311/18, ECLI:EU:C:2020:559.
([5]) Cfr. anche comitato europeo per la protezione dei dati, Criteri di riferimento per l'adeguatezza, WP 254 rev. 01, disponibile all'indirizzo: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

(4) Come chiarito dalla Corte di giustizia dell'Unione europea, un paese terzo non può essere tenuto ad assicurare un livello di protezione identico a quello garantito nell'ordinamento giuridico dell'UE ([6]). In particolare gli strumenti dei quali il paese terzo in questione si avvale per proteggere i dati personali possono essere diversi da quelli attuati all'interno dell'Unione, purché si rivelino efficaci, nella prassi, al fine di assicurare un livello di protezione adeguato ([7]). Il livello di adeguatezza non comporta pertanto una duplicazione pedissequa delle norme dell'Unione. Si tratta piuttosto di determinare se il sistema straniero nel suo insieme, tramite il contenuto essenziale dei diritti alla riservatezza e delle garanzie in materia di protezione dei dati (compresi l'attuazione, l'azionabilità e il controllo effettivi), nonché tramite le circostanze relative ad un trasferimento di dati personali, offre il necessario livello di protezione ([8]).

(5) La Commissione ha analizzato la legge e la prassi della Repubblica federativa del Brasile («Brasile»). Sulla base delle conclusioni di cui ai considerando da 7 a 223, la Commissione conclude che il Brasile garantisce un livello di protezione adeguato per i dati personali trasferiti dall'Unione europea al Brasile nell'ambito di applicazione del regolamento (UE) 2016/679.

(6) Per effetto della presente decisione i trasferimenti da titolari del trattamento e responsabili del trattamento nell'Unione a titolari del trattamento e responsabili del trattamento in Brasile possono aver luogo senza la necessità di ottenere ulteriori autorizzazioni. La presente decisione non incide sull'applicazione diretta del regolamento (UE) 2016/679 a tali soggetti qualora siano soddisfatte le condizioni relative all'ambito di applicazione territoriale di detto regolamento, di cui all'articolo 3 dello stesso.

2. NORME CHE SI APPLICANO AL TRATTAMENTO DEI DATI PERSONALI

2.1. Il quadro costituzionale del Brasile

(7) Il Brasile è una Repubblica federativa composta dall'unione di 26 Stati e del Distretto federale, come stabilito nella sua costituzione federale («costituzione») ([9]). Anche gli Stati brasiliani hanno le proprie costituzioni, che non devono essere in contrasto con la costituzione federale ([10]). Il Brasile ha un sistema presidenziale in cui il presidente e i membri delle camere legislative (ossia la Camera dei deputati e il Senato federale) sono eletti direttamente.

(8) La vita privata e la protezione dei dati sono tutelate dalla costituzione in quanto diritti fondamentali. Più specificamente, l'articolo 5, punto X, della costituzione tutela l'intimità e la vita privata delle persone, mentre l'articolo 5, punto XII, garantisce la segretezza delle comunicazioni di corrispondenza, compresi i dati, e l'articolo 5, punto LXXIX, sancisce il diritto alla protezione dei dati personali online e offline ([11]).

(9) Tutti i diritti previsti dalla costituzione sono applicabili ai brasiliani e agli stranieri residenti in Brasile a norma dell'articolo 5 della stessa. Le leggi federali hanno chiarito che chiunque si trovi nel territorio del Brasile, ivi residente o meno, ha diritto alla tutela dei diritti fondamentali ([12]). La portata della tutela di tali diritti è stata ulteriormente estesa dalla giurisprudenza costituzionale agli stranieri che vivono all'estero, come evidenziato anche dalla dottrina giuridica pertinente ([13]). Pertanto qualsiasi straniero, residente o meno in Brasile, può invocare tali tutele costituzionali ([14]).

([6]) Sentenza della Corte di giustizia del 6 ottobre 2015, Schrems («Schrems I»), C-362/14, ECLI:EU:C:2015:650, punto 73.
([7]) Schrems I, punto 74.
([8]) Schrems I, punto 75.
([9]) Costituzione della Repubblica federativa del Brasile del 1988, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.
([10]) Articolo 25 della costituzione della Repubblica federativa del Brasile del 1988.
([11]) Emendamento costituzionale n. 115 del 10 febbraio 2022, disponibile all'indirizzo: http://www.planalto.gov.br/ccivil_03/Constituicao/Emendas/Emc/emc115.htm#art1.
([12]) Cfr. ad esempio l'articolo 4, punto XIII, della legge n. 13.445 del 24 maggio 2017 (legge sull'immigrazione), disponibile all'indirizzo https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13445.htm#:~:text=Institui%20a%20Lei%20de%20Migra%C3%A7%C3%A3o.&text=Art.,pol%C3%ADticas%20p%C3%BAblicas%20para%20o%20emigrante.
([13]) Cfr. ad esempio FERREIRA FILHO, Manoel Gonçalves. *Direitos humanos fundamentais*. 6. ed., San Paolo: Saraiva, 2004.
([14]) Sentenza del *Superior Tribunal de Justiça*, 4a Turma, 2016, disponibile all'indirizzo: https://www.jusbrasil.com.de/jurisprudencia/stj/863001318.

(10) Nel 1992 il Brasile ha ratificato la Convenzione americana sui diritti dell'uomo, nota come «Patto di San José» («Convenzione») ([15]). Tra le altre disposizioni, l'articolo 11 della Convenzione garantisce il diritto alla vita privata e l'articolo 8 tutela il diritto a un equo processo. Nel 1998 il Brasile ha riconosciuto l'autorità vincolante della Corte interamericana dei diritti umani per l'interpretazione e l'applicazione della Convenzione ([16]). La Corte può emettere decisioni relative all'applicazione dei diritti nell'ambito delle attività svolte dalle autorità pubbliche in Brasile, comprese le autorità che si occupano di pubblica sicurezza e difesa ([17]).

2.2. **Il quadro per la protezione dei dati in Brasile**

(11) Nel 2018 il Brasile ha adottato una normativa generale in materia di protezione dei dati che fornisce garanzie a tutte le persone fisiche, indipendentemente dalla cittadinanza: la legge generale sulla protezione dei dati (Lei Geral de Proteção de Dados, LGPD) ([18]).

(12) Dopo l'adozione la LGPD è stata rafforzata e chiarita attraverso ulteriori atti legislativi. In particolare, tramite la legge n. 13.853 del 2019 è stata istituita l'autorità per la protezione dei dati del Brasile (*Agência Nacional de Proteção de Dados*, ANPD) ([19]), che è stata trasformata in un'autorità indipendente mediante una legge adottata nel 2022 ([20]). Tali disposizioni sono state integrate da altri decreti vincolanti, fra l'altro per migliorare lo status dell'ANPD ([21]), definirne ulteriormente la composizione e la procedura di nomina dei direttori ([22]).

(13) Come descritto più dettagliatamente nei considerando da 125 a 141 della presente decisione, l'ANPD è l'autorità responsabile dell'interpretazione e dell'applicazione della LGPD. In tale contesto, l'ANPD emana a scadenze regolari regolamenti vincolanti per l'interpretazione e l'applicazione della legge. Ad esempio, ha adottato diversi regolamenti per rafforzare ulteriormente il regime sanzionatorio e specificare le norme sulla notifica delle violazioni dei dati ([23]). Ulteriori orientamenti sull'applicazione e sull'interpretazione della LGPD sono forniti dall'ANPD attraverso documenti e guide, come quelli adottati sull'interpretazione della base giuridica (ad esempio, l'interesse legittimo) e dei concetti chiave nell'ambito della LGPD (ad esempio sanzioni, responsabile della protezione dei dati).

([15]) Elenco dei firmatari e ratifica della Convenzione americana sui diritti dell'uomo, disponibile all'indirizzo: http://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights_sign.htm.

([16]) Dichiarazione del Brasile relativa alla Convenzione, disponibile all'indirizzo: http://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights_sign.htm#Brazil.

([17]) Cfr. ad esempio, Escher et al. c. Brazil, sentenza del 6 luglio 2009, disponibile all'indirizzo: https://www.corteidh.or.cr/docs/casos/articulos/seriec_200_ing.pdf.

([18]) Legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati, disponibile all'indirizzo: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm, disponibile in inglese all'indirizzo: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/lgpd-en-lei-no-13-709-capa.pdf.

([19]) Legge n. 13.853 dell'8 luglio 2019 che modifica la LGPD al fine, tra l'altro, di istituire l'autorità per la protezione dei dati - *Autoridade Nacional de Proteção de Dados* (ANPD), disponibile all'indirizzo: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art2.

([20]) Legge n. 14.460, del 25 ottobre 2022, che trasforma l'ANPD in un'autorità con status speciale, disponibile all'indirizzo: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Lei/L14460.htm#art7.

([21]) Decreto n. 1.317 del 17 settembre 2025 che modifica l'LGPD per trasformare l'*Agência Nacional de Proteção de Dados*, disponibile all'indirizzo: https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314.

([22]) Decreto n. 10.474 del 26 agosto 2020 che istituisce l'ANPD e ne definisce la composizione, disponibile all'indirizzo: https://www.in.gov.br/en/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226. Decreto n. 11.758, del 30 ottobre 2023, che modifica la composizione dell'ANPD, disponibile all'indirizzo: http://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11758.htm. Decreto del 5 novembre 2020 sulla nomina dei direttori dell'ANPD. disponibile all'indirizzo: https://www.in.gov.br/en/web/dou/-/decretos-de-5-de-novembro-de-2020-286734594.

([23]) Cfr. l'elenco dei regolamenti dell'ANPD, disponibile all'indirizzo: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes e in particolare il regolamento n. 4, del 24 febbraio 2024, sull'applicazione delle sanzioni amministrative, disponibile all'indirizzo: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077 e il regolamento n. 15, del 24 aprile 2024, sulla notifica delle violazioni dei dati, disponibile all'indirizzo: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024.

(14) Nel quadro del suo impegno internazionale per la promozione e la tutela della protezione dei dati, l'ANPD del Brasile è diventata nel 2023 membro della *Global Privacy Assembly*, insieme a tutte le autorità per la protezione dei dati dell'Unione europea ([24]). Il Brasile ha anche aderito, come osservatore, al Comitato del Consiglio d'Europa per la convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato dei dati di carattere personale ([25]). Il Brasile ha inoltre svolto un ruolo guida in merito a diversi progressi compiuti in seno alle Nazioni Unite (ONU) sul diritto alla vita privata. Insieme alla Germania, il Brasile ha introdotto le risoluzioni delle Nazioni Unite sul diritto alla vita privata nell'era digitale, adottate dall'Assemblea generale delle Nazioni Unite nel 2013 e nel 2014 ([26]). Questa risoluzione dichiara fra l'altro che la sorveglianza e/o l'intercettazione illegali o arbitrarie di comunicazioni, nonché la raccolta illecita o arbitraria di dati personali, in quanto atti altamente intrusivi, violano i diritti alla vita privata e alla libertà di espressione e possono contraddire i principi di una società democratica. La risoluzione invita gli Stati a rivedere le norme sulla raccolta dei dati per allinearle al diritto internazionale in materia di diritti umani e a istituire o mantenere meccanismi di controllo nazionali indipendenti ed efficaci in grado di garantire la trasparenza, ove del caso, e la responsabilità per la sorveglianza statale delle comunicazioni, la loro intercettazione e la raccolta di dati personali ([27]).

(15) In termini di struttura e componenti principali, il quadro giuridico del Brasile che si applica al trasferimento di dati personali nell'ambito della presente decisione è simile a quello applicabile nell'Unione europea. Tale quadro non si basa soltanto sugli obblighi stabiliti dal diritto nazionale e sui diritti garantiti dalla costituzione del paese, ma anche sugli obblighi sanciti dal diritto internazionale, in particolare attraverso l'adesione da parte del Brasile alla Convenzione americana sui diritti umani e il riconoscimento della competenza giurisdizionale della Corte interamericana dei diritti umani ([28]).

2.3. **Ambito di applicazione materiale e territoriale della LGPD**

2.3.1. *Ambito di applicazione territoriale*

(16) La LGPD si applica a qualsiasi forma di trattamento di dati personali in Brasile, indipendentemente dai mezzi utilizzati per svolgere tale attività ([29]).

(17) L'articolo 3 della LGPD precisa l'ambito di applicazione territoriale della legge, indicando che essa si applica: 1) alle attività di trattamento svolte nel territorio nazionale del Brasile (che comprende l'Unione, gli Stati, il Distretto federale e i comuni); 2) alle attività di trattamento finalizzate all'offerta o alla fornitura di beni o servizi o al trattamento dei dati di persone fisiche situate nel territorio nazionale del Brasile; 3) quando i dati personali trattati sono stati raccolti nel territorio nazionale del Brasile. L'ambito è simile a quello previsto dall'articolo 3 del regolamento (UE) 2016/679.

(18) Inoltre l'articolo 3, punto II, della LGPD stabilisce che tutte le forme di trattamento dei dati personali di persone fisiche che si trovano nel territorio nazionale rientrano nell'ambito di applicazione della legge. È quindi compreso il trattamento effettuato per monitorare il comportamento delle persone nel territorio, indipendentemente dal luogo in cui i dati sono trattati.

([24]) La *Global Privacy Assembly* (GPA) è un forum che consente di coordinare le iniziative intraprese da oltre 130 autorità per la protezione dei dati e la vita privata di tutto il mondo. Cfr. l'annuncio emanato dall'ANPD quando è diventata membro della GPA, disponibile all'indirizzo: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-aceita-como-membro-pleno-no-global-privacy-assembly.

([25]) Consiglio d'Europa, osservatori del Comitato per la convenzione n. 108, disponibile all'indirizzo: https://rm.coe.int/list-of-observers-december-2022-bilingual-2781-7012-1734-1/1680a962eb.

([26]) Cfr. ad esempio la risoluzione dell'Assemblea generale delle Nazioni Unite sul diritto alla vita privata nell'era digitale, 18 dicembre 2013, disponibile all'indirizzo: https://digitallibrary.un.org/record/764407?ln=en&v=pdf.

([27]) Risoluzione dell'Assemblea generale delle Nazioni Unite sul diritto alla vita privata nell'era digitale, 18 dicembre 2013, pag. 1.

([28]) Cfr. Corte interamericana dei diritti umani, Domande e risposte sulla competenza giurisdizionale della Corte, disponibile all'indirizzo: https://www.corteidh.or.cr/que_es_la_corte.cfm?lang=en.

([29]) Articolo 3 della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

(19) Infine, secondo la giurisprudenza della Corte suprema federale (*Supremo Tribunal Federal*), le tutele in materia di diritti fondamentali previste dalla costituzione, come il diritto alla protezione dei dati, si applicano a qualsiasi persona, indipendentemente dalla cittadinanza o dalla residenza dell'interessato ([30]).

2.3.2. *Definizione di dati personali*

(20) L'articolo 5, punto I, della LGPD definisce i dati personali come informazioni riguardanti una persona fisica identificata o identificabile. La legge specifica che per «interessato» s'intende una persona fisica a cui si riferiscono i dati personali oggetto di trattamento ([31]).

(21) Inoltre le informazioni pseudonimizzate, ossia che non possono più identificare direttamente o indirettamente una persona specifica o essere associate ad essa senza utilizzare informazioni supplementari per ripristinarne lo stato originale, sono considerate dati personali ai sensi della LGPD ([32]).

(22) Al contrario le informazioni completamente anonimizzate sono escluse dall'ambito di applicazione della LGPD ([33]). Ai sensi dell'articolo 5 della LGPD, i dati anonimizzati sono dati che, tramite i mezzi ragionevoli e tecnici disponibili al momento del trattamento, non possono essere direttamente o indirettamente associati a una persona. L'articolo 12 della LGPD precisa ulteriormente che i dati anonimizzati non sono considerati dati personali, tranne quando il processo di anonimizzazione a cui i dati sono stati sottoposti è stato annullato oppure può essere annullato mediante «sforzi ragionevoli». L'articolo 12 della LGPD sottolinea inoltre che per determinare ciò che è considerato «ragionevole» si tiene conto di fattori oggettivi quali: 1) il costo e il tempo necessari per il processo di annullamento, 2) la tecnologia disponibile, 3) l'uso esclusivo dei mezzi propri del titolare del trattamento. L'approccio all'anonimizzazione e le garanzie introdotte dalla LGPD per affrontare la questione della possibilità di re-identificazione sono simili all'impostazione seguita nell'UE.

(23) Ciò corrisponde all'ambito di applicazione materiale del regolamento (UE) 2016/679 e alle nozioni ivi contenute di «dati personali», «pseudonimizzazione» e «informazioni anonimizzate».

2.3.3. *La definizione di trattamento*

(24) Le definizioni di «trattamento» adottate dall'Unione europea e dall'ordinamento brasiliano fanno entrambe riferimento a «qualsiasi operazione» effettuata in relazione a dati personali ([34]). L'articolo 5, punto X, della LGPD prevede il seguente elenco non esaustivo di attività che costituiscono un «trattamento»: raccolta, produzione, ricezione, classificazione, uso, accesso, riproduzione, trasmissione, distribuzione, trattamento, archiviazione, conservazione, cancellazione, valutazione o controllo di informazioni, modifica, comunicazione, trasferimento, diffusione o estrazione.

2.3.4. *Titolare del trattamento e responsabile del trattamento*

(25) Il concetto di titolare del trattamento è definito nella LGPD e si riferisce alla persona fisica o giuridica, sia essa pubblica o privata, responsabile delle decisioni concernenti il trattamento di dati personali ([35]).

([30]) Decisione del *Superior Tribunal de Justiça*, 4a Turma, 2016, disponibile all'indirizzo: https://www.jusbrasil.com.de/jurisprudencia/stj/863001318.

([31]) Articolo 5, punto V, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([32]) Articolo 13 della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([33]) Articolo 12 della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([34]) Articolo 5, punto X, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([35]) Articolo 5, punto VI, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

(26) Il concetto di responsabile del trattamento è definito nella LGPD e si riferisce alla persona fisica o giuridica, sia essa pubblica o privata, che effettua il trattamento di dati personali per conto del titolare del trattamento ([36]). Il responsabile del trattamento deve effettuare il trattamento secondo le istruzioni fornite dal titolare del trattamento, che è responsabile della verifica del rispetto di tali istruzioni ([37]).

(27) Il titolare del trattamento e il responsabile del trattamento devono tenere un registro delle operazioni di trattamento dei dati personali effettuate, in particolare se basate su un legittimo interesse ([38]).

(28) Ai sensi della LGPD, due o più titolari del trattamento direttamente coinvolti in un trattamento per il quale l'interessato ha subito danni sono responsabili in solido ([39]). Il responsabile del trattamento è responsabile in solido del danno causato dal trattamento se non rispetta gli obblighi della LGPD, quali definiti all'articolo 44 della stessa, o se non ha seguito le istruzioni legali del titolare del trattamento ([40]).

(29) Pertanto le norme che disciplinano il rapporto tra titolari del trattamento e responsabili del trattamento ai sensi della LGPD sono simili a quelle di cui al capo IV del regolamento (UE) 2016/679.

2.3.5. *Esenzione da determinate disposizioni della LGPD*

(30) Come nel quadro del diritto dell'Unione europea, la LGPD non si applica ai dati anonimizzati ([41]), al trattamento di dati personali per finalità puramente domestiche ([42]) o se effettuato esclusivamente a fini di pubblica sicurezza, difesa nazionale, sicurezza dello Stato o indagine e perseguimento di reati ([43]).

(31) L'esenzione nel settore della pubblica sicurezza, della difesa nazionale, della sicurezza dello Stato e dell'indagine e del perseguimento di reati è tuttavia parziale. La Corte suprema federale ha interpretato l'applicabilità della LGPD alla luce della protezione costituzionale dei dati personali e stabilito che i principi, i diritti e gli obiettivi principali della LGPD si applicano a qualsiasi trattamento dei dati personali da parte di autorità pubbliche, anche quando è condotto a fini di «intelligence» ([44]). Inoltre, l'articolo 4, paragrafi da 2 a 4, della LGPD stabilisce le condizioni per il trattamento dei dati personali a fini di sicurezza pubblica, difesa nazionale, sicurezza dello Stato o l'indagine e perseguimento di reati, in particolare per impedire ai soggetti privati di trattare i dati per tali finalità, per incaricare l'ANPD di formulare pareri tecnici e raccomandazioni in materia e per conferire all'ANPD il potere di richiedere una

([36]) Articolo 5, punto VII, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.
([37]) Articolo 39 della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.
([38]) Articolo 37 della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.
([39]) Articolo 42, paragrafo 1, punto II, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.
([40]) Articolo 42, paragrafo 1, punto I, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.
([41]) Articolo 12 della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.
([42]) Articolo 4, punto I, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.
([43]) Articolo 4, punto III, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.
([44]) Corte suprema federale, decisione sul ricorso diretto di incostituzionalità n. 6649, settembre 2022, disponibile all'indirizzo: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

valutazione d'impatto sulla protezione dei dati in relazione a tali attività ([45]). Su tale base l'ANPD ha, ad esempio, svolto indagini e emanato orientamenti, tra cui una nota tecnica indirizzata al ministero della Giustizia e della pubblica sicurezza, in merito all'uso delle tecnologie, compreso il riconoscimento facciale, negli spazi pubblici ([46]). In tale nota, l'ANPD ha ricordato che il trattamento per tali finalità deve essere conforme ai principi generali e ai diritti previsti dalla LGPD ([47]).

(32) L'articolo 4, punto II, della LGPD introduce inoltre un'esenzione parziale dalla legge per il trattamento dei dati personali a scopi di ricerca accademica e a scopi giornalistici e artistici.

(33) Per quanto riguarda la ricerca accademica, l'esenzione è limitata da diversi elementi. In primo luogo, ai sensi dell'articolo 4, punto II, della LGPD, il trattamento deve essere effettuato «esclusivamente» a scopi di ricerca accademica. In secondo luogo, l'articolo 4, punto II, lettera b), della LGPD stabilisce che tali tipi di trattamento sono soggetti agli articoli 7 (requisito della base giuridica) e 11 (norme sul trattamento dei dati sensibili) ([48]). In terzo luogo, l'ANPD ha elaborato una guida orientativa per specificare ulteriormente le norme applicabili al trattamento dei dati a scopi accademici e di ricerca, definendo rigorosamente quali soggetti possono essere considerati «organismi di ricerca» ai sensi dell'articolo 5, punto XVII, della LGPD ([49]). In detti orientamenti, l'ANPD conferma che il trattamento dei dati a scopi di ricerca accademica è esentato dalla LGPD solo parzialmente e che si applicano i principi generali della legge ([50]).

(34) Per quanto riguarda specificamente i dati utilizzati a fini di ricerca sanitaria, la LGPD contiene ulteriori limitazioni. Da un lato, l'articolo 13 della LGPD stabilisce obblighi di sicurezza per le banche dati utilizzate e incoraggia l'uso di tecniche di anonimizzazione e pseudonimizzazione. Prevede inoltre che gli enti di ricerca siano ritenuti responsabili per la mancata attuazione di misure di sicurezza destinate a proteggere i dati personali ([51]). Dall'altro, il trasferimento a terzi di dati utilizzati per la ricerca sanitaria è vietato in qualsiasi circostanza ([52]).

(35) Per quanto riguarda il trattamento dei dati personali a scopi giornalistici e artistici, l'esenzione prevista dalla LGPD è simile a quella di cui all'articolo 85, paragrafo 2, del regolamento (UE) 2016/679. L'esenzione in virtù della LGPD riguarda la situazione in cui il trattamento è effettuato «esclusivamente» a tali fini ([53]). Di conseguenza la LGPD si applica integralmente se la stampa, i media ed enti artistici trattano dati personali per altre finalità, quali la gestione delle risorse umane o l'amministrazione interna.

([45]) Articolo 4, paragrafi da 2 a 4, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([46]) Nota tecnica n. 175/2023 sul progetto di accordo di cooperazione tra il ministero della Giustizia e della pubblica sicurezza e la Federazione brasiliana di calcio per la condivisione di dati personali al fine di migliorare il progetto «stadi sicuri», disponibile all'indirizzo: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/nota-tecnica-no-175-2023-cgf-anpd-acordo-de-cooperacao-mjsp-e-cbf.pdf.

([47]) Nota tecnica n. 175/2023, paragrafo 5.1.

([48]) Articolo 4, punto II, lettera b, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([49]) Guida orientativa dell'ANPD sul trattamento dei dati personali a scopi accademici e di ricerca, giugno 2023, disponibile all'indirizzo: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf.

([50]) Cfr. in particolare le pagine da 18 a 43 della guida orientativa sul trattamento dei dati personali a scopi accademici e di ricerca.

([51]) Articolo 13, paragrafo 2, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([52]) Articolo 13, paragrafo 2, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati. Cfr. anche guida orientativa dell'ANPD sul trattamento dei dati personali a scopi accademici e di ricerca, giugno 2023, pag. 15.

([53]) Articolo 4, punto II, lettera a), della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

(36) L'espressione artistica e la libertà dei media rientrano entrambe nella libertà di espressione di cui all'articolo 5, punto IX, della costituzione, che garantisce la libertà di espressione per l'attività intellettuale, artistica, scientifica e comunicativa. Il bilanciamento tra libertà di espressione e altri diritti (compresi i diritti alla vita privata e alla protezione dei dati) è disciplinato dai criteri stabiliti nella costituzione come interpretata dalla Corte suprema federale. In particolare, l'esercizio del diritto alla libertà di espressione non richiede alcuna autorizzazione preventiva, ma rimane soggetto ai limiti previsti per la tutela di altri diritti fondamentali. Nello specifico, è previsto un risarcimento in caso di danno o violazione del diritto alla vita privata ai sensi dell'articolo 5, punto X, della costituzione. Queste garanzie sono state integrate anche nella legge sul quadro civile di Internet, una legge adottata nel 2014 per tutelare i diritti fondamentali online ([54]). In particolare, l'articolo 7, punto I, di tale legge garantisce l'«inviolabilità della vita privata» e stabilisce il diritto al risarcimento dei danni materiali o morali derivanti dalla violazione. Inoltre nella sua giurisprudenza la Corte suprema federale fa riferimento alla necessità di trovare un equilibrio tra i diritti, conciliando il diritto alla libertà di espressione con l'inviolabilità della vita privata, sottolineando l'importanza del diritto di ricorso e dell'accesso a un mezzo di impugnazione in caso di violazione della vita privata ([55]). Statuendo su un'altra causa, la Corte suprema federale ha ricordato che le libertà di stampa e di comunicazione sociale devono essere esercitate in linea con altri principi costituzionali quali l'inviolabilità della vita privata e il diritto alla protezione dei dati ([56]).

(37) Infine la LGPD esenta dall'ambito di applicazione della legge il trattamento di dati che hanno origine al di fuori del Brasile e che 1) non sono condivisi o comunicati a soggetti coinvolti nel trattamento dei dati in Brasile o 2) provengono da un paese ritenuto adeguato ai sensi della LGPD, purché non siano trasferiti in un altro paese ([57]). L'ANPD ha fornito un'interpretazione vincolante per chiarire rigorosamente questi due scenari nel proprio regolamento sui trasferimenti di dati ([58]).

(38) Nel primo caso, il semplice transito di dati personali all'interno del Brasile, senza alcun ulteriore trattamento nel paese, non rientra nell'ambito di applicazione della legge ([59]). Tuttavia la LGPD è applicabile non appena i dati sono consultati, utilizzati o comunque trattati in Brasile. Anche le norme nazionali vigenti in materia di cibersicurezza e di accesso ai dati da parte delle autorità pubbliche continuano ad applicarsi a questo scenario limitato, indipendentemente dal fatto che i dati siano trattati o semplicemente transitino nel territorio brasiliano.

(39) Nel secondo caso, l'ANPD ha chiarito che solo il ri-trasferimento di dati originariamente trasferiti da un paese che beneficia di una decisione di adeguatezza ai sensi della LGPD non rientra nell'ambito della legge, purché tale trattamento sia disciplinato dalla legge nazionale di tale paese adeguato. Anche in questo caso continuerebbero ad applicarsi le norme sulla cibersicurezza e sull'accesso ai dati da parte delle autorità pubbliche. Nel contesto del trasferimento di dati personali tra l'UE e il Brasile, nel caso in cui l'UE benefici di una decisione di adeguatezza del Brasile, il ri-trasferimento di dati dal Brasile all'UE non rientrerebbe sempre nell'ambito di applicazione dell'articolo 3 del regolamento (UE) 2016/679. Nei casi in cui il trattamento in questione non rientri nell'ambito di applicazione del regolamento (UE) 2016/679, si evince quindi dall'articolo 8, punto II, lettera b), del regolamento sui trasferimenti di dati che la LGPD si applicherebbe al ri-trasferimento di dati dal Brasile all'UE.

([54]) Legge n. 12.965 del 23 aprile 2014, Marco Civil da Internet («quadro civile di Internet»), disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

([55]) Corte suprema federale, decisione sul ricorso diretto di incostituzionalità n. 4815, disponibile all'indirizzo: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4271057.

([56]) Corte suprema federale, decisione sul ricorso diretto di incostituzionalità n. 5418, disponibile all'indirizzo: https://www.jurisprudencia.stf.jus.br/pages/search/sjur446943/false.

([57]) Articolo 4, punto IV, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([58]) Sezione III, allegato I, del regolamento dell'ANPD sui trasferimenti internazionali di dati personali («regolamento sui trasferimenti di dati»), disponibile all'indirizzo: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/regulation-on-international-transfer-of-personal-data.pdf.

([59]) Articolo 8, punto I, del regolamento dell'ANPD sul trasferimento internazionale di dati personali.

2.4. **Garanzie, diritti e obblighi**

2.4.1. *Liceità e correttezza del trattamento*

(40) I dati personali dovrebbero essere trattati in maniera lecita e corretta.

(41) I principi di liceità, buona fede e trasparenza e le basi del trattamento lecito sono stabiliti dagli articoli 6 e 7 della LGPD, con condizioni analoghe a quelle previste dagli articoli 5 e 6 del regolamento (UE) 2016/679.

(42) A norma degli articoli 6 e 7 della LGPD, i titolari del trattamento e i responsabili del trattamento devono trattare le informazioni personali in modo lecito e in buona fede nella misura minima necessaria per la finalità specificata, includendo dati pertinenti, proporzionati e non eccessivi rispetto alla finalità conseguita ([60]).

(43) Tali principi generali di liceità del trattamento sono ulteriormente elaborati nell'articolo 7 della LGPD, che stabilisce le diverse basi giuridiche per il trattamento, comprese le circostanze in cui questo può comportare una variazione di finalità.

(44) Ai sensi dell'articolo 7 della LGPD, il titolare del trattamento e il responsabile del trattamento possono trattare i dati personali solo sulla base di un numero limitato di fondamenti giuridici. I fondamenti giuridici previsti dalla LGPD sono i seguenti: 1) il consenso dell'interessato (punto I); 2) la necessità di eseguire un contratto o procedure preliminari relative a un contratto di cui l'interessato è parte, su richiesta dello stesso (punto V); 3) l'adempimento di un obbligo giuridico o normativo al quale è soggetto il titolare del trattamento ([61]) (punto II); 4) la necessità di proteggere la vita o l'incolumità fisica dell'interessato o di terzi (punto VII); 5) il trattamento di dati da parte di una pubblica amministrazione, necessario per l'esecuzione di politiche pubbliche previste in normative e regolamenti, o in contratti, accordi o atti simili ([62]) (punto III); 6) se necessario per soddisfare i legittimi interessi del titolare del trattamento o di terzi, tranne nel caso in cui prevalgano i diritti e le libertà fondamentali dell'interessato che impongono la protezione dei dati personali (punto IX).

(45) L'articolo 7 della LGPD indica quattro ulteriori basi giuridiche specifiche per il trattamento dei dati, ossia: 1) la realizzazione di studi da parte di enti di ricerca, garantendo, ove possibile, l'anonimizzazione dei dati personali (punto IV); 2) l'esercizio regolare dei diritti nei procedimenti giudiziari, amministrativi o arbitrali ([63]) (punto VI); 3) la tutela della salute, esclusivamente nell'ambito di una procedura condotta da operatori sanitari, servizi sanitari o autorità sanitarie (punto VIII); 4) la protezione del credito (punto X) ([64]).

([60]) Cfr., in particolare, l'articolo 6, frase introduttiva, punti I, III e V, e l'articolo 7 della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([61]) Qualsiasi obbligo giuridico o normativo deve essere definito dalla legge e deve essere necessario e proporzionato.

([62]) Il trattamento deve avvenire conformemente alle disposizioni specifiche in materia di trattamento di dati personali da parte delle autorità pubbliche di cui al capo IV della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD).

([63]) Le procedure sono descritte nella legge n. 9.307 del 23 settembre 1996 – legge sull'arbitrato.

([64]) Per quanto riguarda la protezione del credito, l'integrazione di tale base giuridica nella LGPD ha aumentato il livello di protezione degli interessati, ad esempio garantendo che gli enti creditizi trattino solo i dati personali necessari per l'analisi e il recupero del credito. Dall'adozione della LGPD, gli organi giurisdizionali brasiliani hanno emesso diverse decisioni volte, ad esempio, a limitare il trattamento dei dati a fini di protezione del credito, escludendo il numero di registrazione dell'elettore, il nome della madre, lo stile di vita, la classe sociale, il livello di scolarizzazione, la propensione marginale al consumo e la georeferenziazione, dati ritenuti non necessari. Gli organi giurisdizionali hanno inoltre chiarito che un ulteriore accesso ai dati personali richiederebbe il consenso dell'interessato, limitando così la portata del trattamento dei dati che può avvenire ai fini della protezione del credito. Cfr. Opice Blum Advogados, *Jurimetrics Report*, 2022, disponibile all'indirizzo: https://opiceblum.com.br/wp-content/uploads/2019/07/09-relatorio-jurimetria-2022.pdf.

2.4.2. *Criteri per il consenso*

(46) Gli obblighi formali per l'ottenimento di un consenso valido al trattamento di dati personali a norma della LGPD sono stabiliti dall'articolo 8, che prevede un approccio analogo a quello di cui all'articolo 4, paragrafo 11, e all'articolo 7 del regolamento (UE) 2016/679. In primo luogo, il consenso deve essere espresso per iscritto o con altri mezzi atti a dimostrare una «manifestazione di volontà» da parte dell'interessato ([65]). Nelle sue linee guida, l'ANPD ha chiarito che il consenso deve essere inequivocabile, il che richiede l'ottenimento di una chiara e positiva manifestazione di volontà da parte dell'interessato; non è pertanto possibile ottenere il consenso tacitamente o tramite un'omissione dell'interessato ([66]). In secondo luogo, il consenso deve fare riferimento a «finalità specifiche» e quindi le «autorizzazioni generiche al trattamento» di dati personali sono considerate nulle ([67]). In terzo luogo, il consenso deve essere espresso attraverso informazioni fornite in modo «trasparente, chiaro e inequivocabile» ([68]). Se previsto nell'ambito di un contratto più ampio, il consenso deve figurare in una clausola specifica e distinta che si distingua chiaramente dalle altre disposizioni contrattuali ([69]). Inoltre il consenso non è valido se le informazioni fornite all'interessato presentano «contenuti fuorvianti o abusivi» ([70]). Il titolare del trattamento deve informare l'interessato di qualsiasi modifica riguardante: 1) la finalità specifica del trattamento; 2) il tipo di trattamento o la sua durata; 3) l'identità del titolare del trattamento; 4) qualsiasi informazione relativa al trattamento e all'eventuale condivisione dei dati ([71]). In quarto luogo, il consenso può essere revocato in qualsiasi momento dall'interessato mediante una procedura gratuita ([72]).

(47) La LGPD vieta rigorosamente il trattamento di dati personali qualora il consenso sia viziato o invalido ([73]). La LGPD chiarisce inoltre che al titolare del trattamento incombe l'onere di dimostrare che il consenso è stato legittimamente ottenuto conformemente alla stessa ([74]).

(48) Infine la LGPD stabilisce che, nel caso in cui il consenso sia la base giuridica appropriata per il trattamento e i dati personali siano stati resi manifestamente pubblici dall'interessato, si ritiene che vi sia un'esenzione dall'obbligo di consenso ([75]). La nozione di «dati personali resi manifestamente pubblici» figura anche all'articolo 9 del regolamento (UE) 2016/679. Tuttavia, anche in caso di esenzione dall'obbligo di consenso, i titolari del trattamento e i responsabili del trattamento sono comunque tenuti al rispetto di tutti gli altri diritti e obblighi stabiliti dalla LGPD ([76]). In particolare, i dati resi manifestamente pubblici dall'interessato possono essere ulteriormente trattati a condizione che ciò avvenga per una finalità «legittima e specifica» e che siano rispettati i diritti degli interessati e i principi stabiliti dalla LGPD ([77]).

([65]) Articolo 8, frase introduttiva, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([66]) Guida dell'ANPD sui cookie e sulla protezione dei dati, pagg. 18-19, disponibile all'indirizzo: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf.

([67]) Articolo 8, paragrafo 4, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati. Inoltre, se i dati personali devono essere condivisi tra più titolari del trattamento è richiesto un consenso specifico distinto, a meno che i dati non siano stati resi manifestamente pubblici, come stabilito dall'articolo 7, paragrafo 5, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([68]) Articolo 9, paragrafo 1, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([69]) Articolo 8, paragrafo 1, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([70]) Articolo 9, paragrafo 1, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([71]) Articolo 8, paragrafo 6, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([72]) Articolo 8, paragrafo 5, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([73]) Articolo 8, paragrafo 3, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([74]) Articolo 8, paragrafo 2, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([75]) Articolo 7, paragrafo 4, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati. L'ambito di applicazione di questa misura è limitato, in quanto non comprende il trattamento di dati sensibili autorizzato a norma dell'articolo 9, paragrafo 2, lettera e), del regolamento (UE) 2016/679.

([76]) Articolo 7, paragrafo 4, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([77]) Articolo 7, paragrafo 7, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

2.4.3. *Criteri per il legittimo interesse*

(49) L'articolo 7, punto IX, della LGPD stabilisce che il trattamento dei dati personali non può essere mai effettuato per il perseguimento di un legittimo interesse qualora tale trattamento entri in conflitto con i diritti e le libertà fondamentali degli interessati, sottolineando che prevale la protezione dei dati personali. Questo approccio è simile a quello seguito nell'UE e stabilito all'articolo 6, paragrafo 1, lettera f), del regolamento (UE) 2016/679.

(50) L'articolo 10 della LGPD stabilisce ulteriori condizioni sulla base delle quali i titolari del trattamento possono invocare un «legittimo interesse» come base giuridica per il trattamento dei dati personali. In primo luogo, quando il trattamento dei dati personali si basa su un legittimo interesse, il titolare del trattamento tratta solo i dati personali «strettamente necessari» per la finalità prevista ([78]). In secondo luogo, i titolari del trattamento devono attuare misure per garantire la trasparenza delle loro attività di trattamento ([79]). In terzo luogo, un legittimo interesse può essere invocato solo in «situazioni particolari» ([80]).

(51) Inoltre l'ANPD ha pubblicato una guida sul legittimo interesse, che precisa le condizioni per farlo valere ([81]). La guida chiarisce, ad esempio, che il legittimo interesse non può essere utilizzato come base giuridica per il trattamento di dati sensibili ([82]); inoltre l'allegato della guida contiene un modello di test comparativo per la tutela dei diritti e delle libertà fondamentali che può essere utilizzato da tutti i titolari del trattamento che intendono invocare un legittimo interesse ([83]). L'ANPD può anche richiedere al titolare del trattamento di effettuare una valutazione d'impatto sulla protezione dei dati ([84]).

(52) Nella guida l'ANPD 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; 3) trattamento effettuato per finalità legittime, specifiche ed esplicite ([85]). La prima condizione, «compatibilità con l'ordinamento giuridico», presuppone che il legittimo interesse invocato dal titolare del trattamento sia compatibile con i principi, le norme giuridiche e i diritti fondamentali garantiti in Brasile. Ciò significa, ad esempio, che il trattamento di dati personali previsto non dovrebbe essere vietato da un atto normativo brasiliana né entrare in contrasto, direttamente o indirettamente, con le disposizioni giuridiche o i principi contenuti nel diritto brasiliano. In secondo luogo, il legittimo interesse invocato deve basarsi su situazioni «concrete, chiare e precise», mirate a interessi specifici e ben definiti. Il legittimo interesse invocato non può fondarsi su situazioni astratte o meramente speculative ([86]). L'ANPD specifica inoltre che eventuali interessi non legati alle attività correnti del titolare del trattamento non sono considerati legittimi ([87]). La terza condizione consiste nella necessità di dimostrare una finalità specifica del trattamento. L'ANPD osserva che il legittimo interesse del titolare del trattamento (che giustifica il trattamento) non deve essere confuso con la finalità del

([78]) Articolo 10, paragrafo 1, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([79]) Articolo 10, paragrafo 2, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([80]) L'articolo 10 della LGPD fornisce alcuni esempi di situazioni particolari in cui è possibile invocare un legittimo interesse: 1) per sostenere e promuovere le attività del titolare del trattamento (punto I); 2) per tutelare l'esercizio dei diritti dell'interessato o consentire la prestazione di servizi a beneficio dell'interessato, purché tale trattamento rispetti le legittime aspettative nonché i diritti e le libertà fondamentali dell'interessato (punto II). Legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([81]) Guida dell'ANPD – Basi giuridiche per il trattamento dei dati personali – Legittimo interesse, febbraio 2024 («Guida sul legittimo interesse»), disponibile all'indirizzo: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_legitimo_interesse.pdf.

([82]) Guida dell'ANPD sul legittimo interesse, pag. 8.

([83]) Guida dell'ANPD sul legittimo interesse, allegato 3.

([84]) Articolo 10, paragrafo 3, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([85]) Guida dell'ANPD sul legittimo interesse, pagg. 16-17.

([86]) Guida dell'ANPD sul legittimo interesse, pag. 16, che interpreta l'articolo 10, frase introduttiva, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([87]) Guida dell'ANPD sul legittimo interesse, pag. 16.

trattamento (che costituisce la finalità specifica che si intende conseguire con il trattamento). L'esistenza di un legittimo interesse non elimina l'obbligo per il titolare del trattamento di rispettare il principio di limitazione delle finalità e tutti gli obblighi derivanti dalla LGPD. La finalità deve essere descritta in modo chiaro e preciso, fornendo le informazioni necessarie per delimitare la portata del trattamento e consentire di ponderare gli interessi del responsabile del trattamento o di terzi con i diritti e le legittime aspettative degli interessati ([88]). Ciò significa che, nell'invocare un legittimo interesse al fine di sostenere o promuovere la propria attività, il titolare del trattamento deve definire chiaramente, tra l'altro, quale attività intende promuovere/sostenere e la correlazione con il trattamento previsto.

2.4.4. *Trattamenti di categorie particolari di dati*

(53) Garanzie specifiche dovrebbero essere applicate al trattamento di «categorie particolari» di dati.

(54) L'articolo 5, punto II, della LGPD definisce i dati personali sensibili come quelli riguardanti l'origine razziale o etnica, le convinzioni religiose, le opinioni politiche, l'appartenenza sindacale o l'organizzazione religiosa, filosofica o politica di appartenenza, la salute o la vita sessuale, i dati genetici o biometrici, se collegati a una persona fisica. In base alla giurisprudenza nazionale, il concetto di vita sessuale dovrebbe essere interpretato in modo da comprendere anche l'orientamento o le preferenze sessuali di una persona fisica. In particolare, nella giurisprudenza in materia di matrimonio tra persone dello stesso sesso, la Corte suprema federale ha stabilito che la discriminazione basata sul «sesso» comprende le «preferenze sessuali» ([89]) e che la libertà di esercitare il proprio «orientamento sessuale» è un prerequisito per lo sviluppo della propria personalità, che è oggetto di tutela costituzionale ([90]). Pertanto le categorie di dati sensibili ai sensi del diritto brasiliano sono le stesse di cui all'articolo 9, paragrafo 1, del regolamento (UE) 2016/679.

(55) Gli organi giurisdizionali brasiliani hanno ulteriormente ampliato la definizione di dati personali sensibili ai sensi della LGPD per includervi altri tipi di informazioni che potrebbero essere utilizzate per discriminare le persone fisiche ([91]). Tale interpretazione discende dal diritto di ciascuna persona fisica di essere tutelata contro la discriminazione ai sensi della legislazione brasiliana, come risulta anche dall'articolo 6, punto IX, della LGPD. In particolare la giurisprudenza brasiliana ha chiarito che le informazioni relative ai casellari giudiziari sono considerate dati sensibili ([92]).

(56) Il trattamento di dati sensibili ai sensi della LGPD è autorizzato solo se l'interessato o il suo rappresentante legale ha espresso il proprio «specifico e distinto» consenso per determinate finalità ([93]). Per la validità del consenso si applicano le condizioni di cui ai considerando da 46 a 48 della presente decisione.

(57) Ai sensi dell'articolo 11, punto II, della LGPD, il trattamento di dati sensibili può essere effettuato senza il consenso esplicito dell'interessato: 1) quando è necessario per adempiere un obbligo giuridico o normativo del titolare del trattamento (lettera a)); 2) quando è necessario per il trattamento da parte della pubblica amministrazione ai fini dell'esecuzione di politiche pubbliche previste da disposizioni legislative o regolamentari (lettera b)); 3) per proteggere la vita o l'incolumità fisica dell'interessato o di terzi (lettera e)); 4) per l'esercizio di diritti, anche nel quadro di contratti e nell'ambito di procedimenti amministrativi, giudiziari e arbitrali, conformemente al diritto brasiliano (lettera d)); 5) per proteggere la salute degli interessati, esclusivamente nell'ambito di procedure svolte da professionisti sanitari, servizi sanitari o autorità sanitarie (lettera f)); 6) da organismi di ricerca per condurre studi, garantendo che i dati siano anonimizzati, ove possibile (lettera c)); 7) per garantire la prevenzione delle frodi e la sicurezza degli interessati nell'ambito dei processi di identificazione e autenticazione mediante registrazione nei sistemi elettronici. Pertanto i motivi per il trattamento di dati sensibili ai sensi della LGPD e del regolamento (UE) 2016/679 sono simili.

([88]) Guida dell'ANPD sul legittimo interesse, pag. 17.

([89]) Cfr. la sentenza della Corte suprema federale del Brasile che autorizza il matrimonio tra persone dello stesso sesso, interpretando l'articolo 3, punto IV, della costituzione federale, che vieta qualsiasi discriminazione fondata sul sesso, la razza e il colore. Corte suprema federale, decisione n. 4277, del 5 maggio 2011, sul ricorso diretto di incostituzionalità, punti 2 e 6, disponibile all'indirizzo: https://portal.stf.jus.br/peticaoInicial/verPeticaoInicial.asp?base=ADI&numProcesso=4277.

([90]) Cfr. la sentenza della Corte suprema federale del Brasile che autorizza il matrimonio tra persone dello stesso sesso, pag. 14: quale presupposto imprescindibile per lo sviluppo della personalità umana – il più alto valore tutelato dalla costituzione federale – è essenziale eliminare qualsiasi ostacolo giuridico, anche potenziale, che limiti il pieno esercizio della libertà spettante a ogni essere umano nell'esercitare appieno il proprio *orientamento sessuale*.

([91]) Tribunale superiore del lavoro, decisione TST-E-RR-933-49.2012.5.10.0001, dicembre 2021, disponibile all'indirizzo: https://www.jusbrasil.com.br/jurisprudencia/tst/713123452/inteiro-teor-713123472.

([92]) Tribunale superiore del lavoro, decisione TST-E-RR-933-49.2012.5.10.0001, dicembre 2021.

([93]) Articolo 11, punto I, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

2.4.5. *Limitazione delle finalità*

(58) I dati personali dovrebbero essere raccolti per una finalità specifica e in una maniera non incompatibile con la finalità del trattamento.

(59) L'articolo 6, punto I, della LGPD stabilisce che i dati personali dovrebbero essere trattati per una finalità legittima, determinata ed esplicita di cui l'interessato è informato, senza sottoporli a un ulteriore trattamento «incompatibile» con la finalità iniziale. Tale principio, e la sua formulazione, è quasi identico a quello corrispondente di cui all'articolo 5, paragrafo 1, lettera c), del regolamento (UE) 2016/679. L'articolo 6, punto II, della LGPD stabilisce inoltre che qualsiasi attività di trattamento deve essere compatibile con le finalità comunicate all'interessato.

(60) Dagli orientamenti emanati dall'ANPD risulta che, per determinare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati sono stati inizialmente raccolti, il titolare del trattamento deve dimostrare un nesso tra le due finalità del trattamento e tenere conto delle «legittime aspettative» degli interessati ([94]). In caso di trattamento per ulteriori finalità compatibili, si applicano i principi e gli obblighi della LGPD; occorre quindi garantire che la nuova finalità sia specifica e che i diritti degli interessati siano tutelati. Ciò vale anche per l'ulteriore trattamento di dati resi «manifestamente disponibili» dall'interessato o accessibili al pubblico ([95]).

2.4.6. *Esattezza e minimizzazione dei dati*

(61) I dati dovrebbero essere esatti e, se necessario, dovrebbero essere aggiornati. Dovrebbero essere adeguati, pertinenti e non eccessivi rispetto alle finalità per le quali sono trattati.

(62) Ciò è garantito dai principi della «qualità dei dati» e della «necessità» di cui, rispettivamente, all'articolo 6, punti III e V, della LGPD. Ai sensi dell'articolo 6, punto V, della LGPD, il titolare del trattamento e il responsabile del trattamento garantiscono che i dati personali siano esatti, chiari, pertinenti e aggiornati rispetto alle finalità per le quali sono trattati. L'articolo 6, punto III, della LGPD stabilisce la «limitazione del trattamento al minimo necessario» per conseguire una o più finalità specifiche, in relazione a dati pertinenti, proporzionali e non eccessivi rispetto a tali finalità. Tali principi sono simili a quelli di cui all'articolo 5, paragrafo 1, lettere c) e d), del regolamento (UE) 2016/679.

2.4.7. *Limitazione della conservazione*

(63) In linea di principio i dati non dovrebbero essere conservati per un arco di tempo superiore a quanto necessario per il conseguimento delle finalità per le quali sono trattati.

(64) I principi di «finalità», «necessità» e «accesso» stabiliti, rispettivamente, all'articolo 6, punti I, III e IV della LGPD prevedono requisiti in merito alla limitazione della conservazione. Essi limitano la possibilità di conservare i dati al minimo necessario in relazione alla finalità «legittima, specifica ed esplicita» e impongono di informare gli interessati sulla durata della conservazione.

([94]) Guida dell'ANPD sul legittimo interesse, pag. 26 e allegato 2.

([95]) Articolo 7, paragrafo 7, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati. Cfr. anche il considerando 48 della presente decisione. Il concetto di dati resi «manifestamente disponibili» è rinvenibile anche nel regolamento (UE) 2016/679, mentre per dati «pubblicamente disponibili» s'intendono le informazioni presenti in registri pubblici o banche dati a norma del diritto brasiliano ai sensi della legge n. 12.527 del 18 novembre 2011 – legge sull'accesso alle informazioni, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.

(65) Inoltre il capo II, sezione IV, della LGPD è dedicato alla «cessazione del trattamento dei dati». L'articolo 16 di tale sezione della LGPD impone che tutti i dati personali siano cancellati dopo la cessazione del trattamento per una finalità definita. Tali requisiti, in combinato disposto con i principi di «finalità», «necessità» e «accesso» della LGPD, sono simili agli obblighi derivanti dall'articolo 5, paragrafo 1, lettera e), del regolamento (UE) 2016/679.

(66) Secondo le rigorose eccezioni di cui all'articolo 16 della LGPD, i dati possono essere ulteriormente trattenuti e conservati: 1) per il rispetto di obblighi giuridici o normativi; 2) a fini 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.

(67) I dati conservati sono soggetti agli obblighi in materia di sicurezza dei dati stabiliti nella LGPD e descritti nei considerando da 68 a 78 della presente decisione.

2.4.8. *Sicurezza dei dati*

(68) I dati personali dovrebbero essere trattati in maniera da garantirne la sicurezza, compresa la protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. A tal fine gli operatori dovrebbero adottare misure tecniche od organizzative per proteggere i dati personali da possibili minacce. Tali misure dovrebbero essere valutate tenendo conto dello stato dell'arte e dei costi connessi.

(69) Tale principio è garantito dall'articolo 6, punto VII, della LGPD, che impone l'uso di misure tecniche e amministrative per proteggere i dati personali da accessi non autorizzati e trattamenti accidentali o illeciti, tra cui distruzione, perdita, modifica, comunicazione o diffusione dei dati. Per ridurre tali rischi per la sicurezza dei dati, l'articolo 6, punto VIII, della LGPD impone l'adozione di misure volte a prevenire il verificarsi di danni dovuti al trattamento dei dati personali.

(70) L'articolo 44 della LGPD stabilisce che il trattamento dei dati personali è illecito quando non soddisfa le norme di sicurezza che l'interessato può legittimamente attendersi. Il livello di sicurezza adeguato deve essere determinato tenendo conto, tra l'altro: 1) delle circostanze specifiche relative al trattamento effettuato; 2) del livello ragionevole di rischio atteso; 3) delle tecniche di trattamento disponibili al momento del trattamento stesso ([96]).

(71) Per attuare il principio della sicurezza dei dati, la LGPD prevede una serie di obblighi nel capo VII, sezione I, concernente la «Sicurezza e segretezza dei dati». L'articolo 46 di tale sezione della LGPD impone ai titolari del trattamento e ai responsabili del trattamento di adottare misure di sicurezza, tecniche e amministrative tali da proteggere i dati personali da accessi non autorizzati e da trattamenti accidentali o illeciti, tra cui distruzione, perdita, modifica, comunicazione o qualsiasi tipo di trattamento improprio o illecito. Tali misure devono essere rispettate dalla fase di ideazione del prodotto o servizio fino alla sua realizzazione ([97]). L'articolo 47 della LGPD prevede per tutte le parti coinvolte in qualsiasi fase del trattamento un obbligo generale di rispettare le prescrizioni in materia di sicurezza. Tali obblighi sono simili a quelli previsti dall'articolo 32 del regolamento (UE) 2016/679.

(72) L'articolo 44 della LGPD stabilisce inoltre che il titolare del trattamento o il responsabile del trattamento che omette di adottare misure di sicurezza è ritenuto responsabile dei danni causati in caso di violazione della sicurezza ([98]). L'ANPD può inoltre stabilire norme tecniche minime di sicurezza per garantire il rispetto degli obblighi in materia di sicurezza dei dati ([99]).

([96]) Articolo 44, punti da I a III, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([97]) Articolo 46, paragrafo 2, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([98]) Articolo 44, comma unico, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([99]) Articolo 46, paragrafo 1, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

(73) Ai sensi dell'articolo 48 della LGPD, qualora si verifichi un incidente di sicurezza che può comportare un rischio o causare un danno significativo agli interessati, il titolare del trattamento è tenuto a notificarlo sia all'ANPD che agli interessati. Tale notifica deve avvenire entro un termine ragionevole, come stabilito dall'ANPD, e deve contenere almeno: 1) una descrizione della natura dei dati personali interessati; 2) informazioni che identificano gli interessati coinvolti; 3) un'indicazione delle misure tecniche e di sicurezza adottate per proteggere i dati, fatta salva la tutela della riservatezza commerciale e industriale; 4) una valutazione dei rischi associati all'incidente; 5) il motivo di eventuali ritardi nella comunicazione; 6) una descrizione delle misure adottate o da adottare per attenuare il danno causato o porvi rimedio. L'approccio seguito nella LGPD è in gran parte simile a quello stabilito dagli articoli 33 e 34 del regolamento (UE) 2016/679.

(74) L'ANPD ha adottato ulteriori norme in materia di incidenti relativi alla sicurezza dei dati per chiarire, ad esempio, la definizione di «incidente» e i tempi di notifica dello stesso ([100]).

(75) L'articolo 3, punto XII, del regolamento sulla notifica degli incidenti di sicurezza definisce un incidente di sicurezza come qualsiasi evento avverso confermato connesso alla violazione della riservatezza, dell'integrità, della disponibilità e dell'autenticità della sicurezza dei dati personali. A norma dell'articolo 48 della LGPD, una violazione di dati e un incidente di sicurezza che possono creare rischi per gli interessati devono sempre essere comunicati all'autorità per la protezione dei dati (ANPD) e agli interessati. L'articolo 5 del regolamento sulla notifica degli incidenti di sicurezza chiarisce che un incidente di sicurezza può comportare un rischio per gli interessati se può ledere i loro interessi e diritti fondamentali e se riguarda almeno uno dei seguenti tipi di dati: 1) dati personali sensibili; 2) dati relativi a bambini, adolescenti o anziani; 3) dati finanziari; 4) dati di autenticazione nei sistemi; 5) dati protetti dal segreto legale, giudiziario o professionale; oppure 6) banche dati su vasta scala. Inoltre si ritiene che un incidente di sicurezza incida in modo significativo sugli interessi e sui diritti fondamentali degli interessati quando: 1) può impedire l'esercizio di diritti o la fruizione di un servizio; oppure 2) può causare danni materiali o morali agli interessati, tra cui discriminazione, violazione dell'integrità fisica, del diritto all'immagine e alla reputazione, frode finanziaria o furto d'identità ([101]).

(76) La notifica di un incidente di sicurezza all'ANPD e agli interessati deve avvenire entro tre giorni lavorativi dal momento in cui il titolare del trattamento ne è venuto a conoscenza ([102]). Il regolamento vincolante sulla notifica degli incidenti di sicurezza precisa ai titolari del trattamento le informazioni da fornire all'ANPD e agli interessati. La notifica trasmessa agli interessati deve comprendere in particolare: 1) una descrizione della natura e della categoria dei dati personali interessati; 2) le misure tecniche e di sicurezza utilizzate per proteggere i dati; 3) i rischi connessi all'incidente, individuando i possibili impatti sugli interessati; 4) i motivi del ritardo, nel caso in cui la comunicazione non sia stata effettuata entro 72 ore; 5) le misure che sono state o saranno adottate per eliminare o attenuare gli effetti dell'incidente, se del caso; 6) la data in cui è stato scoperto l'incidente di sicurezza; 7) i dati di contatto per ottenere informazioni e, se del caso, i dati di contatto della persona responsabile ([103]). Nel comunicare l'incidente agli interessati, i titolari del trattamento devono utilizzare un linguaggio semplice e di facile comprensione ([104]). La notifica deve essere effettuata direttamente e individualmente, se è possibile identificare gli interessati coinvolti ([105]).

(77) Inoltre l'ANPD può, ove necessario per salvaguardare i diritti degli interessati, valutare la gravità dell'incidente e ordinare al titolare del trattamento di adottare misure specifiche ([106]). Tali misure possono includere la divulgazione pubblica dell'incidente attraverso canali mediatici adeguati, nonché l'attuazione di misure correttive o di attenuazione. Il responsabile del trattamento deve tenere un registro degli incidenti relativi alla sicurezza dei dati ([107]).

([100]) Regolamento dell'ANPD sulla notifica degli incidenti di sicurezza, aprile 2024, disponibile all'indirizzo: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024.
([101]) Articolo 5, paragrafo 1, del regolamento dell'ANPD sulla notifica degli incidenti di sicurezza, aprile 2024.
([102]) Articoli 6 e 9 del regolamento dell'ANPD sulla notifica degli incidenti di sicurezza, aprile 2024.
([103]) Articolo 9, punti da I a VII, del regolamento dell'ANPD sulla notifica degli incidenti di sicurezza, aprile 2024.
([104]) Articolo 9, paragrafo 1, punto I, del regolamento dell'ANPD sulla notifica degli incidenti di sicurezza, aprile 2024.
([105]) Articolo 9, paragrafo 1, punto II, del regolamento dell'ANPD sulla notifica degli incidenti di sicurezza, aprile 2024.
([106]) Articolo 48, paragrafo 2, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.
([107]) Articolo 10 del regolamento dell'ANPD sulla notifica degli incidenti di sicurezza, aprile 2024.

(78) Infine la LGPD collega le sue norme in materia di buone pratiche e governance (dei dati) agli obblighi in materia di sicurezza dei dati, al fine, tra l'altro, di attenuare i rischi legati al trattamento dei dati ([108]). È fra l'altro promossa l'adozione di programmi interni di governance della vita privata per valutare e attenuare i rischi ([109]).

2.4.9. *Trasparenza*

(79) Gli interessati dovrebbero essere informati dei principali aspetti del trattamento dei dati personali che li riguardano.

(80) Seguendo un approccio analogo a quello di cui all'articolo 12 del regolamento (UE) 2016/679, l'articolo 6, punto VI, della LGPD stabilisce che gli interessati devono ricevere informazioni chiare, precise e facilmente accessibili sia sul trattamento dei loro dati sia sui soggetti che effettuano tale trattamento, nel rispetto del «segreto commerciale e industriale».

(81) L'articolo 9 della LGPD stabilisce un elenco di informazioni che devono essere fornite agli interessati in merito al trattamento dei dati, che comprende: 1) la finalità specifica del trattamento; 2) il tipo di trattamento e la sua durata; 3) l'identificazione del titolare del trattamento; 4) i dati di contatto del titolare del trattamento; 5) informazioni relative al trattamento dei dati da parte del titolare del trattamento e alla finalità dello stesso; 6) le responsabilità dei soggetti impegnati nel trattamento; e 7) i diritti degli interessati, comprese le informazioni relative all'esercizio di tali diritti.

(82) La limitazione relativa al «segreto commerciale e industriale» di cui all'articolo 6, punto VI, e altre disposizioni della LGPD dovrebbero essere interpretate alla luce della legge brasiliana sull'accesso alle informazioni ([110]), che prevede di norma la divulgazione delle informazioni contenute in registri o documenti detenuti da enti pubblici ([111]). Eventuali eccezioni, vale a dire l'imposizione di limitazioni all'accesso a documenti e informazioni, devono essere giustificate e previste dalla legge ([112]). Il segreto commerciale e industriale costituisce una di tali eccezioni ed è contemplato da una specifica disposizione giuridica volta a garantire la tutela delle informazioni relative alle attività commerciali delle persone fisiche o giuridiche di diritto privato ottenute da altri organismi o soggetti nell'esercizio delle proprie attività di controllo, regolamentazione e vigilanza dell'attività economica, la cui divulgazione potrebbe rappresentare un vantaggio competitivo per altri operatori economici ([113]). Le disposizioni della LGPD in materia di «segreto commerciale e industriale» devono pertanto essere interpretate 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.

2.4.10. *Diritti delle persone fisiche*

(83) Gli interessati dovrebbero disporre di determinati diritti azionabili nei confronti del titolare del trattamento o del responsabile del trattamento, in particolare il diritto di accesso ai dati, il diritto di rettifica, il diritto di far cancellare i dati, il diritto di opporsi al trattamento, il diritto alla portabilità dei dati e i diritti nell'ambito del trattamento automatizzato dei dati. Tali diritti possono essere soggetti a limitazioni, nella misura in cui tali limitazioni sono necessarie e proporzionate per salvaguardare obiettivi specifici di interesse pubblico generale.

([108]) Articoli 49 e 50 della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([109]) Articolo 50, frase introduttiva e paragrafo 1, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([110]) Legge n. 12.527 del 18 novembre 2011 – legge sull'accesso alle informazioni, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.

([111]) Articoli 6 e 9 della legge n. 12.527 del 18 novembre 2011 – legge sull'accesso alle informazioni.

([112]) Articolo 22 della legge n. 12.527 del 18 novembre 2011 – legge sull'accesso alle informazioni.

([113]) Articolo 5, comma 2, del decreto n. 7.721 del 16 maggio 2012, relativo alla legge n. 12.527 del 18 novembre 2011 – legge sull'accesso alle informazioni.

(84) Il capo III della LGPD stabilisce i diritti degli interessati in modo analogo a quanto previsto dagli articoli da 15 a 22 del regolamento (UE) 2016/679. L'esercizio di tutti i diritti è gratuito e gli interessati devono essere informati degli stessi ([114]). Ai sensi dell'articolo 21 della LGPD, i dati relativi all'esercizio dei diritti da parte di un interessato non possono essere utilizzati a suo danno. Gli interessati possono presentare ricorso in sede giurisdizionale, a livello individuale o collettivo, in relazione ai loro interessi e diritti ([115]).

(85) I titolari del trattamento sono tenuti a informare «immediatamente» i responsabili del trattamento, con i quali i dati possono essere stati condivisi, in merito a qualsiasi richiesta di rettifica, cancellazione, anonimizzazione, limitazione e opposizione trasmessa dagli interessati, al fine di garantire che tutte le parti coinvolte possano soddisfare tali richieste ([116]).

(86) Ai sensi dell'articolo 9 e dell'articolo 18, punto II, della LGPD, gli interessati godono del diritto all'informazione e del diritto di accesso che consentono loro di ottenere «in qualsiasi momento» informazioni relative al trattamento dei loro dati ([117]). Dette informazioni comprendono: 1) l'identità del titolare del trattamento (punto III); 2) i dati di contatto del titolare del trattamento (punto IV); 3) la finalità specifica del trattamento (punto I); 4) informazioni sull'eventuale condivisione dei dati (punto V); 5) il tipo di trattamento e la sua durata (punto II); 6) i diritti degli interessati, compreso il diritto di proporre reclamo all'autorità di protezione dei dati; 7) le responsabilità assunte dai responsabili del trattamento dei dati. Inoltre l'articolo 10, paragrafo 2, della LGPD impone al titolare del trattamento di essere trasparente in merito al trattamento basato su un legittimo interesse. Analogamente, l'articolo 9 del regolamento sui trasferimenti di dati specifica che gli interessati devono essere informati in caso di trasferimento dei dati personali.

(87) L'articolo 19 della LGPD precisa ulteriormente le modalità di accesso da parte degli interessati alle loro informazioni personali. Su richiesta di un interessato, l'accesso ai dati personali deve essere fornito: immediatamente, «in un formato semplificato», oppure entro 15 giorni, mediante una dichiarazione chiara e completa ([118]). Inoltre l'articolo 19, paragrafo 1, della LGPD stabilisce che i titolari del trattamento devono conservare i dati personali in un formato che faciliti l'esercizio del diritto di accesso. L'interessato può decidere se ricevere le informazioni in formato elettronico o cartaceo ([119]).

(88) Gli interessati hanno il diritto di chiedere la rettifica di dati incompleti, inesatti od obsoleti, ai sensi dell'articolo 18, punto III, della LGPD (diritto di rettifica).

(89) L'articolo 18, punti IV e VI, della LGPD conferisce alle persone fisiche il diritto di chiedere la cancellazione: 1) di dati superflui o eccessivi; 2) di dati trattati con il consenso dell'interessato; oppure 3) di dati trattati illecitamente. La sezione IV, capo II, della LGPD, relativa alla «cessazione del trattamento dei dati», indica altresì che il trattamento dei dati deve cessare se l'interessato si oppone al trattamento o revoca il suo consenso al trattamento ([120]). Dopo la cessazione del trattamento i dati devono essere cancellati ([121]). Pertanto tali disposizioni, in combinato disposto, ampliano indirettamente la portata del diritto alla cancellazione previsto dalla LGPD.

([114]) Articolo 18 della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([115]) Articolo 22 della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([116]) Articolo 18, paragrafo 6, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([117]) Articolo 6, punto VI, articoli 18 e 19 della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([118]) Articolo 19, punti I e II, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([119]) Articolo 19, paragrafo 2, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([120]) Cfr. l'articolo 15, punto III, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD), secondo cui la «comunicazione da parte dell'interessato» si riferisce, tra l'altro, alla revoca del consenso (come indicato nell'articolo). Il significato di «comunicazione» non si limita a questo caso e consente agli interessati di chiedere la cessazione del trattamento.

([121]) Articolo 16 della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

(90) Le persone fisiche hanno il diritto di opporsi al trattamento dei dati sulla base di un fondamento giuridico diverso dal consenso in caso di mancato rispetto della LGPD (diritto di opposizione) ([122]). Ai sensi dell'articolo 15 e dell'articolo 18, punto IV, della LGPD, gli interessati hanno anche il diritto di chiedere la limitazione del trattamento dei dati («blocco»). Tale diritto può essere invocato, in particolare, quando i dati trattati sono superflui o eccessivi o quando i dati sono trattati in modo non conforme alla LGPD ([123]). L'articolo 15, punto II, della LGPD indica che i dati non devono più essere trattati qualora l'interessato invii una «comunicazione» al titolare del trattamento. Sebbene sia soggetta all'«interesse pubblico», interpretato in senso lato, tale disposizione prevede un ampio ambito di applicazione del diritto indiretto di opposizione che è equivalente al diritto di opposizione previsto dal regolamento (UE) 2016/679.

(91) Le persone fisiche hanno il diritto di richiedere una «copia elettronica completa» dei loro dati affinché questi possano essere utilizzati da altri soggetti (diritto alla portabilità) ([124]). Come nell'UE, gli interessati possono richiedere tale copia solo se i dati sono stati trattati sulla base del consenso o di un contratto.

(92) Sebbene qualsiasi decisione basata sul trattamento automatizzato di dati raccolti nell'UE sia solitamente adottata da un titolare del trattamento (che ha un rapporto diretto con l'interessato e rientra quindi direttamente nell'ambito di applicazione del regolamento (UE) 2016/679), va rilevato come la LGPD disciplini questo tipo di trattamento in modo analogo a quanto previsto dall'articolo 22 del regolamento (UE) 2016/679. In primo luogo, l'articolo 6, punto IX, della LGPD riconosce il principio di non discriminazione come principio di protezione dei dati, in base al quale è vietato trattare dati per finalità discriminatorie illecite o abusive. Tale principio è applicabile a qualsiasi trattamento ed è particolarmente pertinente nel contesto del trattamento automatizzato. Inoltre, ai sensi dell'articolo 20 della LGPD, gli interessati hanno il diritto di chiedere il riesame delle decisioni adottate unicamente sulla base del trattamento automatizzato di dati che incidono sui loro interessi, comprese le decisioni intese a definire il loro profilo personale, professionale, di consumo e di credito, o gli aspetti della loro personalità. Nel rispondere alla richiesta di un interessato, il titolare del trattamento deve fornire informazioni chiare sui criteri e sulla procedura utilizzati per la decisione automatizzata ([125]). Se tali informazioni non possono essere fornite all'interessato a causa del «segreto commerciale e industriale», l'ANPD ha il potere di effettuare un audit per verificare eventuali aspetti discriminatori nel trattamento automatizzato dei dati personali ([126]). Pertanto il «segreto commerciale e industriale» non può essere invocato per rifiutare di rispondere alla richiesta dell'interessato.

(93) L'articolo 23 della LGPD stabilisce che la procedura e il periodo di tempo per l'esercizio dei diritti degli interessati, nel caso in cui questi siano trattati da autorità pubbliche, sono disciplinati da normative specifiche ([127]). Ad esempio, la normativa brasiliana sull'*habeas data* disciplina il diritto delle persone fisiche di accedere alle informazioni relative ai dati conservati nei registri o nelle banche dati del governo o di un ente pubblico ([128]). La normativa in questione stabilisce disposizioni specifiche per il diritto di accesso, che deve essere concesso entro 10 giorni dalla richiesta di una persona fisica, e il diritto di rettifica, che deve essere concesso entro 15 giorni dalla richiesta ([129]). Analogamente, la legge federale brasiliana sulle procedure amministrative stabilisce il diritto all'informazione e il diritto di accesso delle persone fisiche nell'ambito delle procedure amministrative ([130]). La legge

([122]) Articolo 18, paragrafo 2, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([123]) Articolo 18, punto IV, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([124]) Articolo 19, paragrafo 3, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([125]) Articolo 20, paragrafo 1, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([126]) Articolo 20, paragrafo 2, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([127]) Articolo 23, paragrafo 3, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([128]) Legge n. 9.507 del 12 novembre 1997 – legge brasiliana sull'*habeas data*, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/leis/l9507.htm.

([129]) Articoli 7 e 8 della legge n. 9.507 del 12 novembre 1997 – legge brasiliana sull'*habeas data*. La legge prevede vie di ricorso in caso di mancato rispetto delle richieste trasmesse da persone fisiche.

([130]) Cfr., in particolare, l'articolo 6 della legge n. 9.784 del 29 gennaio 1999 – legge federale sulle procedure amministrative, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/leis/l9784.htm. La legge stabilisce procedure e termini per le comunicazioni con le persone fisiche, nonché vie di ricorso in caso di non conformità.

brasiliana sull'accesso alle informazioni prevede inoltre obblighi di informazione e trasparenza per le autorità pubbliche, le imprese pubbliche e i tre rami del governo (legislativo, esecutivo e giudiziario) in Brasile ([131]). Le disposizioni di tali leggi rafforzano il diritto di accesso e il diritto all'informazione previsti dalla LGPD per il trattamento dei dati da parte delle autorità pubbliche. Quando tali normative non prevedono i diritti specifici stabiliti dalla LGPD (ad esempio i diritti relativi al processo decisionale automatizzato), gli interessati possono esercitare tali diritti facendo valere la LGPD.

(94) Qualsiasi violazione dei diritti degli interessati sarà trattata dall'ANPD come una violazione «media» o «grave» della legge, a seconda del fattore pertinente, e può pertanto essere soggetta al livello più elevato di sanzioni e ammende. È importante sottolineare che, sulla base del regolamento dell'ANPD sulle sanzioni, il semplice fatto che un diritto dell'interessato sia stato pregiudicato da una violazione significa che tale violazione non può essere considerata «leggera» ([132]).

(95) Dall'entrata in applicazione della LGPD, l'ANPD ha ricevuto un numero costante di reclami e richieste da parte di persone fisiche in merito ai loro diritti in materia di protezione dei dati ([133]). Tale numero è aumentato in modo significativo dal luglio 2024, quando l'ANPD ha introdotto una piattaforma modernizzata e di facile utilizzo per la presentazione di richieste e reclami ([134]). Da allora l'ANPD riceve ogni mese circa 400 reclami e 100 richieste da persone fisiche ([135]).

2.4.11. *Trasferimenti successivi*

(96) Il livello di protezione offerto ai dati personali trasferiti dall'Unione verso titolari del trattamento e responsabili del trattamento in Brasile non deve essere compromesso da ulteriori trasferimenti di tali dati a destinatari che si trovano in un paese terzo.

(97) Tali «trasferimenti successivi» costituiscono trasferimenti internazionali dal Brasile dalla prospettiva del titolare del trattamento brasiliano.

(98) Il capo V della LGPD istituisce un quadro per i trasferimenti internazionali di dati personali. Le disposizioni di questo capo sono ulteriormente integrate da un regolamento vincolante sui trasferimenti internazionali di dati (regolamento sui trasferimenti di dati), adottato dall'ANPD nell'agosto 2024 ([136]).

(99) Il regolamento sui trasferimenti di dati definisce il «trasferimento» come un'operazione di trattamento mediante la quale un soggetto incaricato del trattamento trasmette e condivide dati personali o fornisce l'accesso ad essi a un altro soggetto incaricato del trattamento e un «trasferimento internazionale di dati» come un trasferimento di dati personali verso un paese estero o un'organizzazione internazionale di cui il paese è membro ([137]).

([131]) Articoli 1, 6 e 9 della legge n. 12.527 del 18 novembre 2011 – legge sull'accesso alle informazioni.

([132]) Articolo 8, paragrafo 2, del regolamento dell'ANPD sul calcolo e sull'applicazione delle sanzioni amministrative, febbraio 2023 («regolamento sulle sanzioni»), disponibile all'indirizzo: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077.

([133]) Relazione dell'ANPD sul quarto anno dell'ANPD, novembre 2023, pagg. 24-25, disponibile all'indirizzo: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/balanco-de-4-anos-anpd-2024.pdf/view.

([134]) Piattaforma dell'ANPD per le persone fisiche, disponibile all'indirizzo: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados.

([135]) Relazione dell'ANPD sul quarto anno dell'ANPD, novembre 2023, pag. 25.

([136]) Regolamento dell'ANPD sui trasferimenti internazionali di dati, agosto 2024, disponibile in portoghese all'indirizzo: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396 e in inglese all'indirizzo: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/regulation-on-international-transfer-of-personal-data.pdf.

([137]) Articolo 3, punti III e IV, del regolamento dell'ANPD sui trasferimenti internazionali di dati, agosto 2024, e articolo 5, punto XV, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

(100) Le norme sui trasferimenti internazionali stabilite dalla LGPD e dal regolamento sui trasferimenti di dati si applicano a tutti i trattamenti che rientrano nell'ambito di applicazione della LGPD. L'articolo 7 del regolamento sui trasferimenti di dati chiarisce espressamente che l'applicabilità della LGPD a un trasferimento internazionale di dati non dipende dai mezzi tecnici utilizzati per il trattamento, dall'ubicazione geografica dei dati o dalla presenza fisica del titolare del trattamento o del responsabile del trattamento ([138]). Piuttosto, ciò che determina l'applicabilità è l'esistenza di un nesso sostanziale tra l'attività di trattamento dei dati e il Brasile.

(101) Analogamente agli articoli da 44 a 49 del regolamento (UE) 2016/679, l'articolo 33 della LGPD stabilisce le circostanze esclusive in cui un trasferimento internazionale di dati può essere autorizzato. Tali circostanze sono ulteriormente specificate all'articolo 9 del regolamento sui trasferimenti di dati.

(102) Un trasferimento internazionale di dati può aver luogo se si verificano tutte e tre le circostanze che seguono: in primo luogo, un trasferimento internazionale di dati può essere effettuato soltanto per finalità legittime, specifiche ed esplicite comunicate all'interessato, escludendo qualsiasi trattamento successivo incompatibile con tali finalità ([139]); in secondo luogo, il trasferimento internazionale di dati deve fondarsi su una valida base giuridica stabilita dall'articolo 7 della LGPD (o dall'articolo 11 in caso di dati sensibili) ([140]); in terzo luogo, deve essere utilizzato un meccanismo di trasferimento di dati «valido» ([141]).

(103) L'articolo 33 della LGPD prevede diversi meccanismi per il trasferimento di dati.

(104) In primo luogo, una decisione di adeguatezza può essere adottata nei confronti di un paese terzo o di un'organizzazione internazionale (articolo 33, punto I). Nel determinare se un paese terzo o un'organizzazione internazionale garantisce un livello adeguato di protezione dei dati personali, l'ANPD prende in considerazione diversi criteri stabiliti nell'ambito della LGPD e del regolamento sui trasferimenti di dati ([142]) che sono simili a quelli previsti dal diritto dell'UE. Questi comprendono: 1) la legislazione generale e quella settoriale in vigore nel paese di destinazione o applicabili all'organizzazione internazionale, che hanno un impatto diretto sulla protezione dei dati personali ([143]); 2) il tipo di dati ([144]); 3) la garanzia che il paese terzo o l'organizzazione internazionale prevede un livello di protezione dei dati personali e tutela i diritti degli interessati coerente con la LGPD ([145]); 4) l'adozione di misure tecniche e organizzative adeguate per garantire la sicurezza dei dati e attenuare i rischi di impatti negativi sulla vita privata e su altri diritti fondamentali ([146]); 5) la presenza di meccanismi giudiziari e istituzionali atti a garantire i diritti alla protezione dei dati, in particolare attraverso l'istituzione di un'autorità di controllo indipendente dotata di poteri e risorse adeguati per monitorare e applicare le disposizioni in materia di protezione dei dati ([147]); 6) qualsiasi altra circostanza specifica che sia pertinente al contesto del trasferimento internazionale di dati ([148]).

([138]) Articolo 7 del regolamento dell'ANPD sui trasferimenti internazionali di dati, agosto 2024.
([139]) Articolo 9 del regolamento dell'ANPD sui trasferimenti internazionali di dati, agosto 2024.
([140]) Articolo 9, punto I, del regolamento dell'ANPD sui trasferimenti internazionali di dati, agosto 2024.
([141]) Articolo 9, punto II, del regolamento dell'ANPD sui trasferimenti internazionali di dati, agosto 2024.
([142]) Articolo 34 della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) e capo V del regolamento dell'ANPD sui trasferimenti internazionali di dati, agosto 2024.
([143]) Articolo 34, punto I, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) e articolo 11, punto I, del regolamento dell'ANPD sui trasferimenti internazionali di dati, agosto 2024.
([144]) Articolo 34, punto II, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) e articolo 11, punto II, del regolamento dell'ANPD sui trasferimenti internazionali di dati, agosto 2024.
([145]) Articolo 34, punto III, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) e articolo 11, punto III, del regolamento dell'ANPD sui trasferimenti internazionali di dati, agosto 2024.
([146]) Articolo 34, punto IV, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) e articolo 11, punto IV, del regolamento dell'ANPD sui trasferimenti internazionali di dati, agosto 2024.
([147]) Articolo 11, paragrafo 3, del regolamento dell'ANPD sui trasferimenti internazionali di dati, agosto 2024.
([148]) Articolo 34, punto VI, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) e articolo 11, punto VI, del regolamento dell'ANPD sui trasferimenti internazionali di dati, agosto 2024.

(105) Per valutare il livello di protezione dei dati personali nell'ambito di una decisione di adeguatezza, l'ANPD terrà anche conto degli elementi seguenti: 1) i rischi e i benefici previsti da una specifica decisione di adeguatezza, considerando, tra l'altro, la garanzia dei principi, dei diritti dell'interessato e del regime di protezione dei dati previsti dalla LGPD; e 2) l'impatto della decisione sul flusso internazionale di dati, sulle relazioni diplomatiche, sul commercio internazionale e sulla cooperazione internazionale del Brasile con altri paesi e organizzazioni internazionali ([149]). La valutazione e l'emissione di una decisione di adeguatezza sono di competenza dell'ANPD ([150]). Attualmente l'ANPD sta lavorando esclusivamente a una decisione di adeguatezza con l'Unione europea.

(106) In secondo luogo, l'articolo 33, punto II, stabilisce che i trasferimenti di dati possono aver luogo quando i titolari del trattamento forniscono garanzie di conformità ai principi e ai diritti degli interessati nonché al regime di protezione dei dati previsti dalla LGPD. Ciò può essere garantito da 1) clausole contrattuali specifiche (punto II, lettera a)); 2) clausole contrattuali tipo (punto II, lettera b)); 3) norme vincolanti d'impresa (punto II, lettera c)); oppure 4) sigilli, certificazioni e codici di condotta approvati (punto II, lettera d)).

(107) I titolari del trattamento possono avvalersi di disposizioni contrattuali specifiche per i trasferimenti internazionali nonché di clausole contrattuali tipo approvate dall'ANPD ([151]). Ai sensi del regolamento sui trasferimenti di dati, l'ANPD ha adottato una serie di clausole contrattuali tipo che contemplano tutte le prescrizioni pertinenti in materia di protezione dei dati (ossia i diritti degli interessati, la vigilanza e il controllo indipendenti, le misure di sicurezza dei dati, le garanzie sui trasferimenti successivi, ecc.) ([152]). Tali clausole prevedono disposizioni che non possono essere modificate dalle parti del contratto ([153]). Le clausole sono modulari per potersi adattare a diversi scenari di trasferimento dei dati (ad esempio, dal titolare del trattamento al responsabile del trattamento, oppure tra responsabili del trattamento) ([154]).

(108) Per quanto riguarda le norme vincolanti d'impresa, il capo VI del regolamento sui trasferimenti di dati dell'ANPD chiarisce in che modo tale meccanismo può essere utilizzato, nonché le prescrizioni per la validità di dette norme. L'ANPD ricorda, in particolare, la «natura vincolante» dello strumento per tutti i «membri del gruppo o conglomerato» che vi fanno ricorso, gli obblighi relativi ai diritti degli interessati e al loro esercizio, le norme applicabili in materia di responsabilità ([155]) e tutte le informazioni obbligatorie che le norme vincolanti d'impresa devono contenere ([156]). Le norme vincolanti d'impresa sono soggette alla previa approvazione dell'ANPD secondo una procedura definita nel capo VIII del regolamento sui trasferimenti di dati, che impone alle imprese di presentare una documentazione completa all'ANPD e prevede un processo di riesame da parte dell'ANPD ([157]). Le imprese sono inoltre tenute a comunicare all'ANPD eventuali questioni che possano compromettere la conformità alla LGPD, inclusi i casi in cui alcuni membri del gruppo diventano soggetti a obblighi stranieri ([158]). Tutte le norme vincolanti d'impresa approvate saranno pubblicate sulla pagina web dell'ANPD e le imprese sono tenute a informare in modo trasparente in merito ai trasferimenti internazionali effettuati ([159]).

([149]) Articolo 12 del regolamento dell'ANPD sui trasferimenti internazionali di dati, agosto 2024.

([150]) La procedura per l'emissione di una decisione di adeguatezza è descritta nella sezione III del regolamento sui trasferimenti internazionali di dati dell'agosto 2024.

([151]) Articolo 35 della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([152]) Allegato II del regolamento dell'ANPD sui trasferimenti internazionali di dati, agosto 2024.

([153]) Allegato II, sezione II, del regolamento dell'ANPD sui trasferimenti internazionali di dati, agosto 2024.

([154]) Allegato II, clausola 4, del regolamento dell'ANPD sui trasferimenti internazionali di dati, agosto 2024. I titolari del trattamento e i responsabili del trattamento possono scegliere l'«opzione» appropriata che corrisponde alla loro situazione ai sensi di tale clausola.

([155]) Articolo 3, punto VIII, del regolamento dell'ANPD sui trasferimenti internazionali di dati, agosto 2024. Secondo la definizione di entità responsabile, un'impresa con sede in Brasile è responsabile di eventuali violazioni delle norme vincolanti d'impresa, anche se derivanti da un atto compiuto da un membro del gruppo economico con sede in un altro paese: l'approccio è simile a quello previsto all'articolo 47, paragrafo 1, lettera f), del regolamento (UE) 2016/679.

([156]) Articolo 27 del regolamento dell'ANPD sui trasferimenti internazionali di dati, agosto 2024.

([157]) Articoli 27 e 28 e capo VIII del regolamento dell'ANPD sui trasferimenti internazionali di dati, agosto 2024.

([158]) Articolo 25, punto VIII, del regolamento dell'ANPD sui trasferimenti internazionali di dati, agosto 2024.

([159]) Articolo 32 del regolamento dell'ANPD sui trasferimenti internazionali di dati, agosto 2024. Questo articolo indica inoltre che le imprese sono tenute a mettere le norme vincolanti d'impresa a disposizione degli interessati su loro richiesta.

(109) L'ANPD può anche designare organismi di certificazione per mettere a punto sigilli, certificazioni o codici di condotta per i trasferimenti di dati ([160]). Le decisioni e le attività svolte da tali organismi di certificazione possono essere riesaminate dall'ANPD, che può rivedere e revocarne le decisioni in caso di non conformità con la LGPD ([161]).

(110) Infine, la LGPD contiene un elenco di «situazioni specifiche» in cui può essere effettuato un trasferimento internazionale: 1) quando è necessario per la cooperazione giuridica internazionale tra agenzie pubbliche, conformemente al diritto internazionale; 2) quando è necessario per proteggere la vita o l'incolumità fisica dell'interessato o di terzi; 3) quando è autorizzato dall'ANPD; 4) quando è relativo a un impegno nell'ambito della cooperazione internazionale; 5) quando è necessario per l'esecuzione di una politica pubblica o di un obbligo giuridico di un'autorità pubblica; 6) quando gli interessati hanno acconsentito al trasferimento specifico dei dati dopo essere stati informati della natura del trattamento; 7) quando è necessario per adempiere un obbligo giuridico o normativo, in relazione a quanto disposto da un contratto, o per l'esercizio di diritti nell'ambito di procedure giudiziarie, amministrative o arbitrali ([162]). Come indicato nel regolamento sui trasferimenti di dati, i trasferimenti internazionali possono essere effettuati in dette situazioni soltanto se conformi alle specificità del caso particolari e agli obblighi giuridici applicabili ([163]).

(111) Per quanto riguarda la situazione specifica in cui il trasferimento dei dati può essere effettuato sulla base del consenso degli interessati, essa richiede che 1) sia rispettato il criterio formale per l'ottenimento di un consenso valido (ossia essere specifico, libero, inequivocabile e informato); 2) gli interessati siano informati della natura del trasferimento *prima* che sia effettuato (ad es. in merito alla giurisdizione del trasferimento previsto e al livello di protezione che garantisce, alla mancanza di una decisione di adeguatezza o di altri meccanismi di trasferimento dei dati; alla durata dei trasferimenti); 3) il consenso sia ottenuto per ciascun trasferimento specificamente e separatamente a ogni altro trattamento. Come indicato nel considerando 46, il tacito accordo non può essere considerato una forma di consenso valida e gli interessati hanno il diritto di revocare il consenso in ogni momento.

(112) Il regolamento sui trasferimenti di dati inquadra rigorosamente il ricorso a tutti questi meccanismi dettando diverse condizioni. Queste comprendono, in particolare, l'obbligo di fornire all'interessato informazioni chiare, accurate e facilmente accessibili sul trasferimento, di garantire ed essere in grado di dimostrare che i trasferimenti internazionali siano effettuati nel rispetto dei principi e dei diritti dell'interessato e non alterino il livello di protezione previsto dalla LGPD, indipendentemente dal paese di ubicazione dei dati personali oggetto del trasferimento, e ciò anche dopo la fine del trattamento e nel caso di trasferimenti successivi ([164]). Tali condizioni si applicano anche quando i trasferimenti sono condotti sulla base di «situazioni specifiche», per garantire la continuità della protezione a prescindere dallo strumento usato per effettuare un trasferimento internazionale.

(113) Le norme descritte nei considerando da 96 a 112 della presente decisione assicurano pertanto la continuità della protezione quando i dati personali sono ulteriormente trasferiti dal Brasile in un modo che è essenzialmente equivalente a quanto previsto dal regolamento (UE) 2016/679.

2.4.12. *Responsabilizzazione*

(114) Secondo il principio di responsabilizzazione, i soggetti che trattano dati sono tenuti a mettere in atto misure tecniche e organizzative adeguate per rispettare efficacemente i loro obblighi in materia di protezione dei dati e per essere in grado di dimostrare tale rispetto, in particolare all'autorità di controllo competente.

([160]) Articolo 35, paragrafo 3, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([161]) Articolo 35, paragrafo 4, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([162]) Articolo 33, punti da III a IX, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([163]) Articolo 1, comma unico, del regolamento dell'ANPD sui trasferimenti internazionali di dati, agosto 2024.

([164]) Articolo 2, punti I e IV, e articolo 4, del regolamento dell'ANPD sui trasferimenti internazionali di dati, agosto 2024. Come tutti i trasferimenti internazionali, qualsiasi trasferimento effettuato nell'ambito di tali scenari deve avvenire per finalità legittime, specifiche ed esplicite comunicate all'interessato, escludendo qualsiasi trattamento successivo incompatibile con tali finalità, come stabilito dall'articolo 9, frase introduttiva, del regolamento dell'ANPD sui trasferimenti internazionali di dati, agosto 2024.

(115) L'articolo 6, punto X, della LGPD stabilisce il principio di responsabilizzazione in base al quale il titolare del trattamento e il responsabile del trattamento adottano misure «efficaci e capaci» di dimostrare il rispetto della LGPD.

(116) Come mezzo per garantire la responsabilizzazione, l'articolo 50 della LGPD prevede che i titolari del trattamento e i responsabili del trattamento possano adottare norme e modelli di governance interni, in particolare per garantire buone pratiche nella gestione dei reclami e delle richieste degli interessati, nel rispetto degli obblighi di sicurezza e di tutti gli altri obblighi previsti dalla LGPD («buone pratiche e governance»). Tali programmi dovrebbero comprendere anche piani per attività formative, un meccanismo di supervisione interna e l'attenuazione dei rischi.

(117) La LGPD prevede inoltre l'obbligo di nominare un responsabile della protezione dei dati che svolga un ruolo significativo nella progettazione e nell'attuazione di tali programmi interni. A norma dell'articolo 5, punto VIII, il responsabile della protezione dei dati funge da collegamento tra il titolare del trattamento, gli interessati e l'ANPD. L'articolo 41 della LGPD impone a tutti i titolari del trattamento di nominare un responsabile della protezione dei dati e di rendere pubblica la sua identità.

(118) La LGPD conferisce all'ANPD il potere di introdurre un'esenzione dall'obbligo in capo ai titolari del trattamento e ai responsabili del trattamento di nominare un responsabile della protezione dei dati ([165]). Nel suo regolamento relativo all'applicazione della LGPD alle piccole e medie imprese (PMI), l'ANPD ha stabilito che talune piccole imprese, PMI, start-up e organizzazioni senza scopo di lucro possono rientrare nell'ambito di tale esenzione ([166]). Nello specifico, l'ambito dell'esenzione copre i soggetti seguenti: microimprese, piccole imprese, start-up, soggetti giuridici di diritto privato, comprese le organizzazioni senza scopo di lucro, conformemente alla legislazione vigente, nonché persone fisiche e soggetti privati resi anonimi che trattano dati personali ([167]). Ai sensi del diritto brasiliano, per microimprese ([168]), piccole imprese ([169]) o start-up ([170]) s'intendono le imprese con un unico dipendente o un numero contenuto di dipendenti ([171]) e i cui ricavi lordi annui sono inferiori a una data soglia ([172]).

(119) L'esenzione dalla nomina di un responsabile della protezione dei dati non si applica a nessuna di tali società ed entità, indipendentemente dalle loro dimensioni o dai loro ricavi, nel caso di trattamenti «ad alto rischio» di dati personali ([173]). Un trattamento è considerato ad alto rischio se, cumulativamente, presenta almeno una delle caratteristiche generali che seguono: 1) trattamento di dati personali su larga scala; 2) trattamento di dati che può incidere in modo significativo sui diritti e sugli interessi fondamentali degli interessati; e almeno una delle caratteristiche specifiche che seguono: 1) impiego di tecnologie emergenti o innovative; 2) sorveglianza o controllo di aree accessibili al pubblico; 3) uso esclusivo di processi decisionali automatizzati; 4) trattamento di dati sensibili o

([165]) Articolo 41, paragrafo 3, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([166]) Regolamento dell'ANPD sull'applicazione della LGPD alle piccole e medie imprese («regolamento sulle PMI»), aprile 2024, disponibile all'indirizzo: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022.

([167]) Articolo 2, punto I, del regolamento dell'ANPD sulle PMI, aprile 2024.

([168]) Per «microimpresa» si intende un'impresa con ricavi lordi annui pari o inferiori a 360 000 real brasiliani («R$»). Cfr. l'articolo 3, punto I, della legge complementare n. 123 del 14 dicembre 2006 – legge sullo status nazionale delle micro, piccole e medie imprese. L'importo di 360 000 R$ equivale a 56 500 EUR.

([169]) Per «piccola impresa» o «PMI» si intende un'impresa con ricavi lordi annui di almeno 360 000 R$ e pari o inferiori a 4 800 000 R$. Cfr. l'articolo 3, punto II, della legge complementare n. 123 del 14 dicembre 2006 – legge sullo status nazionale delle micro, piccole e medie imprese. L'importo di 4 800 000 R$ equivale a 753 000 EUR.

([170]) Per «start-up» si intende un'impresa o un'organizzazione aziendale, sia essa nascente o recentemente operativa, le cui attività sono caratterizzate dall'innovazione applicata al proprio modello aziendale o ai prodotti o servizi da questa offerti. Cfr. l'articolo 2, punto III, del regolamento dell'ANPD sulle PMI, aprile 2024.
Una start-up può essere registrata come tale per un massimo di 10 anni e può avere ricavi annui lordi non superiori a 16 000 000 R$. Cfr. l'articolo 4, punto I, della legge complementare n. 182 del 1º giugno 2021 – legge sulle start-up, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp182.htm L'importo di 16 000 000 R$ equivale a 2 500 000 EUR.

([171]) Cfr. in particolare l'articolo 2, punto II, del regolamento dell'ANPD sulle PMI, aprile 2024, e l'articolo 41 della legge n. 14.195 del 26 agosto 2021 – legge sulla costituzione delle società, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14195.htm.

([172]) Legge complementare n. 123 del 14 dicembre 2006 – legge sullo status nazionale delle micro, piccole e medie imprese, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp123.htm.

([173]) Articolo 4 del regolamento dell'ANPD sulle PMI, aprile 2024.

di dati concernenti minori o anziani ([174]). Un trattamento «su larga scala» di dati personali è definito come un trattamento che coinvolge un numero significativo di interessati, considerando anche il volume dei dati in questione, nonché la durata, la frequenza e l'estensione geografica del trattamento effettuato ([175]). Un trattamento di dati che può incidere in modo significativo sui diritti e sugli interessi fondamentali degli interessati è, tra l'altro, quello in cui l'attività di trattamento può impedire l'esercizio di diritti o la fruizione di un servizio, nonché causare danni materiali o morali agli interessati, tra cui discriminazione, violazione dell'integrità fisica, del diritto all'immagine e alla reputazione, frode finanziaria o furto d'identità ([176]).

(120) L'ANPD ha adottato un regolamento vincolante sul ruolo del responsabile della protezione dei dati che ne chiarisce ulteriormente i compiti ([177]). Tale regolamento ricorda l'obbligo per i soggetti privati e le autorità pubbliche di pubblicare informazioni sull'identità del proprio responsabile della protezione dei dati ([178]). L'articolo 10 del regolamento ricorda l'obbligo per i titolari del trattamento e i responsabili del trattamento di garantire, tra l'altro, che il responsabile della protezione dei dati possa svolgere i suoi compiti in modo indipendente, senza indebite interferenze, in particolare fornendo orientamenti sulle pratiche da adottare in relazione alla protezione dei dati personali, e che abbia accesso diretto al più alto livello dirigenziale e a tutti i dipendenti coinvolti nelle decisioni strategiche per il trattamento dei dati all'interno di un'entità. Analogamente, il responsabile della protezione dei dati deve svolgere le sue funzioni e i suoi compiti con etica, integrità e indipendenza tecnica, evitando situazioni che possono configurare un conflitto di interessi ([179]).

(121) Il ruolo del responsabile della protezione dei dati è stato una priorità dell'azione esecutiva dell'ANPD. Ad esempio, le prime sanzioni comminate dall'ANPD hanno riguardato una società che è stata sanzionata e ha ricevuto un ammonimento specifico per non aver dimostrato di aver nominato un responsabile della protezione dei dati ([180]). La società ha poi nominato un responsabile della protezione dei dati durante il procedimento amministrativo per conformarsi al provvedimento dell'ANPD. Da allora l'ANPD ha continuato a comminare sanzioni a soggetti pubblici e privati in relazione alle disposizioni riguardanti la nomina di un responsabile della protezione dei dati previste dalla LGPD ([181]).

(122) La valutazione d'impatto sulla protezione dei dati è un altro strumento importante per garantire la responsabilizzazione: consente di valutare e determinare l'impatto di un trattamento. Ai sensi dell'articolo 38 della LGPD, l'ANPD può chiedere al titolare del trattamento o al responsabile del trattamento di effettuare una valutazione d'impatto sulla protezione dei dati ([182]), che deve includere una descrizione del tipo di trattamento dei dati personali nonché le misure, le garanzie e i meccanismi previsti per attenuare i rischi. Inoltre la sezione II della LGPD prevede disposizioni in materia di responsabilizzazione che conferiscono all'ANPD il potere di richiedere la pubblicazione della valutazione d'impatto sulla protezione dei dati o di raccomandare l'adozione di «buone pratiche» per la protezione dei dati personali da parte delle autorità pubbliche ([183]).

(123) Alla luce degli obblighi e delle prassi in materia di responsabilizzazione di cui ai considerando da 114 a 122 della presente decisione, il quadro brasiliano attua il principio di responsabilizzazione in modo analogo alle misure di cui al capo 4, sezioni 3 e 4, del regolamento (UE) 2016/679, anche prevedendo diversi meccanismi per garantire e dimostrare la conformità alla LGPD.

2.5. **Vigilanza ed esecuzione**

(124) Al fine di garantire un livello adeguato di protezione dei dati nella pratica, dovrebbe esistere un'autorità di controllo indipendente cui siano conferiti i poteri di monitorare e assicurare il rispetto delle norme in materia di protezione dei dati. Tale autorità dovrebbe agire in piena indipendenza e imparzialità nell'esercizio delle proprie funzioni e dei propri poteri.

([174]) Articolo 4, punti I e II, del regolamento dell'ANPD sulle PMI, aprile 2024.
([175]) Cfr., ad esempio, l'articolo 4, paragrafo 1, del regolamento dell'ANPD sulle PMI, aprile 2024.
([176]) Cfr., ad esempio, l'articolo 4, paragrafo 2, del regolamento dell'ANPD sulle PMI, aprile 2024.
([177]) Regolamento dell'ANPD sul ruolo del responsabile della protezione dei dati in relazione al trattamento dei dati personali («regolamento sul responsabile della protezione dei dati»), luglio 2024, disponibile all'indirizzo: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074.
([178]) Articoli 5 e 9 del regolamento dell'ANPD sul responsabile della protezione dei dati, luglio 2024.
([179]) Articolo 18 del regolamento dell'ANPD sul responsabile della protezione dei dati, luglio 2024.
([180]) Cfr. la relazione di istruzione n. 1/2023 dell'ANPD - Telekall Infoservice, disponibile all'indirizzo: https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000489_2022_62_decisao_telekall_inforservice.pdf.
([181]) Cfr., ad esempio, la relazione di istruzione n. 5/2024 dell'ANPD - Ministério da Saúde, disponibile all'indirizzo: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/decisoes-em-processos-sancionadores-1/relatorio_de_instrucao_5_publico_ocultado.pdf.
([182]) Articolo 38 della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.
([183]) Sezione II della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

2.5.1. *Vigilanza indipendente*

(125) In Brasile l'autorità di controllo indipendente incaricata del monitoraggio e dell'applicazione della LGPD è l'Agência Nacional de Proteção de Dados (ANPD).

(126) L'ANPD è stata istituita dall'articolo 55-A della LGPD ed è stata trasformata in un organismo indipendente dapprima mediante un decreto provvisorio e poi mediante una legge del 2022 ([184]). L'adozione della legge che ha modificato la natura dell'ANPD ha comportato l'introduzione di alcuni cambiamenti nella LGPD per revocare le disposizioni che subordinavano il funzionamento e le operazioni finanziarie dell'ANPD alle autorizzazioni che dovevano essere rilasciate dall'esecutivo a norma della legge di bilancio del Brasile ([185]). La disposizione modificata della LGPD riconosce che l'ANPD è un'autorità speciale, dotata di autonomia tecnica e decisionale nonché di mezzi propri e con sede nel Distretto federale ([186]).

(127) In quanto «autorità di natura speciale», l'ANPD dispone dell'autonomia necessaria per svolgere pienamente le sue funzioni giuridiche ed esercitare i poteri stabiliti dalla LGPD, compresa la gestione amministrativa dell'agenzia ([187]). Ciò include l'autonomia nella gestione delle spese e delle assunzioni ([188]). L'ANPD è stata inizialmente creata come «autorità» e in seguito, nel settembre 2025, ha cambiato nome diventando un'«agenzia», in linea con altri 11 enti di regolamentazione che godono di questo grado superiore di indipendenza in Brasile (ad es. l'agenzia nazionale per l'elettricità, l'agenzia nazionale per le telecomunicazioni ecc.) ([189]).

(128) Le risorse dell'ANPD provengono in gran parte dal bilancio generale dello Stato federale brasiliano. Inoltre il bilancio dell'ANPD può comprendere donazioni, sovvenzioni o altri crediti di cui all'articolo 55-L della LGPD. Dalla sua istituzione nel 2021, l'ANPD è cresciuta in maniera esponenziale. Le relazioni annuali dell'ANPD indicano che alla fine del 2023 l'autorità contava 141 dipendenti/funzionari pubblici, pur essendo stata istituita solo quattro anni prima ([190]). Il bilancio annuale dell'ANPD per il 2025 è di 18 milioni di R$ ([191]). Nel settembre 2025 è stata annunciata la creazione in Brasile di un nuovo percorso di carriera nel servizio pubblico sulla «protezione dei dati», con 200 posti, nel quadro di un ampliamento del personale dell'ANPD previsto per i prossimi anni ([192]).

([184]) L'articolo 55-A della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD), nella sua formulazione originaria, è stato modificato dalla legge n. 14.460 del 25 ottobre 2022 – legge che trasforma l'ANPD in un'autorità con status speciale. Per quanto riguarda l'indipendenza, cfr. la misura provvisoria n. 1.124, del 13 giugno 2022, che trasforma l'ANPD in un'autorità con status speciale, disponibile all'indirizzo https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Mpv/mpv1124.htm, e legge n. 14.460 del 25 ottobre 2022 – legge che trasforma l'ANPD in un'autorità con status speciale, disponibile all'indirizzo https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Lei/L14460.htm. La possibilità per il governo di modificare lo status dell'ANPD per aumentarne l'indipendenza era illustrata in dettaglio nell'articolo 55-A, paragrafo 1, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati, successivamente revocato.

([185]) Cfr. l'articolo 9 della legge n. 14.460 del 25 ottobre 2022 – legge che trasforma l'ANPD in un'autorità con status speciale, che revoca e sostituisce l'articolo 55-A della legge n. 13.709, del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([186]) Articolo 7 della legge n. 14.460 del 25 ottobre 2022 – legge che trasforma l'ANPD in un'autorità con status speciale.

([187]) Cfr. ANPD, L'ANPD diventa un'autorità di natura speciale, giugno 2022, disponibile all'indirizzo: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-torna-se-autarquia-de-natureza-especial.

([188]) Articolo 55-L della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([189]) Articolo 1 del decreto n. 1.317 del 17 settembre 2025 che modifica l'LGPD per trasformare l'Agência Nacional de Proteção de Dados, disponibile all'indirizzo: https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314, e articolo 2, punto XII, della legge n. 13.848 del 25 giugno 2019 sull'organizzazione delle agenzie di regolamentazione, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13848.htm.

([190]) Relazione dell'ANPD sul quarto anno dell'ANPD, novembre 2023, pag. 8, disponibile all'indirizzo: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/balanco-de-4-anos-anpd-2024.pdf/view.

([191]) 18 225 566 R$ (2 857 768 EUR). Cfr. la legge annuale di bilancio, pag. 190, disponibile all'indirizzo: LEI15121-VOLUME I.pdf.

([192]) Articolo 9, punto I, del decreto n. 1.317 del 17 settembre 2025 che modifica l'LGPD per trasformare l'Agência Nacional de Proteção de Dados, disponibile all'indirizzo: https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314.

(129) L'ANPD è composta da un consiglio di amministrazione (l'organo direttivo più alto), un consiglio nazionale per la protezione dei dati personali e della vita privata (dotato di poteri consultivi) e diversi uffici e unità amministrative ([193]). Questa struttura è stabilita nell'articolo 55-C della LGPD e ulteriormente precisata in due decreti adottati rispettivamente nel 2020 e nel 2023 ([194]).

(130) Il consiglio di amministrazione è composto da cinque direttori, tra cui il presidente dell'Autorità. Ciascun membro del consiglio di amministrazione dell'ANPD è nominato per cinque anni dal presidente della Repubblica del Brasile, previa approvazione del Senato federale ([195]).

(131) I direttori sono brasiliani e hanno un alto livello di istruzione pertinente alla carica ([196]). Per garantire la loro indipendenza, tutti i direttori devono astenersi, tra l'altro, da qualsiasi attività legata a profitti o attività politica, nonché dal ricoprire incarichi di direzione o di consulenza in qualsiasi impresa ([197]). Inoltre la legge brasiliana che disciplina l'esercizio di posizioni dirigenziali all'interno della pubblica amministrazione federale stabilisce che coloro che ricoprono funzioni equivalenti a quelle dei direttori dell'ANPD non possono, tra l'altro, svolgere attività incompatibili con le loro funzioni ([198]). Ciò include l'esercizio di attività di consulenza o intermediazione di interessi privati (anche informalmente) o la prestazione di servizi a favore di entità soggette alla vigilanza o alla regolamentazione dell'ANPD, anche su base occasionale. Al termine del loro mandato presso l'ANPD e per i sei mesi successivi, ai direttori è precluso l'esercizio di determinate funzioni che possono far sorgere il rischio di un conflitto di interessi ([199]).

(132) I direttori possono perdere il proprio incarico solo in circostanze specifiche previste dall'articolo 55-E della LGPD, vale a dire in seguito a dimissioni, condanne giudiziarie definitive e inappellabili o licenziamento a causa di un procedimento amministrativo disciplinare. La legge federale sul pubblico impiego stabilisce che tale sanzione deve essere giustificata e può essere proposta solo in caso di reati specifici dimostrati (ad esempio colpa grave, corruzione, uso irregolare di fondi pubblici) ([200]). Queste norme e procedure garantiscono ai direttori dell'ANPD una tutela istituzionale nell'esercizio delle loro funzioni. Finora nessun direttore dell'ANPD è stato licenziato o è stato oggetto di procedimenti disciplinari. Il consiglio di amministrazione dell'ANPD è stato istituito ed è rimasto invariato a seguito di un cambiamento di amministrazione in Brasile avvenuto nel 2023.

([193]) Articolo 55-C della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([194]) Decreto n. 10.474, del 26 agosto 2020, sulla struttura dell'ANPD, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10474.htm, modificato dal decreto n. 11.758, del 30 ottobre 2023, sulla struttura modificata dell'ANPD, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11758.htm#art1.

([195]) Articolo 55-D, paragrafi 1 e 3, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati, e articolo 12 del decreto n. 1.317 del 17 settembre 2025 che modifica l'LGPD per trasformare l'Agência Nacional de Proteção de Dados, disponibile all'indirizzo: https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314. L'articolo 12 del decreto estende la durata del mandato dei direttori dell'ANPD da quattro a cinque anni per allinearla con tutte le altre agenzie di regolamentazione indipendenti esistenti in Brasile. Tutti i direttori dell'ANPD nominati prima dell'adozione di detto decreto completeranno un mandato di quattro anni, come previsto dalla legge al momento della loro nomina.

([196]) Articolo 55-D, paragrafo 2, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([197]) Articolo 11 del decreto n. 10.474, del 26 agosto 2020, sulla struttura dell'ANPD.

([198]) Articolo 5 della legge n. 12.813 del 16 maggio 2013 – legge sul conflitto di interessi per i dipendenti pubblici e altre funzioni nelle autorità pubbliche, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12813.htm.

([199]) Articolo 6 della legge n. 12.813 del 16 maggio 2013 – legge sul conflitto di interessi per i dipendenti pubblici e altre funzioni nelle autorità pubbliche.

([200]) L'elenco completo ed esaustivo dei reati figura all'articolo 132 della legge n. 8112 dell'11 dicembre 1990 – legge federale sul pubblico impiego e sui funzionari pubblici. Disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/leis/l8112cons.htm. Cfr. anche il capo V della legge sulle condizioni per l'applicazione di una sanzione.

(133) I compiti e i poteri dell'ANPD sono specificati all'articolo 55-J della LGPD. Comprendono, in particolare, l'elaborazione di politiche e orientamenti in materia di protezione dei dati, la promozione dell'adozione di norme che facilitino il controllo degli interessati sui dati personali che li riguardano, l'indagine sulle violazioni dei diritti individuali, la gestione dei reclami, il rispetto della LGPD e la comminazione di sanzioni, la garanzia di attività di formazione e promozione nel settore della protezione dei dati nonché lo scambio e la cooperazione con le autorità di protezione dei dati di paesi terzi ([201]).

(134) L'ANPD dispone di un organo consultivo costituito dal consiglio nazionale per la protezione dei dati personali e della vita privata, istituito dall'articolo 58-A della LGPD. Tale organo è composto da rappresentanti del potere esecutivo, legislativo e giudiziario, nonché della società civile, dei sindacati e del mondo delle imprese ([202]). Ha un ruolo puramente consultivo, che consiste nella preparazione di studi o relazioni annuali sulla protezione dei dati, nell'organizzazione di dibattiti pubblici e audizioni sulla protezione dei dati personali e della vita privata, nella formulazione di raccomandazioni non vincolanti all'ANPD e nella diffusione di conoscenze sulla protezione dei dati personali e della vita privata ([203]). La cooperazione tra l'ANPD e il consiglio nazionale è incentrata sulla promozione della protezione dei dati personali e della vita privata in Brasile. Il consiglio nazionale non ha poteri in materia di monitoraggio e applicazione della LGPD, in quanto soltanto l'ANPD ha l'autorità di sorvegliare l'applicazione della legge e farla rispettare, ad esempio, promulgando regolamenti, conducendo indagini e comminando sanzioni. In quanto autorità indipendente, l'ANPD non è tenuta a seguire alcun suggerimento formulato dal consiglio nazionale tramite le sue relazioni o le sue raccomandazioni non vincolanti.

2.5.2. *Applicazione, sanzioni comprese*

(135) Per garantire la conformità, il legislatore ha conferito all'ANPD tanto poteri di indagine quanto quelli di esecuzione, che spaziano dagli ammonimenti alle sanzioni amministrative pecuniarie.

(136) Per quanto riguarda i poteri di indagine, se si sospetta o è stata segnalata una violazione della LGPD, o se è necessario per tutelare i diritti degli interessati che sono stati o potrebbero essere violati, l'ANPD può effettuare in qualsiasi momento audit e ispezioni in loco presso titolari del trattamento del settore pubblico e privato e chiedere tutte le informazioni necessarie ([204]). In particolare, il regolamento vincolante sui poteri sanzionatori dell'ANPD stabilisce che i titolari del trattamento e i responsabili del trattamento devono garantire all'ANPD l'accesso a uffici/edifici, attrezzature, applicazioni, impianti, sistemi, strumenti e risorse tecnologiche, documenti, dati e informazioni di natura tecnica, operativa e di altro tipo pertinenti per la valutazione delle attività di trattamento dei dati personali, che siano in loro possesso o in possesso di terzi ([205]).

([201]) Articolo 55-J, punti da I a XXIV, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([202]) Per maggiori informazioni sui membri e sulle attività del consiglio nazionale, cfr. ANPD, Consiglio nazionale per la protezione dei dati personali e della vita privata, disponibile all'indirizzo: https://www.gov.br/anpd/pt-br/cnpd-2.

([203]) Articolo 58-B della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([204]) Articolo 55-J, punto XVI, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD), articolo 4, punto I, del decreto n. 10.474, del 26 agosto 2020, sulla struttura dell'ANPD e articolo 12 del regolamento dell'ANPD sulla notifica degli incidenti di sicurezza, aprile 2024.

([205]) Articolo 5 del regolamento dell'ANPD sui poteri sanzionatori dell'ANPD, ottobre 2021, disponibile all'indirizzo: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no1-2021.

(137) Nell'ambito dei suoi poteri correttivi, l'ANPD può emettere ammonimenti, ammende o altre sanzioni, tra cui ordini di cessazione temporanea del trattamento dei dati o di cancellazione di dati personali ([206]). 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 ([207]). Per rendere un'entità conforme, possono essere applicate varie sanzioni cumulative. Con un ammonimento, l'ANPD concede al titolare del trattamento un periodo di tempo specifico per adottare misure correttive al fine di rendere il trattamento conforme alla LGPD ([208]). In caso di inadempimento, si applicano sanzioni supplementari. Ad esempio, l'ANPD ha emesso diversi ammonimenti nei confronti del ministero della Salute, tra l'altro per aver mancato di produrre una valutazione d'impatto sulla protezione dei dati e di notificare una violazione dei dati ([209]). L'ANPD può imporre diverse sanzioni congiuntamente per tutelare i diritti degli interessati o per garantire il rispetto della LGPD. Ad esempio, l'ANPD può imporre una sanzione amministrativa pecuniaria per una violazione della LGPD emettendo contemporaneamente l'ordine di cancellare i dati legati a tale violazione ([210]). In caso di sanzioni non pecuniarie, l'ANPD può anche decidere di imporre «ammende giornaliere» fino al momento necessario per garantire il rispetto (della LGPD) entro un dato termine ([211]). L'ammenda giornaliera è applicata cumulativamente, considerando il tempo che intercorre tra l'incidenza dell'ammenda e l'adempimento dell'obbligo, e fino a un massimo di 50 milioni di R$ ([212]).

(138) Ai sensi dell'articolo 52, punto II, della LGPD, l'ANPD può infliggere sanzioni amministrative pecuniarie, oltre ad ammende giornaliere, fino al 2 % dei ricavi di un'entità in Brasile e fino a un massimo di 50 milioni di R$ ([213]). Le ammende possono essere cumulative in caso di violazioni multiple. Alcuni mesi dopo aver adottato il suo regolamento sulle sanzioni, l'ANPD ha inflitto le sue prime ammende pecuniarie nei confronti di una società di telecomunicazioni che non aveva individuato una base giuridica per il trattamento né nominato un responsabile della protezione dei dati. La società ha ricevuto un ammonimento e due ammende per un totale di 14 400 R$ ([214]). Nel regolamento vincolante sulle sanzioni, l'ANPD ha suddiviso le sanzioni in tre livelli di gravità, leggero, medio e grave ([215]), a seconda di un fattore consolidato, come il tipo di dati trattati e il relativo volume, il tipo di trattamento o l'impatto sui diritti dell'interessato. Ad esempio, le violazioni riguardanti il trattamento di dati personali sensibili sono soggette al massimo livello di sanzioni irrogabile dall'ANPD ([216]).

(139) Il regolamento sulle sanzioni prevede una metodologia per il calcolo delle ammende, anche per tenere conto di fattori aggravanti e/o attenuanti ([217]). Ad esempio, un'ammenda può essere aumentata del 10 % in caso di violazioni specifiche ripetute o addirittura del 90 % per ciascuna misura correttiva non rispettata entro un termine stabilito ([218]). Analogamente, un'ammenda può essere ridotta del 50 % se la violazione è sanata subito dopo l'avvio del procedimento amministrativo da parte dell'ANPD ([219]).

([206]) Articolo 55 e articolo 55-J, punto IV, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) e regolamento dell'ANPD sulle sanzioni, febbraio 2023.

([207]) Articolo 52, paragrafo 3. Legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([208]) Articolo 52, punto I, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([209]) Cfr. la decisione n. 4/2024 dell'ANPD, disponibile all'indirizzo https://www.gov.br/anpd/pt-br/centrais-de-conteudo/relatorio_de_instrucao_no_4_2024_fis_cgf_anpd_v-publica.pdf e la decisione n. 5/2024 dell'ANPD, disponibile all'indirizzo: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/decisoes-em-processos-sancionadores-1/relatorio_de_instrucao_5_publico_ocultado.pdf.

([210]) Articolo 52, punto VI, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([211]) Articolo 16 del regolamento dell'ANPD sulle sanzioni, febbraio 2023.

([212]) Articolo 16, paragrafo 1, del regolamento dell'ANPD sulle sanzioni, febbraio 2023. L'importo di 50 milioni di real brasiliani è pari a circa 7,8 milioni di EUR.

([213]) L'importo di 50 milioni di real brasiliani è pari a circa 7,8 milioni di EUR.

([214]) Decisione n. 1/2023 dell'ANPD, disponibile all'indirizzo: https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000489_2022_62_decisao_telekall_inforservice.pdf.

([215]) Articolo 8 del regolamento dell'ANPD sulle sanzioni, febbraio 2023.

([216]) Articolo 8, paragrafo 3, punto I, lettera d), del regolamento dell'ANPD sulle sanzioni, febbraio 2023.

([217]) Allegato I, articoli 12 e 13, del regolamento dell'ANPD sulle sanzioni, febbraio 2023.

([218]) Articolo 12, punti da I a IV, del regolamento dell'ANPD sulle sanzioni, febbraio 2023.

([219]) Articolo 13, punto I, del regolamento dell'ANPD sulle sanzioni, febbraio 2023.

(140) L'ordinamento brasiliano combina pertanto diversi tipi di sanzioni, dalle misure correttive alle sanzioni amministrative pecuniarie. L'ANPD ha iniziato a esercitare i propri poteri non appena la sua competenza sanzionatoria è divenuta effettiva ([220]). Finora ha emesso sanzioni e raccomandazioni nei confronti sia delle autorità pubbliche, anche nel settore della sicurezza, sia di operatori privati ([221]). Le sanzioni finora irrogate dall'ANPD riguardano un'ampia gamma di questioni, tra cui la mancata nomina di un responsabile della protezione dei dati, incidenti di sicurezza, comprese violazioni dei dati, o la mancata collaborazione con l'ANPD. Oltre all'irrogazione di sanzioni pecuniarie, l'ANPD è stata particolarmente attiva nell'utilizzare l'intera gamma dei poteri correttivi ad essa attribuiti, ad esempio per ordinare a titolari del trattamento di effettuare una valutazione d'impatto sulla protezione dei dati o di cessare il trattamento dei dati personali. Ad esempio, nel luglio 2024 l'ANPD ha emesso un provvedimento nei confronti di una grande piattaforma di social media, ordinando la sospensione del trattamento dei dati personali destinato all'addestramento di sistemi di intelligenza artificiale generativa (IA) in tutti i suoi prodotti ([222]). Oltre a questa misura preventiva, volta a tutelare i diritti fondamentali degli interessati, l'ANPD ha emesso un'ammenda giornaliera di 50 000 R$, applicabile fino a quando il trattamento non è stato reso conforme alla LGPD ([223]). Infine l'ANPD ha annunciato l'avvio di indagini nei confronti di diverse grandi piattaforme tecnologiche multinazionali, società di social media e una banca, proseguendo nel contempo le indagini nei confronti di soggetti del settore pubblico ([224]). Nei suoi pochi anni di attività, l'ANPD ha dato prova di vantare una solida esperienza in materia di applicazione delle norme, avvalendosi dell'intera gamma dei suoi poteri esecutivi.

(141) Infine, le sanzioni amministrative previste dalla LGPD non sostituiscono l'applicazione di altre sanzioni amministrative, civili e penali, comprese quelle stabilite dal codice brasiliano per la tutela del consumatore ([225]) e dal quadro civile di Internet ([226]). In particolare, il codice brasiliano per la tutela del consumatore impone alle imprese di fornire ai consumatori informazioni sulle loro operazioni commerciali e attività ([227]). L'articolo 56 del codice per la tutela del consumatore elenca inoltre le sanzioni irrogabili alle imprese in caso di non conformità, che vanno dalle ammende al divieto di vendere o produrre un prodotto o all'obbligo di sospendere un servizio. Inoltre gli articoli da 61 a 74 del codice per la tutela del consumatore elencano i reati per i quali i responsabili delle imprese possono dover scontare da sei mesi a due anni di prigione, anche in caso di dichiarazioni false o ingannevoli in relazione a un servizio o di promozione di un servizio che può arrecare danno al consumatore. Ad esempio, nel 2014 il dipartimento brasiliano per la difesa e la tutela del consumatore ha inflitto a una società di telecomunicazioni un'ammenda di 3,5 milioni di R$ per aver violato il codice per la tutela del consumatore e il quadro civile di Internet in relazione all'utilizzo del tracciamento per la pubblicità comportamentale online e alla vendita di dati di navigazione ([228]).

(142) Da quanto precede risulta che il sistema brasiliano garantisce nella pratica un'applicazione efficace delle sue norme in materia di protezione dei dati.

2.5.3. *Ricorso*

(143) Al fine di garantire una protezione adeguata e, in particolare, il rispetto dei diritti individuali, l'interessato dovrebbe avere a disposizione mezzi di ricorso efficaci in sede amministrativa e giudiziaria, compreso il risarcimento dei danni.

([220]) Registro delle sanzioni dell'ANPD, disponibile all'indirizzo: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/decisoes-em-processos-sancionadores-1/decisoes-em-processos-sancionadores?_authenticator=7951f0a70d3d125fd05e11a1e544b72d2c61f304.

([221]) Cfr., ad esempio, la nota tecnica n. 175/2023 sul progetto di accordo di cooperazione tra il ministero della Giustizia e della pubblica sicurezza e la Federazione brasiliana di calcio per la condivisione di dati personali al fine di migliorare il progetto «stadi sicuri», disponibile all'indirizzo: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/nota-tecnica-no-175-2023-cgf-anpd-acordo-de-cooperacao-mjsp-e-cbf.pdf.

([222]) Misura preventiva dell'ANPD, votazione n. 11/2024, disponibile all'indirizzo: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-cautelar-do-tratamento-de-dados-pessoais-para-treinamento-da-ia-da-meta/SEI_0130047_Voto_11.pdf.

([223]) L'importo di 50 000 R$ equivale a 7 800 EUR.

([224]) L'elenco completo e aggiornato delle indagini e dei casi in corso avviati dall'ANPD è disponibile al seguente indirizzo: https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/processos-de-fiscalizacao.

([225]) Legge n. 8.079 dell'11 settembre 1990 – legge sulla tutela del consumatore, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm.

([226]) Legge n. 12.965 del 23 aprile 2014, Marco Civil da Internet («quadro civile di Internet»), disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

([227]) Articolo 6 della legge n. 8.079 dell'11 settembre 1990 – legge sulla tutela del consumatore.

([228]) L'importo di 3,50 milioni di R$ era pari a circa 1,5 milioni di EUR al tasso di cambio vigente all'epoca.

(144) Il sistema brasiliano offre alle persone fisiche diversi meccanismi per far valere efficacemente i loro diritti e ottenere un ricorso.

(145) Innanzitutto le persone fisiche che ritengono che i loro diritti o i loro interessi in materia di protezione dei dati siano stati violati o che intendono esercitare i propri diritti alla protezione dei dati possono rivolgersi al titolare del trattamento pertinente. Ai sensi dell'articolo 9 della LGPD, il titolare del trattamento deve fornire, tra l'altro, i dati di contatto per consentire agli interessati di presentare le loro richieste e domande ([229]).

(146) Inoltre, ai sensi della LGPD e dell'ordinamento giuridico brasiliano, le persone fisiche che ritengono che i loro diritti o interessi in materia di protezione dei dati siano stati violati dal titolare del trattamento o dal responsabile del trattamento dei dati personali hanno a disposizione diverse vie di ricorso.

(147) In primo luogo, chiunque ritenga che i suoi diritti o interessi in materia di protezione dei dati siano stati violati dal titolare del trattamento o dal responsabile del trattamento può presentare un reclamo o segnalare tale violazione all'ANPD ([230]). L'ANPD dispone di una pagina apposita sul suo sito web per consentire agli interessati di presentare un reclamo in caso di violazione della LGPD o una petizione in caso di questioni connesse a una richiesta rivolta a un titolare del trattamento in merito ai loro diritti in materia di protezione dei dati ([231]). Come spiegato nel considerando 138 della presente decisione, l'ANPD può imporre una sanzione in risposta a un reclamo, secondo quanto specificato all'articolo 52 della LGPD. Il regolamento sui poteri sanzionatori dell'ANPD ha istituito la procedura amministrativa per i suoi procedimenti, compresi i termini, le procedure che disciplinano il diritto di essere ascoltati e la pubblicazione della decisione ([232]).

(148) Le decisioni dell'ANPD possono essere impugnate dagli interessati presentando ricorso al consiglio di amministrazione dell'ANPD entro 10 giorni dal ricevimento della decisione pertinente ([233]). In virtù del loro diritto a un ricorso effettivo, le persone fisiche possono anche 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 (compreso il rifiuto di trattare un reclamo o il rigetto nel merito di un reclamo) ([234]).

(149) In secondo luogo, l'ANPD può incoraggiare la «conciliazione diretta» (mediazione) tra gli interessati e i titolari del trattamento, al fine di dare priorità alla risoluzione del problema e al risarcimento dei danni da parte del titolare del trattamento ([235]). Queste procedure non impediscono agli interessati di presentare un reclamo o di accedere ad altre vie di ricorso.

(150) In terzo luogo, per quanto riguarda il risarcimento dei danni, l'articolo 42 della LGPD stabilisce l'obbligo per il titolare del trattamento o il responsabile del trattamento di porre rimedio ai danni materiali, morali, individuali o collettivi causati ad altri dal trattamento di dati personali. Gli interessati possono intentare un'azione legale, a livello individuale o collettivo, per chiedere il risarcimento di tali danni ([236]). La LGPD stabilisce che un giudice può invertire l'onere della prova a favore dell'interessato, in particolare nei casi in cui la produzione di elementi di prova da parte dell'interessato sarebbe eccessivamente gravosa ([237]).

(151) In quarto luogo, quando una violazione dei diritti degli interessati rientra nell'ambito di applicazione del diritto inteso alla tutela del consumatore e dei rapporti con il consumatore, la protezione garantita in questo settore è applicabile e può essere invocata in giudizio ([238]).

([229]) Articolo 9, in combinato disposto con l'articolo 55-J, punto V, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([230]) Articolo 55-J, punto V, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([231]) Cfr. ANPD, Servizi per gli interessati, deposito di un reclamo o di una petizione, disponibile all'indirizzo: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/denuncia-peticao-de-titular.

([232]) Sezioni II e III del regolamento dell'ANPD sui poteri sanzionatori dell'ANPD, ottobre 2021.

([233]) Articolo 59 del regolamento dell'ANPD sui poteri sanzionatori dell'ANPD, ottobre 2021.

([234]) Articolo 22 della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([235]) Articolo 17, punto VIII, del regolamento dell'ANPD sui poteri sanzionatori dell'ANPD, ottobre 2021.

([236]) Articolo 42, paragrafo 3, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([237]) Articolo 42, paragrafo 2, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([238]) Articolo 45 della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

(152) In quinto luogo, la Corte suprema federale brasiliana ha riconosciuto che le persone fisiche hanno il diritto di richiedere un provvedimento ingiuntivo in caso di violazioni dei loro diritti ai sensi della costituzione, compreso il diritto alla protezione dei dati personali ([239]). In tale contesto un organo giurisdizionale può ad esempio ordinare ai titolari del trattamento di sospendere o interrompere qualsiasi attività illecita. Inoltre è possibile chiedere l'esecuzione di diritti di protezione dei dati, compresi quelli protetti dalla LGPD, tramite azioni civili. L'articolo 22 della LGPD prevede esplicitamente che la difesa dei diritti degli interessati possa essere esercitata dinanzi a un organo giurisdizionale e, più in generale, che le persone fisiche possano promuovere ricorsi in materia di protezione dei dati a livello individuale o collettivo.

(153) L'ordinamento brasiliano offre pertanto varie possibilità di ricorso, che spaziano da opzioni facilmente accessibili e a basso costo (ad esempio, la presentazione di reclami all'ANPD) a vie giudiziarie, tra cui la possibilità di ottenere un risarcimento dei danni o di chiedere un ricorso collettivo.

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

(154) La Commissione ha valutato altresì le limitazioni e le garanzie, compresi i meccanismi di vigilanza e di ricorso individuale disponibili nella normativa brasiliana per quanto riguarda la raccolta e il successivo utilizzo da parte di autorità pubbliche brasiliane dei dati personali trasferiti verso titolari del trattamento e responsabili del trattamento in Brasile per motivi di interesse pubblico, in particolare per finalità di contrasto penale e di sicurezza nazionale («accesso da parte di pubbliche amministrazioni»).

(155) Nel valutare se le condizioni in base alle quali l'accesso da parte delle pubbliche amministrazioni ai dati trasferiti verso il Brasile ai sensi della presente decisione soddisfino la verifica dell'«equivalenza sostanziale» ai sensi dell'articolo 45, paragrafo 1, del regolamento (UE) 2016/679, come interpretato dalla Corte di giustizia dell'Unione europea alla luce della Carta dei diritti fondamentali, la Commissione ha tenuto conto in particolare dei criteri illustrati in appresso.

(156) Innanzitutto qualsiasi limitazione nell'esercizio del diritto alla protezione dei dati personali deve essere prevista dalla legge e implica che la base giuridica che consente l'ingerenza in tali diritti deve definire essa stessa la portata della limitazione dell'esercizio del diritto considerato. ([240]).

(157) In secondo luogo, per soddisfare il requisito di proporzionalità secondo cui le deroghe e le limitazioni alla protezione dei dati personali devono operare nei limiti dello stretto necessario in una società democratica per soddisfare gli obbiettivi specifici di interesse generale equivalenti a quelli riconosciuti dall'Unione, la legislazione del paese terzo in questione che consente tale ingerenza deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura in questione e impongano requisiti minimi in modo che le persone i cui dati sono trasferiti dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati personali contro il rischio di abusi ([241]). In particolare, essa deve indicare in quali circostanze e a quali condizioni possa essere adottata una misura che prevede il trattamento di siffatti dati ([242]) nonché assoggettare il soddisfacimento di tali requisiti alla vigilanza indipendente ([243]).

([239]) Nel 2020 la Corte suprema federale brasiliana ha emesso una sentenza di sospensione di un'ordinanza presidenziale esecutiva che avrebbe costretto le società di telecomunicazioni a condividere i dati degli abbonati con l'agenzia di censimento, riconoscendo per la prima volta la protezione dei dati come diritto fondamentale e aprendo così la strada all'inclusione del diritto nella costituzione brasiliana. Cfr. Corte suprema federale, decisione sul ricorso diretto di incostituzionalità n. 6387 del 7 maggio 2020. Disponibile all'indirizzo: https://www.stf.jus.br/arquivo/cms/noticianoticiastf/anexo/adi6387mc.pdf.

([240]) Cfr. Schrems II, punti 174 e 175, e la giurisprudenza citata. Cfr. anche, per quanto riguarda l'accesso da parte di autorità pubbliche di Stati membri, la causa C-623/17 «Privacy International», ECLI:EU:C:2020:790, punto 65; e le cause riunite C-511/18, C-512/18 e C-520/18 «La Quadrature du Net and Others», ECLI:EU:C:2020:791, punto 175.

([241]) Cfr. Schrems II, punti 176 e 181, e la giurisprudenza citata. Cfr. anche, per quanto riguarda l'accesso da parte di autorità pubbliche di Stati membri, Privacy International, punto 68; e La Quadrature du Net and Others, punto 132.

([242]) Schrems II, punto 176. Cfr. anche, per quanto riguarda l'accesso da parte di autorità pubbliche di Stati membri, Privacy International, punto 68; e La Quadrature du Net and Others, punto 132.

([243]) Schrems II, punto 179.

(158) In terzo luogo tale legislazione e i suoi requisiti devono essere legalmente vincolanti ai sensi del diritto interno. Ciò riguarda innanzitutto tutte le autorità del paese terzo in questione, ma tali requisiti giuridici devono altresì poter essere fatti valere dinanzi agli organi giurisdizionali nei confronti di tali autorità ([244]). In particolare gli interessati devono disporre della possibilità di esperire mezzi di ricorso dinanzi a un giudice indipendente e imparziale al fine di avere accesso a dati personali che li riguardano, o di ottenere la rettifica o la soppressione di tali dati. ([245]).

3.1. **Quadro giuridico generale**

(159) Le limitazioni e le garanzie che si applicano alla raccolta e all'uso successivo dei dati personali da parte delle autorità pubbliche brasiliane derivano dal quadro costituzionale globale, da leggi specifiche che disciplinano le loro attività nei settori del contrasto penale e della sicurezza nazionale, nonché dalle norme che si applicano specificamente al trattamento dei dati personali.

(160) Innanzitutto l'accesso ai dati personali da parte delle autorità pubbliche brasiliane è disciplinato dal principio generale di legalità sancito dalla costituzione brasiliana, da cui discendono i principi di ragionevolezza, necessità e proporzionalità ([246]). In particolare, a norma dell'articolo 5 della costituzione, i diritti e le libertà fondamentali (compreso il diritto alla vita privata e alla protezione dei dati) possono essere limitati soltanto dalla legge e solo se necessario per motivi imperativi di sicurezza nazionale, pubblica sicurezza o altre finalità specifiche di interesse pubblico dettate dalla legge. Tali limitazioni devono essere ragionevoli e proporzionate ([247]). In particolare, la valutazione del motivo di interesse pubblico è essenziale per determinare la proporzionalità dell'ingerenza, alla luce del principio di legalità. L'articolo 5, punto LIV, della costituzione stabilisce inoltre che nessuno può essere privato della sua libertà o dei suoi beni senza un giusto processo.

(161) In secondo luogo, l'ordinamento brasiliano garantisce l'*habeas data* come mezzo di ricorso costituzionale a tutela del diritto di accesso, rettifica e cancellazione dei dati personali detenuti dalle autorità pubbliche o in serie di dati o registri pubblici ([248]). Questo principio funge da garanzia contro l'uso improprio o la violazione della vita privata in relazione al trattamento dei dati da parte degli enti pubblici. Chiunque può presentare una domanda o una richiesta sulla base dell'*habeas data*, indipendentemente dalla propria cittadinanza ([249]).

(162) In terzo luogo, i principi e i diritti generali di cui ai considerando da 155 a 158 sono tenuti in considerazione anche nelle normative specifiche che disciplinano i poteri delle autorità di contrasto e di sicurezza nazionale. Ad esempio, il quadro civile di Internet prevede misure che richiedono un provvedimento giudiziario preventivo per l'accesso ai dati nonché limitazioni all'accesso ai dati online ([250]). Analogamente, la legge sulle intercettazioni telefoniche stabilisce misure e garanzie specifiche per il trattamento dei dati relativi alle telecomunicazioni ([251]). Nel settore della sicurezza nazionale, la legge che istituisce il sistema di intelligence brasiliano prevede misure per l'accesso legittimo ai dati a fini di sicurezza nazionale ([252]).

([244]) Cfr. Schrems II, punti 181 e 182.

([245]) Cfr. Schrems I, punto 95 e Schrems II, punto 194. A tale riguardo la Corte di giustizia dell'Unione europea ha sottolineato in particolare che il rispetto dell'articolo 47 della Carta dei diritti fondamentali, garantendo il diritto a un ricorso effettivo dinanzi un organo giurisdizionale indipendente e imparziale, «è anch'esso parte del livello di protezione richiesto all'interno dell'Unione e […] deve essere constatato dalla Commissione prima di adottare una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 1, del [regolamento (UE) 2016/679]» (Schrems II, punto 186).

([246]) Articolo 5, punto II, della costituzione della Repubblica federativa del Brasile del 1988.

([247]) Il Brasile è soggetto alla giurisdizione della Corte interamericana dei diritti umani che, tra l'altro, ha riconosciuto il principio di proporzionalità come «essenziale in una società democratica» e che le limitazioni ai diritti fondamentali sono legittime solo se mirano a conseguire un obiettivo pubblico imperativo. Cfr., ad esempio, MENDES, Gilmar Ferreira. *Fundamental rights and judicial control*. San Paolo: Saraiva, 2012, pag. 78.

([248]) Articolo 5, punti LXXII e LXXVII, della costituzione della Repubblica federativa del Brasile del 1988.

([249]) Cfr. anche i considerando 9 e 11 della presente decisione.

([250]) Legge n. 12.965 del 23 aprile 2014, Marco Civil da Internet («quadro civile di Internet»), disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

([251]) Legge n. 9.296 del 24 luglio 1996 – legge sulle intercettazioni telefoniche, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm.

([252]) Legge n. 9.883 del 7 dicembre 1999 – legge che istituisce il sistema di intelligence brasiliano.

(163) In quarto luogo, il trattamento dei dati personali da parte delle autorità pubbliche, anche per finalità di contrasto e di sicurezza nazionale, è soggetto alle prescrizioni in materia di protezione dei dati di cui alla LGPD. Come descritto nel considerando 31 della presente decisione, l'esenzione relativa all'applicazione della LGPD nel settore della sicurezza pubblica, della difesa nazionale, della sicurezza dello Stato e dell'indagine e del perseguimento di reati prevista dalla LGPD è parziale. La Corte suprema federale ha interpretato l'applicabilità della LGPD alla luce della protezione costituzionale dei dati personali e stabilito che i principi, i diritti e gli obiettivi principali della LGPD si applicano a qualsiasi trattamento dei dati personali da parte di autorità pubbliche, anche quando è condotto a fini di contrasto in materia penale o di sicurezza nazionale ([253]). Su tale base, ad esempio, l'ANPD ha svolto indagini ed emanato orientamenti, tra cui una nota tecnica alle autorità pubbliche per le attività connesse alla pubblica sicurezza, in cui ha ricordato che il trattamento per tali finalità di interesse pubblico deve rispettare i principi e i diritti generali previsti dalla LGPD ([254]).

(164) Infine le persone fisiche possono invocare i loro diritti e le loro libertà costituzionali dinanzi alla Corte suprema federale se ritengono che siano stati violati dalle autorità pubbliche nell'esercizio delle loro funzioni. Le persone fisiche possono inoltre presentare ricorso, in relazione ai loro diritti in materia di protezione dei dati, dinanzi ad organi di vigilanza indipendenti (ad esempio l'ANPD) e ad organi giurisdizionali, come specificato nei considerando da 143 a 153 della presente decisione.

3.2. **Accesso e uso da parte delle autorità pubbliche brasiliane per motivi di contrasto penale**

(165) Il diritto brasiliano impone una serie di limitazioni in materia di accesso e uso di dati personali per finalità di contrasto penale e prevede meccanismi di vigilanza e ricorso che sono in linea con i requisiti di cui ai considerando da 155 a 158 della presente decisione. Le condizioni in cui tale accesso può avvenire e le garanzie applicabili all'uso di tali poteri sono valutate in dettaglio nelle sezioni che seguono.

3.2.1. *Base giuridica, limitazione e garanzie*

(166) L'accesso ai dati personali da parte delle autorità pubbliche per motivi di contrasto in materia penale avviene solitamente sulla base di un provvedimento giudiziario preventivo emesso da un'autorità giudiziaria competente ([255]). In deroga a tale regola, le autorità di polizia e le procure, nei casi specificamente previsti dalla legge, possono avere accesso ai dati delle persone indagate contenuti in un registro pubblico, vale a dire i dati relativi alla loro qualifica personale, all'affiliazione e all'indirizzo ([256]). L'elenco esaustivo dei registri accessibili, previsto dalla legge, comprende i dati di brasiliani o persone residenti in Brasile e non comprenderebbe l'accesso ai dati trasferiti dall'UE; di conseguenza non rientrerebbe nell'ambito di applicazione della presente decisione ([257]). L'accesso a questi registri è disciplinato dal principio costituzionale di legalità - da cui discendono i principi di ragionevolezza, necessità e proporzionalità - e può essere soggetto a controllo giurisdizionale ex post, come illustrato nei considerando da 159 a 161.

(167) Le autorità brasiliane che hanno il diritto di accedere ai dati personali e di raccogliere tali dati per motivi di contrasto penale mediante un provvedimento giudiziario preventivo sono: 1) la polizia civile; 2) la polizia federale; 3) la procura statale; 4) la procura federale; 5) i giudici e gli organi giurisdizionali; 6) le commissioni parlamentari d'inchiesta.

([253]) Corte suprema federale, decisione sul ricorso diretto di incostituzionalità n. 6649, settembre 2022, disponibile all'indirizzo: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([254]) Nota tecnica n. 175/2023, paragrafo 5.1.

([255]) Cfr., ad esempio, l'articolo 5, punto XII, della costituzione della Repubblica federativa del Brasile del 1988.

([256]) Articoli 15 e 16 della legge n. 12.850 del 2 agosto 2013 – legge sulle associazioni a delinquere e sulle indagini penali, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm.

([257]) I registri accessibili comprendono: registri per l'impiego, registri elettorali, registri telefonici, registri finanziari, registri di fornitori di servizi internet e registri di carte di credito. Le informazioni contenute in tali registro comprendono dati sulle persone abbonate ai servizi o che usano i servizi pubblici in questione. Articoli 15 e 16 della legge n. 12.850 del 2 agosto 2013 – legge sulle associazioni a delinquere e sulle indagini penali, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm.

(168) Ai sensi dell'articolo 3-B del codice penale, un giudice incaricato del controllo della legalità dell'indagine penale e della tutela dei diritti individuali può emettere un provvedimento giudiziario che autorizzi: 1) l'intercettazione telefonica di comunicazioni su computer e sistemi connessi o altre forme di comunicazione; 2) la rimozione dell'obbligo della riservatezza fiscale, bancaria, dei dati e telefonica; 3) la perquisizione e il sequestro presso un'abitazione; 4) l'accesso a informazioni riservate; 5) altre misure per ottenere elementi di prova che limitano i diritti fondamentali della persona indagata ([258]).

3.2.1.1. Intercettazione delle comunicazioni

(169) La riservatezza della corrispondenza delle comunicazioni elettroniche e telefoniche è considerata un diritto fondamentale nel quadro giuridico brasiliano ([259]).

(170) Le autorità pubbliche possono accedere a tali dati solo in casi eccezionali ai fini di indagini o azioni penali. L'intercettazione delle comunicazioni deve sempre essere una misura sussidiaria ed eccezionale, consentita solo in mancanza di altri mezzi per risolvere un caso specifico, come stabilito dalla Corte suprema federale ([260]). Le modalità di intercettazione delle comunicazioni online e telefoniche sono disciplinate dalla legge sulle intercettazioni telefoniche ([261]).

(171) L'articolo 2 della legge sulle intercettazioni telefoniche stabilisce condizioni rigorose per l'accesso alle comunicazioni. Qualsiasi intercettazione delle comunicazioni necessita di un'autorizzazione giudiziaria preventiva. Occorre che una valida richiesta di intercettazione sia presentata a un giudice da parte delle autorità pubbliche autorizzate, che possono essere 1) l'autorità di polizia competente, nell'ambito di indagini penali oppure 2) il rappresentante della procura, nell'ambito di indagini o azioni penali ([262]). L'intercettazione delle comunicazioni telefoniche non è autorizzata in nessuna delle seguenti circostanze, conformemente agli obblighi di necessità e proporzionalità: 1) se non vi sono prove ragionevoli della commissione di un reato o della partecipazione allo stesso; 2) se le prove possono essere fornite con altri mezzi disponibili; 3) se il fatto oggetto dell'indagine costituisce un reato punibile con la reclusione ([263]).

(172) Inoltre la legge sulle intercettazioni telefoniche prevede che la richiesta di intercettazione debba chiarire il carattere necessario della misura ([264]). L'autorizzazione giudiziaria preventiva deve essere motivata e deve valutare la proporzionalità dei mezzi utilizzati per condurre l'intercettazione ([265]). Il giudice può autorizzare l'accesso al contenuto delle comunicazioni per un periodo massimo di 15 giorni. Tale termine può essere prorogato con una nuova decisione giudiziaria se viene dimostrato il carattere indispensabile della misura ([266]). Qualsiasi intercettazione di comunicazioni, compreso il monitoraggio ambientale, effettuata in assenza di un'autorizzazione giudiziaria o per motivi non autorizzati dalla legge costituisce un reato punibile con la reclusione fino a quattro anni ([267]).

([258]) Decreto legge n. 3.689 del 3 ottobre 1941 – codice penale, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.
([259]) Articolo 5, punto XII, della costituzione della Repubblica federativa del Brasile del 1988.
([260]) Corte suprema federale, HC 108147/PR, 2012, disponibile all'indirizzo: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4067401.
([261]) Articolo 1 della legge n. 9.296 del 24 luglio 1996 – legge sulle intercettazioni telefoniche.
([262]) Articolo 2, punti I e II, della legge n. 9.296 del 24 luglio 1996 – legge sulle intercettazioni telefoniche.
([263]) Articolo 2 della legge n. 9.296 del 24 luglio 1996 – legge sulle intercettazioni telefoniche.
([264]) Articolo 4 della legge n. 9.296 del 24 luglio 1996 – legge sulle intercettazioni telefoniche.
([265]) Articolo 5 della legge n. 9.296 del 24 luglio 1996 – legge sulle intercettazioni telefoniche.
([266]) Articolo 5 della legge n. 9.296 del 24 luglio 1996 – legge sulle intercettazioni telefoniche.
([267]) Articolo 10 della legge n. 9.296 del 24 luglio 1996 – legge sulle intercettazioni telefoniche.

(173) Come regola generale, i dati consultati e raccolti per motivi di contrasto penale ai sensi della legge sulle intercettazioni telefoniche sono conservati per la durata del trattamento e successivamente cancellati quando non sono più necessari per il procedimento giudiziario, conformemente agli orientamenti vincolanti del sistema giudiziario ([268]). L'articolo 9 della legge sulle intercettazioni telefoniche stabilisce inoltre che, quando i contenuti raccolti non sono collegati alla questione oggetto dell'indagine, i dati sono resi «inutilizzabili» ([269]).

(174) Per quanto riguarda i metadati di comunicazione, l'articolo 17 della legge sulle associazioni a delinquere e sulle indagini penali impone alle compagnie telefoniche di conservare le informazioni degli utenti residenti in Brasile e le registrazioni di chiamate telefoniche (esclusivamente i numeri telefonici) per cinque anni ([270]). L'accesso a questo registro, conservato da ANATEL (agenzie di regolamentazione nel settore della telecomunicazione in Brasile) è limitato a specifici enti pubblici e richiede un'autorizzazione giudiziaria, come illustrato sopra.

(175) Per quanto riguarda le informazioni disponibili online, l'articolo 7 del quadro civile di Internet garantisce anche l'inviolabilità e la riservatezza del flusso di comunicazioni via Internet, salvo provvedimento giudiziario, conformemente alla legge, nonché l'inviolabilità e la riservatezza delle comunicazioni private salvate, salvo provvedimento giudiziario ([271]).

(176) Ai sensi dell'articolo 10 del quadro civile di Internet, l'accesso ai contenuti delle comunicazioni online e ai dati di connessione (compresi i metadati) può avvenire solo mediante un provvedimento giudiziario preventivo. A norma dell'articolo 22 del quadro civile di Internet, la richiesta di un provvedimento giudiziario deve comprendere: prove fondate del verificarsi del reato (punto I); una giustificazione motivata dell'utilità dei dati richiesti a fini di indagine o di prova (punto II); e il periodo cui si riferiscono i dati (punto III). L'articolo 13 impone inoltre ai fornitori di servizi Internet o di applicazioni di conservare i registri di connessione per un anno «in un ambiente controllato e sicuro» ([272]). Non è previsto un obbligo analogo di conservazione dei dati in relazione al contenuto delle comunicazioni online. L'accesso ai registri di connessione conservati può essere concesso a un'autorità competente solo sulla base di un'autorizzazione giudiziaria, alle condizioni descritte nel presente considerando ([273]).

(177) L'articolo 11 del quadro civile di Internet ricorda che qualsiasi operazione che comporti la raccolta, la conservazione o qualsiasi altro trattamento di registri, dati personali o comunicazioni da parte di fornitori di servizi di connessione e applicazioni Internet in Brasile deve rispettare la legislazione brasiliana e i diritti alla vita privata, alla protezione dei dati personali e alla riservatezza delle comunicazioni e dei registri privati. Dalle garanzie di cui ai considerando da 175 a 177 consegue che in Brasile generalmente non è autorizzata la raccolta e la conservazione massiccia dei dati di comunicazione.

3.2.1.2. Revoca dell'obbligo di tutela della riservatezza fiscale, bancaria, dei dati e delle comunicazioni

(178) In Brasile la riservatezza della corrispondenza delle comunicazioni elettroniche (compresi i dati elettronici) e delle comunicazioni telefoniche è oggetto di tutela costituzionale ([274]). La LGPD protegge inoltre l'uso dei dati e delle informazioni sulle comunicazioni ([275]), mentre la legge sulla riservatezza degli istituti finanziari tutela la riservatezza delle informazioni fiscali e bancarie ([276]).

([268]) Articolo 20 della risoluzione n. 324 del 20 giugno 2020, disponibile all'indirizzo: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/atos-do-poder-judiciario/resolucao-no-324-de-30-de-junho-de-2020.

([269]) Articolo 9 della legge n. 9.296 del 24 luglio 1996 – legge sulle intercettazioni telefoniche.

([270]) Articolo 17 della legge n. 12.850 del 2 agosto 2013 – legge sulle associazioni a delinquere e sulle indagini penali, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm.

([271]) Articolo 7 della legge n. 12.965 del 23 aprile 2014, Marco Civil da Internet («quadro civile di Internet»).

([272]) Articolo 13, frase introduttiva, della legge n. 12.965 del 23 aprile 2014, Marco Civil da Internet («quadro civile di Internet»).

([273]) Articolo 13, paragrafo 5, della legge n. 12.965 del 23 aprile 2014, Marco Civil da Internet («quadro civile di Internet»).

([274]) Articolo 5, punto XII, della costituzione della Repubblica federativa del Brasile del 1988.

([275]) Cfr. l'articolo 2 della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([276]) Legge complementare n. 105 del 10 gennaio 2001 – legge sulla riservatezza delle operazioni degli istituti finanziari, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm.

(179) Le autorità pubbliche possono accedere a tali informazioni solo in casi eccezionali a fini di indagini o azioni penali. L'intercettazione delle comunicazioni deve sempre essere una misura sussidiaria ed eccezionale, consentita solo in mancanza di altri mezzi per risolvere un caso specifico, come stabilito dalla Corte suprema federale ([277]).

(180) I criteri e le garanzie per l'accesso ai dati e alle comunicazioni sono stabiliti nell'ambito del quadro civile di Internet e della legge sulle intercettazioni telefoniche e sono specificati nei considerando da 169 a 177 della presente decisione.

(181) Per quanto riguarda i dati fiscali e bancari, l'articolo 1 della legge sulla riservatezza degli istituti finanziari stabilisce le condizioni per la revoca dell'obbligo generale di garanzia della riservatezza di tali informazioni. In primo luogo, l'obbligo di tutela della riservatezza può essere revocato solo mediante un'autorizzazione giudiziaria ([278]). In secondo luogo, le misure possono essere autorizzate solo per l'indagine o il perseguimento di reati seguenti: 1) terrorismo; 2) traffico illecito di sostanze stupefacenti o sostanze simili; 3) contrabbando o traffico di armi, munizioni o materiale destinato alla loro produzione; 4) estorsione mediante rapimento; 5) reati contro il sistema finanziario nazionale; 6) reati contro la pubblica amministrazione; 7) reati contro il sistema fiscale e la sicurezza sociale; 8) riciclaggio di denaro o occultamento di beni; 9) associazione con un'organizzazione criminale ([279]). L'articolo 10 della legge stabilisce inoltre che l'obbligo di tutela della riservatezza dei dati fiscali e bancari non può essere revocato per altri fini e che il mancato rispetto di tale limitazione costituisce un reato punibile con la reclusione fino a quattro anni ([280]).

3.2.1.3. Perquisizioni e sequestri

(182) La costituzione federale prevede di norma che le perquisizioni e i sequestri possano aver luogo solo in circostanze eccezionali rigorosamente definite o secondo quanto previsto dalla legge e sulla base di un provvedimento giudiziario emesso da un'autorità giudiziaria competente e nel rispetto del giusto processo ([281]). Le perquisizioni e i sequestri devono rispettare il principio di legalità ed essere effettuati nella misura necessaria.

(183) Le perquisizioni e i sequestri possono aver luogo senza un provvedimento giudiziario nelle circostanze eccezionali seguenti: 1) in caso di *flagrante delicto* (ossia se un reato è commesso in presenza di un'autorità di contrasto); 2) in caso di calamità naturali (al fine di salvare vite umane o beni); 3) per fornire assistenza a una persona che non è in grado di manifestare il proprio consenso e che necessita di aiuto ([282]). La giurisprudenza della Corte suprema federale del Brasile ha chiarito che le autorità di contrasto non possono basarsi su «denunce anonime» e «comportamenti sospetti» per effettuare perquisizioni o sequestri senza un mandato, in quanto ciò non è conforme all'obbligo della legalità e non fornisce alle autorità una valida giustificazione per infrangere l'inviolabilità del domicilio ([283]).

(184) In termini di garanzie procedurali, in linea con i principi costituzionali del Brasile, i dispositivi elettronici non possono essere soggetti ad alcuna perquisizione se non vi è il ragionevole sospetto che contengano dati o tracce pertinenti del reato e, di norma, se non è stato emesso un provvedimento giudiziario ([284]). Inoltre una persona fisica non può essere costretta a fornire dati se ciò può violare i suoi diritti costituzionali, come il diritto di non incriminarsi ([285]). Nel presentare una richiesta per un mandato di perquisizione all'organo giurisdizionale, l'autorità

([277]) Corte suprema federale, HC 108147/PR, 2012, disponibile all'indirizzo: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4067401.

([278]) Articolo 3-B del decreto legge n. 3.689 del 3 ottobre 1941 – codice penale, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.

([279]) Articolo 1, paragrafo 4, punti da I a IX, della legge complementare n. 105 del 10 gennaio 2001 – legge sulla riservatezza delle operazioni degli istituti finanziari, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm.

([280]) Articolo 10 della legge complementare n. 105 del 10 gennaio 2001 – legge sulla riservatezza delle operazioni degli istituti finanziari, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm.

([281]) Articolo 5, punto XI, della costituzione della Repubblica federativa del Brasile del 1988.

([282]) Articolo 5, punto XI, della costituzione della Repubblica federativa del Brasile del 1988.

([283]) Corte suprema federale, 2020, causa J.S. Ricorso straordinario n. 603616.

([284]) Articolo 5, punto XI, della costituzione della Repubblica federativa del Brasile del 1988.

([285]) Articolo 5, punto LXIII, della costituzione della Repubblica federativa del Brasile del 1988. Cfr. anche il decreto legge n. 2.848 del 7 dicembre 1940 – codice di procedura penale, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.

di contrasto penale deve fornire i fatti e le prove pertinenti a sostegno della necessità di accedere al sistema informatico e ai dati ivi contenuti, utilizzando credenziali di accesso acquisite legalmente ([286]). Se l'organo giurisdizionale concede il mandato di perquisizione, le autorità utilizzeranno le credenziali di accesso per accedere al sistema informatico e ai dati ivi contenuti, conformemente ai termini e alle condizioni specificati nel mandato. Una volta che la perquisizione o l'accesso sono stati portati a termine, le autorità competenti devono presentare all'organo giurisdizionale una relazione che descriva l'esito della perquisizione o dell'accesso e fornisca un elenco dei dati o delle informazioni ottenuti.

3.2.1.4. Accesso alle informazioni riservate

(185) L'articolo 4 della legge sull'accesso alle informazioni definisce le informazioni riservate come informazioni che sono temporaneamente soggette a limitazioni dell'accesso del pubblico a causa della loro natura essenziale per la sicurezza della società e dello Stato ([287]). I dati personali possono rientrare nell'ambito di applicazione delle informazioni riservate così definite.

(186) L'articolo 6 della legge sull'accesso alle informazioni impone agli enti pubblici di proteggere le informazioni riservate e di limitarne l'accesso. Per quanto riguarda l'accesso a informazioni su dati e comunicazioni, nonché a informazioni bancarie e fiscali, l'accesso alle informazioni riservate per le indagini e le azioni penali può avvenire solo sulla base di un'autorizzazione giudiziaria, in casi eccezionali, ed è consentito solo in mancanza di altri mezzi per risolvere un caso specifico, come stabilito dalla Corte suprema federale e dalla legge ([288]).

3.2.1.5. Altre misure per ottenere elementi di prova che limitano i diritti fondamentali della persona indagata

(187) Per «altre misure per ottenere elementi di prova che limitano i diritti fondamentali della persona indagata» s'intende, ad esempio, la possibilità di disporre la detenzione preventiva o di sottoporre una persona a sorveglianza fisica. In linea di principio, tali misure non sono pertinenti nel contesto del trasferimento di dati basato su una decisione di adeguatezza.

(188) Per completezza, tali misure, proposte da un'autorità pubblica, possono essere attuate solo sulla base di un'autorizzazione giudiziaria. Le misure proposte devono rispettare il principio di legalità sancito dalla costituzione, essere disposte in casi eccezionali e se altre alternative non sono possibili, come stabilito dalla Corte suprema federale.

3.2.2. *Ulteriore utilizzo delle informazioni*

(189) Per quanto riguarda l'ulteriore utilizzo di dati personali per un'altra finalità da parte di un'autorità pubblica, l'articolo 9 della legge sulle intercettazioni telefoniche stabilisce che, quando i contenuti raccolti non sono correlati alla questione oggetto di un'indagine specifica, i dati sono resi «inutilizzabili». L'articolo 13 del quadro civile di Internet limita inoltre la conservazione dei dati di connessione in un registro al periodo massimo di un anno. L'articolo 10 della legge sulla riservatezza degli istituti finanziari limita altresì la finalità per la quale l'obbligo di tutela della riservatezza dei dati fiscali e bancari può essere revocato ([289]). Queste misure riducono nella pratica la possibilità di un ulteriore utilizzo delle informazioni.

([286]) Articolo 240 del decreto legge n. 2.848 del 7 dicembre 1940 – codice di procedura penale.
([287]) Articolo 4, punto III, della legge n. 12.527 del 18 novembre 2011 – legge sull'accesso alle informazioni.
([288]) Corte suprema federale, HC 108147/PR, 2012, disponibile all'indirizzo: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4067401 e articolo 3-B del decreto legge n. 3.689 del 3 ottobre 1941 – codice penale, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.
([289]) Articolo 10 della legge complementare n. 105 del 10 gennaio 2001 – legge sulla riservatezza delle operazioni degli istituti finanziari, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm.

(190) Inoltre, cosa ancora più importante, la Corte suprema federale ha stabilito che la LGPD si applica alla condivisione di dati personali tra enti pubblici, anche quando sono condivisi tra autorità di contrasto e agenzie di intelligence ([290]). In particolare, la Corte ha ricordato che la condivisione di dati personali tra organismi ed enti della pubblica amministrazione 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. La Corte ha aggiunto che il trattamento di dati personali effettuato da enti pubblici in contrasto con i parametri giuridici e costituzionali fa sorgere la responsabilità civile dello Stato per i danni subiti dalle persone fisiche, conformemente all'articolo 42 della LGPD.

(191) Per quanto riguarda la condivisione di dati personali tra le autorità di contrasto in materia penale in Brasile e autorità analoghe di paesi terzi, tali attività sono disciplinate da strumenti di diritto internazionale, in linea con la LGPD. A tale riguardo, l'articolo 33, punto III, della LGPD 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. In Brasile, il ministero della Giustizia e della pubblica sicurezza funge da autorità centrale per la cooperazione giuridica internazionale in materia penale. Il ministero ha il compito di ricevere, analizzare, trasmettere e monitorare l'esecuzione delle richieste di cooperazione internazionale con le autorità straniere, nel rispetto delle norme di diritto internazionale applicabili e della LGPD. Il trattamento dei dati personali necessario per la cooperazione giuridica internazionale è soggetto ai principi della limitazione delle finalità (articolo 6, punto I, della LGPD), della liceità e della correttezza del trattamento (articoli 6 e 7 della LGPD), della minimizzazione e dell'esattezza dei dati (articolo 6, punti III e V, della LGPD), della trasparenza (articolo 6, punto VI, della LGPD), della sicurezza dei dati (articolo 6, punto VII, della LGPD) e della limitazione della conservazione (articolo 6, punti I, III e IV e articolo 16 della LGPD). La possibile divulgazione di dati personali a terzi (compresi paesi terzi) può avvenire soltanto nel rispetto di tali principi, dopo aver valutato il rispetto dei principi di necessità e proporzionalità e garantendo la continuità della protezione e il rispetto dei diritti degli interessati (articolo 2, del regolamento sui trasferimenti di dati).

(192) I poteri delle autorità di contrasto in materia penale in Brasile per quanto riguarda la raccolta di dati e l'accesso agli stessi sono pertanto circoscritti da norme chiare e precise previste dalla legge e sono soggetti a una serie di garanzie. Queste garanzie comprendono in particolare la garanzia di una vigilanza sull'esecuzione di tali misure, anche attraverso l'approvazione giudiziaria preventiva e la predisposizione di garanzie che limitano la durata dell'accesso e della conservazione delle informazioni in linea con i principi di necessità e proporzionalità.

3.2.3. *Vigilanza*

(193) In Brasile, le attività delle autorità di contrasto in materia penale sono soggette a vigilanza da parte di diversi organismi.

(194) In primo luogo, come confermato dalla Corte suprema federale, l'ANPD è autorizzata a vigilare sul trattamento dei dati personali effettuato dalle autorità di contrasto in materia penale in base a determinate prescrizioni previste dalla LGPD ([291]). In questo contesto, l'ANPD può esercitare i poteri correttivi e di indagine di cui dispone ai sensi della LGPD. Ad esempio, l'ANPD ha indagato sulle attività della polizia federale, del ministero della Giustizia e della pubblica sicurezza e su altri enti pubblici che svolgono attività di sicurezza a livello federale, statale o locale o che hanno competenze in materia di contrasto ([292]). L'ANPD può indagare di propria iniziativa o in seguito a richieste e reclami, che possono essere presentati, ad esempio, da singoli individui, organizzazioni della società civile e autorità pubbliche. Ad esempio, l'ANPD ha svolto diverse indagini sull'uso delle videocamere in seguito a richieste della società civile ([293]).

([290]) Corte suprema federale, decisione sul ricorso diretto di incostituzionalità n. 6649, settembre 2022, disponibile all'indirizzo: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([291]) Cfr. il considerando 163 della presente decisione e la decisione sul ricorso diretto di incostituzionalità n. 6649 del 15 settembre 2022 della Corte suprema federale, disponibile all'indirizzo: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([292]) Si vedano le ispezioni dell'ANPD, compresi i casi 00261.000836/2021-76 e 00261.001028/2021-26, disponibili all'indirizzo: https://www.gov.br/anpd/pt-br/assuntos/fiscalizacao-2/saiba-como_fisalizamos?_authenticator=b05dbbec15247ce4c8b7065d588ef945f6d4d340.

([293]) Si vedano le ispezioni dell'ANPD, caso 00261.002211/2022-20 sull'uso della telecamera di sicurezza da parte della città di Fortaleza. Le richieste all'ANPD sono disponibili al seguente indirizzo: https://www.gov.br/anpd/pt-br/assuntos/fiscalizacao-2/saiba-como_fisalizamos/arquivos-processos-de-fiscalizacao-concluidos/processosesec_pblico00261-002211_2022-20.pdf.

(195) In secondo luogo, le attività delle autorità di contrasto in materia penale sono soggette a vigilanza da parte del sistema giudiziario. Gli organi giurisdizionali hanno il potere di autorizzare la raccolta di dati personali e l'accesso agli stessi nelle circostanze di cui ai considerando da 165 a 187. Essi hanno inoltre il potere di irrogare sanzioni civili e penali, tra cui una pena detentiva o l'ordine di porre fine a determinate attività, in caso di abuso o mancato rispetto della legislazione in vigore.

(196) In terzo luogo la procura, un'istituzione indipendente e permanente in Brasile responsabile della difesa dell'ordinamento giuridico e del sistema democratico, ha il potere di esercitare un controllo esterno sulle attività di polizia ([294]). Come stabilito nella risoluzione relativa alla procura, il controllo esterno delle attività di polizia ha lo scopo di mantenere la regolarità e l'adeguatezza delle procedure impiegate nello svolgimento delle attività di polizia, con particolare riguardo al rispetto dei diritti fondamentali garantiti dalla costituzione e dalle leggi federali ([295]). In tale veste, la procura può, tra l'altro, effettuare visite in loco, anche non programmate, esaminare le indagini, vigilare sul sequestro di beni e monitorare il rispetto dei mandati ([296]). Qualsiasi violazione della legge è denunciata agli organi giurisdizionali. Nell'esercizio delle sue funzioni, la procura è stata coinvolta nell'indagine e nel perseguimento di casi di violenza, abuso di potere e violazioni dei diritti umani da parte della polizia. La procura vigila inoltre sulla protezione dei dati, avviando o aderendo ad azioni legali sulla base delle tutele costituzionali e promuovendo i diritti alla protezione dei dati insieme all'ANPD. Ad esempio, la procura ha presentato le sue argomentazioni alla Corte suprema federale che ha sostenuto una decisione storica che riconosce la protezione dei dati come diritto fondamentale in Brasile ([297]). Sulla pagina web della procura è disponibile un registro delle sue azioni riguardanti la LGPD ([298]).

3.2.4. *Ricorso*

(197) Il sistema brasiliano offre diversi mezzi giudiziari e amministrativi per ottenere ricorso, compreso il risarcimento dei danni. Tali meccanismi offrono agli interessati mezzi di ricorso effettivi in sede amministrativa e giudiziale che consentono loro in particolare di ottenere l'applicazione dei loro diritti, compreso il diritto di avere accesso ai propri dati personali o di ottenerne la rettifica o la cancellazione.

(198) In primo luogo, le persone fisiche possono presentare ricorso dinanzi agli organi giurisdizionali, anche per il risarcimento dei danni. La costituzione federale e il codice di procedura civile forniscono le basi giuridiche per chiedere il risarcimento dei danni immateriali o materiali causati da un'autorità pubblica che ha raccolto o utilizzato illecitamente dati a fini criminali ([299]). In particolare, la costituzione indica espressamente che il diritto alla vita privata implica un «diritto al risarcimento» del danno materiale o immateriale derivante dalla sua violazione ([300]). Le decisioni degli organi giurisdizionali sono impugnabili dinanzi alla Corte suprema federale e, in seguito, alla Corte interamericana dei diritti umani. Nel 2009 la Corte interamericana dei diritti umani ha ordinato al Brasile di risarcire i lavoratori delle cooperative agricole a causa di intercettazioni telefoniche improprie effettuate nello Stato di Paraná nel 1999 in violazione della legge sulle intercettazioni telefoniche e della Convenzione americana sui diritti umani ([301]).

([294]) Articolo 127 della costituzione della Repubblica federativa del Brasile del 1988.
([295]) Articolo 20 della risoluzione n. 20 del 28 maggio 2007 – controllo esterno delle attività di polizia, disponibile all'indirizzo: https://www.cnmp.mp.br/portal/images/Comissoes/CSP/Resolu%C3%A7%C3%B5es_/Resolu%C3%A7%C3%A3o_20.pdf.
([296]) Articolo 4 della risoluzione n. 20 del 28 maggio 2007 – controllo esterno delle attività di polizia.
([297]) Cfr. il considerando 199 della presente decisione e la decisione sul ricorso diretto di incostituzionalità n. 6.387 del maggio 2020 della Corte suprema federale, disponibile all'indirizzo: https://www.stf.jus.br/arquivo/cms/noticianoticiastf/anexo/adi6387mc.pdf.
([298]) Procura, «La LGPD presso la procura», disponibile all'indirizzo: https://www.mpf.mp.br/servicos/lgpd/lgpd-no-mpf.
([299]) Cfr., ad esempio, l'articolo 43 della legge n. 10.408 del 10 gennaio 2002 – codice di procedura civile, disponibile all'indirizzo: https://www.planalto.gov.br//ccivil_03/leis/2002/l10406compilada.htm.
([300]) Articolo 5, punto X, della costituzione della Repubblica federativa del Brasile del 1988.
([301]) Corte interamericana dei diritti dell'uomo, causa Escher et al. c. Brasile, eccezioni, argomenti nel merito, mezzi di ricorso e costi. Sentenza del 6 luglio 2009, disponibile all'indirizzo http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf.

(199) In secondo luogo le persone fisiche, indipendentemente dalla loro cittadinanza, possono avvalersi della tutela stabilita dalla nozione dell'*habeas data* per ottenere ulteriormente l'accesso e la rettifica dei loro dati detenuti dalle autorità pubbliche ([302]). Su tale base, le persone fisiche possono anche intentare causa dinanzi agli organi giurisdizionali, tra cui un «ricorso diretto di incostituzionalità» (Ação Direta de Inconstitucionalidade) presso la Corte suprema federale. La decisione storica della Corte suprema federale del 2020, che ha aperto la strada al riconoscimento della protezione dei dati da parte del Brasile come diritto fondamentale, ha avuto origine dai ricorsi diretti di incostituzionalità depositati sulla base del principio dell'*habeas data* ([303]). In questo caso era coinvolta anche la procura, che sosteneva la posizione delle persone fisiche e della società civile che aveva presentato la causa. Era stata contestata un'ordinanza esecutiva che prevedeva la condivisione dei dati personali di oltre 200 milioni di abbonati ai servizi di telecomunicazione con l'Istituto brasiliano di geografia e statistica durante la pandemia di COVID-19 ([304]). La Corte suprema federale ha ritenuto che l'ordinanza esecutiva violasse i diritti fondamentali alla vita privata e alla riservatezza delle comunicazioni tutelati dalla costituzione ([305]). L'ordinanza esecutiva è stata sospesa e la Corte ha stabilito che la protezione dei dati deve essere presa in considerazione e tutelata come un diritto fondamentale, analogamente al diritto alla vita privata ([306]). Al momento della decisione la LGPD non era ancora in vigore. Pertanto il collegio giudicante ha fatto riferimento al diritto comparato, in particolare alla giurisprudenza della Corte federale costituzionale tedesca e all'articolo 8 della Carta dei diritti fondamentali dell'Unione europea, per sostenere la propria interpretazione di incostituzionalità dell'ordinanza esecutiva, nonché alla propria interpretazione dei diritti fondamentali alla dignità e alla vita privata garantiti dalla costituzione e al riconoscimento dell'*habeas data* come strumento per tutelare il diritto all'autodeterminazione informativa ([307]).

(200) In terzo luogo, le persone fisiche possono presentare ricorso nei confronti dell'ANPD per violazioni della LGPD ai sensi dell'articolo 55-J, punto V, e alle condizioni specificate nei considerando 146 e 149 della presente decisione. Le persone fisiche possono inoltre esercitare nei confronti delle autorità pubbliche i loro diritti in materia di protezione dei dati sanciti dalla LGPD ([308]).

(201) I meccanismi di ricorso descritti nei considerando da 197 a 200 della presente decisione forniscono agli interessati mezzi di ricorso effettivi in sede amministrativa e giudiziale che consentono loro in particolare di far valere i loro diritti, compreso il diritto alla protezione di tali dati.

3.3. **Accesso e uso da parte delle autorità pubbliche brasiliane per finalità di sicurezza nazionale**

(202) Il diritto del Brasile contempla una serie di limitazioni e garanzie in relazione all'accesso e all'uso di dati personali per finalità di sicurezza nazionale e prevede meccanismi di vigilanza e ricorso in questo settore che sono in linea con i requisiti di cui ai considerando da (156) a (158) della presente decisione. Le condizioni in cui tale accesso può avvenire e le garanzie applicabili all'uso di tali poteri sono valutate in dettaglio nelle sezioni che seguono.

([302]) Cfr. i considerando 9 e 161 della presente decisione.

([303]) Corte suprema federale, decisione sul ricorso diretto di incostituzionalità n. 6.387, maggio 2020, disponibile all'indirizzo: https://www.stf.jus.br/arquivo/cms/noticianoticiastf/anexo/adi6387mc.pdf.

([304]) Ordinanza esecutiva n. 954 del 17 aprile 2020, sospesa, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm.

([305]) Corte suprema federale, decisione sul ricorso diretto di incostituzionalità n. 6.387, maggio 2020, pag. 12.

([306]) Corte suprema federale, decisione sul ricorso diretto di incostituzionalità n. 6.387, maggio 2020, pag. 8.

([307]) Cfr. Corte suprema federale, decisione sul ricorso diretto di incostituzionalità n. 6.387, maggio 2020, pag. 4 e International Bar Association, «The impact of COVID-19 for data protection in Brazil: the perspective of Brazil's supreme court», disponibile all'indirizzo: https://www.ibanet.org/article/82b25a81-7422-4f07-aaa8-9c2db19e22af#:~:text=On%206%20and%207%20May%202020%2C%20the,as%20an%20independent%20fundamental%20right%20in%20Brazil.&text=The%20processing%20of%20data%20is%20allowed%20only,legal%20principles%2C%20such%20as%20transparency%20and%20security.

([308]) Articolo 23 della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

3.3.1. *Basi giuridiche, limitazioni e garanzie*

(203) In Brasile i dati personali possono essere consultati a fini di sicurezza nazionale nell'ambito delle attività di intelligence sulla base della legge che istituisce il sistema di intelligence brasiliano (SISBIN) ([309]). L'articolo 1 di tale legge stabilisce in linea generale che il sistema di intelligence brasiliano deve rispettare e preservare i diritti e le garanzie individuali e le altre disposizioni della costituzione federale, dei trattati, delle convenzioni, degli accordi e degli impegni internazionali di cui la Repubblica federativa del Brasile è parte o firmataria ([310]). Ciò include la garanzia dei principi di necessità e proporzionalità nonché del diritto alla protezione dei dati ([311]). Le attività attribuite al sistema di intelligence brasiliano sono ulteriormente descritte in decreti vincolanti ([312]).

(204) Ai sensi dell'articolo 4 della legge che istituisce il sistema di intelligence brasiliano, i soggetti facenti parte del SISBIN possono ottenere e analizzare dati specifici a fini di sicurezza nazionale (*Segurança Pública*). Il concetto di sicurezza nazionale è disciplinato da una legge del 2021 che ha modificato il codice penale ([313]) e che ha revocato la legge brasiliana sulla sicurezza nazionale ([314]). La legge del 2021 ha stabilito un elenco esaustivo di «reati» contro la sicurezza nazionale che definisce tale nozione. Tali reati sono i 1) reati contro la «sovranità nazionale» (tra cui atti di guerra, invasione della contea, tentato sequestro di parte del territorio nazionale per formare un nuovo paese, condivisione di informazioni classificate con governi stranieri od organizzazioni criminali straniere che potrebbero mettere a rischio l'ordine costituzionale della sovranità nazionale, agevolazione o falsificazione dell'accesso ai sistemi di informazione da parte di persone non autorizzate) ([315]); 2) reati contro le «istituzioni democratiche» (tra cui il tentativo violento di porre fine allo Stato di diritto impedendo o limitando i poteri costituzionali e il colpo di Stato) ([316]); 3) reati contro il «funzionamento delle istituzioni democratiche durante il processo elettorale» (tra cui l'interruzione del processo elettorale e la limitazione o l'ostacolo dell'esercizio dei diritti politici mediante l'uso della violenza) ([317]); 4) reati contro il funzionamento dei servizi essenziali (tra cui il sabotaggio dei mezzi di comunicazione pubblica, delle strutture di difesa, con l'obiettivo di porre fine allo Stato di diritto) ([318]). L'articolo 359-T della legge chiarisce che l'esercizio della libertà di espressione, dei diritti e dei poteri costituzionali nonché lo svolgimento di attività giornalistiche, anche attraverso marce, incontri, scioperi, raduni o qualsiasi altra forma di manifestazione politica a fini sociali, non possono essere considerati reati ([319]). La politica di intelligence nazionale stabilisce una serie di obiettivi principali in materia di intelligence che le autorità devono prendere in considerazione, come la prevenzione del «sabotaggio» o dello «spionaggio» ([320]). In quanto «documento di orientamento di alto livello», la politica di intelligence nazionale non amplia tuttavia l'elenco dei reati connessi al concetto di sicurezza nazionale né ne modifica la definizione ([321]).

([309]) Legge n. 9.883 del 7 dicembre 1999 – legge che istituisce il sistema di intelligence brasiliano, disponibile all'indirizzo: https://www.gov.br/mj/pt-br/acesso-a-informacao/atuacao-internacional/legislacao-traduzida/lei-no-9-883-de-7-de-dezembro-de-1999_eng_rev-d.pdf.

([310]) Articolo 1, paragrafo 1, della legge n. 9.883 del 7 dicembre 1999 – legge che istituisce il sistema di intelligence brasiliano.

([311]) Cfr. il considerando 160 della presente decisione.

([312]) Decreto n. 8.793/2016, del 29 giugno 2016, sulla politica di intelligence nazionale, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8793.htm e decreto n. 4.376/2002, del 13 settembre 2002, sull'organizzazione e sul funzionamento del sistema di intelligence brasiliano, disponibile all'indirizzo: https://www.gov.br/mj/pt-br/acesso-a-informacao/atuacao-internacional/legislacao-traduzida/decreto-no-4-376-de-13-de-setembro-de-2002-seopi_eng_rev-d.pdf.

([313]) Legge n. 14.197 del 1º settembre 2021 – legge che modifica il codice penale e revoca la legge del 1983 sulla sicurezza nazionale, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14197.htm.

([314]) Legge n. 7.170 del 14 dicembre 1983, revocata – legge sulla sicurezza nazionale, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/LEIS/L7170.htm.

([315]) Capo I della legge n. 14.197 del 1º settembre 2021 – legge che modifica il codice penale e revoca la legge del 1983 sulla sicurezza nazionale.

([316]) Capo II della legge n. 14.197 del 1º settembre 2021 – legge che modifica il codice penale e revoca la legge del 1983 sulla sicurezza nazionale.

([317]) Capo III della legge n. 14.197 del 1º settembre 2021 – legge che modifica il codice penale e revoca la legge del 1983 sulla sicurezza nazionale.

([318]) Capo IV della legge n. 14.197 del 1º settembre 2021 – legge che modifica il codice penale e revoca la legge del 1983 sulla sicurezza nazionale.

([319]) Articolo 359-T della legge n. 14.197 del 1º settembre 2021 – legge che modifica il codice penale e revoca la legge del 1983 sulla sicurezza nazionale.

([320]) Articolo 3 del decreto n. 8.793/2016, del 29 giugno 2016, sulla politica di intelligence nazionale, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8793.htm.

([321]) Introduzione, primo paragrafo, del decreto n. 8.793/2016, del 29 giugno 2016, sulla politica di intelligence nazionale, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8793.htm.

(205) I dati che possono essere consultati e analizzati per prevenire i suddetti reati contro la sicurezza nazionale comprendono le informazioni cui le autorità pubbliche che fanno parte del SISBIN hanno accesso nell'ambito delle loro operazioni, conformemente alle condizioni descritte nei considerando da 165 a 187 della presente decisione (ossia sulla base di un'autorizzazione giudiziaria rilasciata per una finalità chiaramente definita). I dati condivisi con il SISBIN sono trattati con un sistema elettronico sicuro criptato, con registri di accesso affinché le informazioni siano tracciabili e verificabili ([322]). Come chiarito dalla Corte suprema federale, la condivisione dei dati con il SISBIN è soggetta ai principi della LGPD, compresi la limitazione delle finalità (articolo 6, punto I, della LGPD), della minimizzazione e dell'esattezza dei dati (articolo 6, punti III e V, della LGPD), della trasparenza (articolo 6, punto VI, della LGPD), della sicurezza dei dati (articolo 6, punto VII, della LGPD) e della limitazione della conservazione (articolo 6, punti I, III e IV e articolo 16 della LGPD) ([323]).

(206) L'articolo 2 della legge che istituisce il sistema di intelligence brasiliano indica che possono aderire a tale sistema solo le autorità pubbliche. Il SISBIN è composto dall'Agenzia brasiliana di intelligence (ABIN) e da rappresentanti di centri di intelligence, ministeri, segretariati e agenzie della pubblica amministrazione federale. L'elenco delle autorità aderenti al SISBIN è contenuto in un decreto sull'organizzazione e il funzionamento del sistema ([324]).

(207) L'ABIN è l'organo centrale del sistema di intelligence ed è responsabile della pianificazione, dell'esecuzione, del coordinamento, della vigilanza e della supervisione delle attività di intelligence. Tali attività devono essere svolte utilizzando mezzi e tecniche riservati basati sulle informazioni. Per svolgere i propri compiti, l'ABIN riceve informazioni e dati specifici dalle diverse autorità pubbliche che fanno parte del SISBIN in relazione alla sicurezza nazionale. Le autorità che fanno parte del SISBIN sono tenute a fornire tali informazioni ([325]), in quanto la legge non autorizza l'ABIN a raccogliere informazioni in modo autonomo. La legittimità dell'obbligo di condivisione dei dati da parte dei membri del SISBIN è stata messa in discussione dinanzi alla Corte suprema federale ([326]). Nella sua sentenza del 2021, la Corte suprema federale ha chiarito che i dati condivisi dalle autorità pubbliche con l'ABIN devono rispettare rigorose finalità di interesse pubblico (ad esempio, la difesa delle istituzioni pubbliche e dell'interesse nazionale) e ha ricordato che la finalità specifica e legittima di ciascuna attività di condivisione dei dati è determinata mediante una procedura formale soggetta ad autorizzazione giudiziaria e definita in essa ([327]). Tali limitazioni si applicano anche a qualsiasi ulteriore condivisione dei dati tra autorità pubbliche ([328]).

(208) Infine il trattamento dei dati effettuato tramite il SISBIN deve proteggere le informazioni dall'accesso di persone o organismi non autorizzati. L'articolo 5 del decreto sul funzionamento del SISBIN prevede esplicitamente che il coordinamento e la condivisione dei dati tra le autorità aderenti al sistema devono rispettare la legislazione in materia di segreto professionale e sicurezza, protezione dei dati personali e sicurezza delle informazioni e delle

([322]) Cfr., ad esempio, l'opuscolo del SISBIN, pag. 18, disponibile all'indirizzo: https://www.gov.br/abin/pt-br/institucional/sisbin/cart_ingles.pdf.

([323]) Corte suprema federale, decisione sul ricorso diretto di incostituzionalità n. 6649, settembre 2022, disponibile all'indirizzo: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([324]) Articolo 7 del decreto n. 11.693, del 6 settembre 2023, sull'organizzazione e sul funzionamento del SISBIN, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11693.htm. Tra le autorità aderenti al SISBIN figurano ad esempio: il centro di intelligence del ministero della Difesa, la direzione per l'intelligence penitenziaria del segretariato nazionale del ministero della Giustizia e della pubblica sicurezza, il segretariato generale per le relazioni esterne del ministero degli Affari esteri e la direzione dell'intelligence della polizia federale.

([325]) Articolo 4 della legge n. 9.883 del 7 dicembre 1999 – legge che istituisce il sistema di intelligence brasiliano, disponibile all'indirizzo: https://www.gov.br/mj/pt-br/acesso-a-informacao/atuacao-internacional/legislacao-traduzida/lei-no-9-883-de-7-de-dezembro-de-1999_eng_rev-d.pdf.

([326]) Corte suprema federale, decisione sul ricorso diretto di incostituzionalità n. 6529 del 15 ottobre 2021, disponibile all'indirizzo: https://www.jusbrasil.com.br/jurisprudencia/stf/1303041724/inteiro-teor-1303041733.

([327]) Corte suprema federale, decisione sul ricorso diretto di incostituzionalità n. 6529, del 15 ottobre 2021, pag. 22.

([328]) Corte suprema federale, decisione sul ricorso diretto di incostituzionalità n. 6529, del 15 ottobre 2021, pag. 3.

conoscenze, che include la LGPD quale principale legge brasiliana in materia di protezione dei dati personali ([329]). L'articolo 6 del decreto precisa altresì che le informazioni scambiate dalle autorità aderenti al SISBIN devono rispettare il principio della certezza del diritto, della necessità e dell'interesse pubblico e avere una finalità legittima ([330]). Il SISBIN riconosce inoltre l'importanza di rispettare la LGPD nei documenti pubblicati e nelle procedure interne ([331]).

(209) I poteri delle autorità che trattano dati a fini di sicurezza nazionale in Brasile sono pertanto circoscritti da norme chiare e precise previste dalla legge e sono soggetti a una serie di garanzie. Queste garanzie comprendono in particolare la vigilanza garantita sull'esecuzione di tali misure, anche attraverso l'approvazione giudiziaria preventiva e la predisposizione di garanzie che limitano l'accesso alle informazioni in linea con i principi di necessità e proporzionalità.

3.3.2. *Ulteriore utilizzo delle informazioni*

(210) Il trattamento dei dati personali raccolti dalle autorità brasiliane a fini di sicurezza nazionale è soggetto ai principi della limitazione delle finalità (articolo 6, punto I, della LGPD), della liceità e della correttezza del trattamento (articoli 6 e 7 della LGPD), della minimizzazione e dell'esattezza dei dati (articolo 6, punti III e V, della LGPD), della trasparenza (articolo 6, punto VI, della LGPD), della sicurezza dei dati (articolo 6, punto VII, della LGPD) e della limitazione della conservazione (articolo 6, punti I, III e IV e articolo 16 della LGPD).

(211) La possibile divulgazione di dati personali a terzi (compresi paesi terzi e tramite accordi internazionali) può avvenire soltanto nel rispetto dei principi della LGPD, dopo aver valutato il rispetto dei principi di necessità e proporzionalità e garantendo la continuità della protezione e il rispetto dei diritti degli interessati (articolo 2, del regolamento sui trasferimenti di dati).

3.3.3. *Vigilanza*

(212) Le attività delle autorità di sicurezza nazionale brasiliane sono soggette a vigilanza da parte di organismi diversi. Il decreto sulla strategia di intelligence nazionale del Brasile rileva l'importanza di disporre di vari livelli di meccanismi di vigilanza per proteggere lo «Stato di diritto democratico» ([332]). La Corte suprema federale ha ricordato l'importanza di tale vigilanza in una causa relativa al trattamento dei dati nell'ambito del SISBIN, affermando che l'efficacia delle attività di intelligence è spesso legata alla segretezza del processo e delle informazioni raccolte. Nello Stato di diritto democratico, tale funzione è soggetta al controllo esterno del potere legislativo e del potere giudiziario al fine di valutare se la segretezza imposta sia adeguata ai rigorosi obiettivi pubblici cui è rivolta ([333]).

(213) In primo luogo, è previsto un controllo da parte dell'organo esecutivo, che garantisce che gli obiettivi conseguiti dal sistema di intelligence nonché le politiche da attuare e i piani formulati rispondano adeguatamente alle esigenze della società. L'organo esecutivo è inoltre responsabile di garantire che la spesa dei servizi di intelligence sia effettuata in modo razionale ed esclusivamente per azioni legittime, necessarie e utili per lo Stato. Nel quadro brasiliano, tale controllo è esercitato dalla Camera delle relazioni esterne e della difesa nazionale del Consiglio del governo, responsabile della vigilanza dell'attuazione delle attività condotte dalla polizia nazionale di intelligence, e dall'Ufficio per la sicurezza istituzionale, responsabile del coordinamento dell'attività di intelligence federale ([334]).

([329]) Articolo 5 del decreto n. 11.693, del 6 settembre 2023, sull'organizzazione e sul funzionamento del SISBIN.

([330]) Articolo 6 del decreto n. 11.693, del 6 settembre 2023, sull'organizzazione e sul funzionamento del SISBIN.

([331]) Cfr., ad esempio, l'opuscolo del SISBIN, pag. 9, in cui si menziona che uno degli obiettivi di questo riposizionamento è quello di aumentare i livelli di tracciabilità e trasparenza dei processi interni del SISBIN attraverso l'adozione di strumenti e piattaforme digitali appositamente pensati a tal fine. Tali strumenti devono essere allineati al quadro giuridico istituito dalla legge sull'accesso alle informazioni e dalla legge generale sulla protezione dei dati (LGPD), entrambe adottate nel 2012. Disponibile all'indirizzo: https://www.gov.br/abin/pt-br/institucional/sisbin/cart_ingles.pdf.

([332]) Sezione 2.4, quarto comma, del decreto del 15 dicembre 2017 su una strategia nazionale in materia di intelligence.

([333]) Corte suprema federale, decisione del 15 ottobre 2021, pag. 2.

([334]) Sezione 2.4 del decreto, del 15 dicembre 2017, su una strategia nazionale in materia di intelligence. disponibile all'indirizzo: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/dsn/Dsn14503.htm.

(214) In secondo luogo, l'organo legislativo esercita un controllo sulle attività di intelligence. Tale controllo ha lo scopo di verificare sia la legittimità che l'efficacia dell'attività di intelligence. I capi dei partiti di maggioranza e di minoranza della Camera dei deputati e del Senato federale, nonché i presidenti delle commissioni per le relazioni esterne e la difesa nazionale della Camera dei deputati e del Senato federale, fanno parte dell'organo esterno di vigilanza delle attività di intelligence denominato Comissão mista de Controle da Atividade de Inteligência (CCAI) ([335]). Il controllo esercitato dall'organo legislativo sulle attività di intelligence è stato stabilito dalla legge che ha istituito il sistema di intelligence brasiliano nel 1999, mentre il ruolo e i poteri di controllo della CCAI sono stati notevolmente rafforzati da una risoluzione vincolante adottata dal Congresso del 2013 ([336]). La risoluzione ha affrontato le carenze precedentemente individuate al fine di istituzionalizzare ulteriormente la CCAI, dotandola di una struttura e di un segretariato permanenti, chiarendone i poteri e aumentando la trasparenza delle sue attività. Il ruolo, le attività e i poteri della CCAI sono specificati in tale risoluzione e dalla legge. La CCAI monitora e controlla le attività di intelligence condotte dagli organi della pubblica amministrazione federale, in particolare quelli facenti parte del SISBIN, per garantire che tali attività siano svolte nel rispetto della costituzione e per tutelare i diritti e le garanzie delle persone fisiche, della società e dello Stato ([337]). La CCAI può effettuare un riesame a posteriori, ma anche audit e controlli di operazioni in corso ([338]). I membri di tale organo dispongono della massima libertà di accesso ai documenti. La CCAI redige relazioni annuali sulle sue attività, senza includere informazioni che possano pregiudicare la sicurezza nazionale ([339]). Come specificato nel considerando 222 della presente decisione, la CCAI può anche ricevere ed esaminare i reclami di singole persone fisiche.

(215) In terzo luogo, l'ANPD vigila sulla conformità, da parte delle autorità di sicurezza nazionali, del trattamento dei dati personali, nel rispetto dei parametri definiti dalla LGPD. La LGPD si applica in parte al trattamento di dati personali effettuato a fini di pubblica sicurezza, difesa nazionale, sicurezza dello Stato o indagine e perseguimento di reati ([340]). In questo contesto, l'ANPD può esercitare i poteri correttivi e di indagine di cui dispone ai sensi della LGPD. Ad esempio, l'ANPD può effettuare in qualsiasi momento audit di tutte le autorità pubbliche, compresa l'agenzia di intelligence ([341]).

(216) Infine il sistema giudiziario si occupa delle azioni legali intentate dai cittadini contro le autorità pubbliche e, in tale contesto, può supervisionare le attività svolte a fini di sicurezza nazionale per garantire il rispetto di tutti i diritti costituzionali e del quadro legislativo pertinente, compresa la LGPD. Le decisioni degli organi giurisdizionali sono impugnabili dinanzi alla Corte suprema federale e, in seguito, alla Corte interamericana dei diritti umani.

3.3.4. *Ricorso*

(217) Il sistema brasiliano offre diversi mezzi giudiziari e amministrativi per ottenere ricorso, compreso il risarcimento dei danni. Tali meccanismi offrono agli interessati mezzi di ricorso effettivi in sede amministrativa e giudiziale che consentono loro in particolare di ottenere l'applicazione dei loro diritti, compreso il diritto di avere accesso ai propri dati personali o di ottenerne la rettifica o la cancellazione.

([335]) Articolo 6, paragrafo 1, della legge n. 9.883 del 7 dicembre 1999 – legge che istituisce il sistema di intelligence brasiliano.

([336]) Risoluzione n. 2 del 2021-CN sulla Comissão mista de Controle da Atividade de Inteligência (CCAI), disponibile all'indirizzo: https://www2.camara.leg.br/legin/fed/rescon/2013/resolucao-2-22-novembro-2013-777449-publicacaooriginal-141944-pl.html.

([337]) Sezione 2.4 del decreto, del 15 dicembre 2017, su una strategia nazionale in materia di intelligence.

([338]) Cfr. in particolare l'articolo 3 della risoluzione n. 2 del 2021-CN sulla Comissão mista de Controle da Atividade de Inteligência (CCAI).

([339]) Articolo 13 della risoluzione n. 2 del 2021-CN sulla Comissão mista de Controle da Atividade de Inteligência (CCAI).
Le informazioni sulle riunioni e i documenti preparati dalla CCAI sono disponibili online e regolarmente aggiornati agli indirizzi che seguono: https://legis.senado.leg.br/atividade/comissoes/comissao/449/ e https://www.congressonacional.leg.br/legislacao-e-publicacoes/glossario-legislativo/-/legislativo/termo/comissao_mista_de_controle_das_atividades_de_inteligencia_ccai_cn.

([340]) Articolo 4 della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

([341]) Articolo 55-J, punto XI, della legge n. 13.709 del 14 agosto 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD) – legge generale sulla protezione dei dati.

(218) Come specificato nel considerando 9 della presente decisione, l'accesso ai mezzi di ricorso è garantito ai cittadini brasiliani e di paesi terzi, indipendentemente dal fatto che si trovino o meno nel territorio nazionale.

(219) In primo luogo, le persone fisiche dispongono di un diritto «assoluto» di intentare un'azione legale per tutelare i loro diritti. Ai sensi delle norme generali del codice di procedura civile, per intentare un'azione in giudizio non occorre che una persona fisica dimostri un danno (vale a dire che dimostri di essere soggetta a sorveglianza o che i suoi dati sono stati trattati per finalità di sicurezza nazionale). La persona fisica può esercitare i propri diritti in base all'*habeas data* in relazione ai dati trattati dalle autorità di intelligence ([342]).

(220) In caso di ricorso dinanzi a un organo giurisdizionale, le persone fisiche possono chiedere il risarcimento dei danni. Analogamente a quanto avviene per il trattamento a fini di contrasto penale, la costituzione federale e il codice di procedura civile forniscono le basi giuridiche per chiedere il risarcimento dei danni immateriali o materiali causati da un'autorità pubblica che ha raccolto o utilizzato illecitamente dati, anche attraverso azioni collettive ([343]).

(221) In secondo luogo, la Corte suprema federale ha confermato l'applicazione parziale della LGPD alle finalità di sicurezza nazionale e, per estensione, il potere dell'ANPD di gestire i reclami relativi al trattamento di dati personali da parte delle autorità pubbliche a fini di sicurezza nazionale ([344]). Nella stessa sentenza, la Corte ha osservato che il trattamento di dati personali effettuato da enti pubblici in contrasto con i parametri giuridici e costituzionali impone la responsabilità civile dello Stato per i danni subiti dalle persone fisiche ai sensi dell'articolo 42 della LGPD ([345]).

(222) In terzo luogo, la CCAI può ricevere e istruire denunce di violazioni dei diritti e delle garanzie fondamentali commesse da organismi pubblici ed enti che svolgono attività di intelligence e controspionaggio, presentate da qualsiasi cittadino, partito politico o associazione ([346]). Su tale base, la CCAI può effettuare controlli o indagini. La CCAI offre pertanto un'ulteriore via amministrativa di ricorso in caso di violazioni dei diritti connesse al trattamento dei dati a fini di sicurezza nazionale. Le denunce ricevute dalla CCAI possono poi essere ulteriormente sottoposte agli organi giurisdizionali.

(223) I diversi mezzi di ricorso disponibili nell'ambito del regime brasiliano consentono alle persone fisiche di ottenere un risarcimento. In particolare, le persone fisiche possono contestare la legittimità dell'operato delle autorità pubbliche e di intelligence, nonché ottenere il risarcimento dei danni.

4. **CONCLUSIONI**

(224) La Commissione ritiene che la Repubblica federativa del Brasile, tramite la LGPD, assicuri un livello di protezione dei dati personali trasferiti dall'Unione europea che è essenzialmente equivalente a quello garantito dal regolamento (UE) 2016/679.

(225) Inoltre la Commissione ritiene che, nel complesso, i meccanismi di vigilanza e i mezzi di ricorso previsti dalla normativa brasiliana consentano di individuare e affrontare nella pratica eventuali violazioni delle norme in materia di protezione dei dati commesse dai titolari del trattamento e dai responsabili del trattamento in Brasile e offrano all'interessato mezzi di ricorso che gli consentono di accedere ai dati personali che lo riguardano e, in ultima analisi, di ottenerne la rettifica o la cancellazione.

([342]) Cfr. il considerando 9 della presente decisione.

([343]) Cfr., ad esempio, l'articolo 43 della legge n. 10.408 del 10 gennaio 2002 – codice di procedura civile, disponibile all'indirizzo: https://www.planalto.gov.br//ccivil_03/leis/2002/l10406compilada.htm e articolo 1 della legge n. 7.397 del 24 luglio 1985 – legge sulla responsabilità civile, disponibile all'indirizzo: https://www.planalto.gov.br/ccivil_03/leis/l7347orig.htm.

([344]) Cfr. i considerando 31 e 162 della presente decisione e la decisione sul ricorso diretto di incostituzionalità n. 6649 del 15 settembre 2022 della Corte suprema federale, disponibile all'indirizzo: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([345]) Corte suprema federale, decisione sul ricorso diretto di incostituzionalità n. 6649, del 15 settembre 2022, punto 8, disponibile all'indirizzo: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([346]) Articolo 3, punto XI, della risoluzione n. 2 del 2021-CN sulla Comissão mista de Controle da Atividade de Inteligência (CCAI).

(226) Infine, sulla base delle informazioni disponibili sull'ordinamento giuridico brasiliano, la Commissione ritiene che qualsiasi ingerenza attuata nell'interesse pubblico, in particolare per finalità di contrasto penale e di sicurezza nazionale, da parte di autorità pubbliche brasiliane in relazione ai diritti fondamentali delle persone i cui dati personali sono trasferiti dall'Unione europea al Brasile sarà limitata a quanto strettamente necessario a conseguire l'obiettivo legittimo in questione, e che contro tali ingerenze esista un'efficace tutela giuridica.

(227) Pertanto, alla luce delle conclusioni della presente decisione, è opportuno decidere che il Brasile garantisce un livello di protezione adeguato ai sensi dell'articolo 45 del regolamento (UE) 2016/679, interpretato alla luce della Carta dei diritti fondamentali dell'Unione europea, per i dati personali trasferiti dall'Unione europea a titolari del trattamento e responsabili del trattamento in Brasile soggetti alla LGPD.

5. EFFETTO DELLA PRESENTE DECISIONE E AZIONE DELLE AUTORITÀ DI PROTEZIONE DEI DATI

(228) Gli Stati membri e i loro organi sono tenuti ad adottare le misure necessarie per conformarsi agli atti delle istituzioni dell'Unione, che si presumono legittimi e producono pertanto effetti giuridici, finché non siano stati revocati o annullati nel contesto di un ricorso per annullamento ovvero dichiarati invalidi a seguito di un rinvio pregiudiziale o di un'eccezione di illegittimità.

(229) Di conseguenza, una decisione di adeguatezza adottata dalla Commissione a norma dell'articolo 45, paragrafo 3, del regolamento (UE) 2016/679 è vincolante per tutti gli organi degli Stati membri che ne sono i destinatari, comprese le autorità di controllo indipendenti. In particolare i trasferimenti da un titolare del trattamento o un responsabile del trattamento nell'Unione europea verso titolari del trattamento o responsabili del trattamento in Brasile possono avvenire senza la necessità di ottenere ulteriori autorizzazioni.

(230) È opportuno ricordare che, ai sensi dell'articolo 58, paragrafo 5, del regolamento (UE) 2016/679, e come spiegato dalla Corte di giustizia nella sentenza Schrems, quando un'autorità nazionale di protezione dei dati mette in dubbio, anche in seguito a un reclamo, la compatibilità di una decisione di adeguatezza della Commissione con i diritti fondamentali della persona fisica concernenti la tutela della vita privata e la protezione dei dati, il diritto nazionale deve prevedere mezzi di ricorso per l'affermazione di tali obiezioni dinanzi un organo giurisdizionale nazionale, che può essere tenuto a effettuare un rinvio pregiudiziale alla Corte di giustizia ([347]).

6. MONITORAGGIO, SOSPENSIONE, ABROGAZIONE O MODIFICA DELLA PRESENTE DECISIONE

(231) Secondo la giurisprudenza della Corte di giustizia ([348]), e come riconosciuto dall'articolo 45, paragrafo 4, del regolamento (UE) 2016/679, la Commissione dovrebbe monitorare costantemente gli sviluppi nel paese terzo registrati dopo l'adozione di una decisione di adeguatezza, al fine di valutare se il paese terzo continui a garantire un livello di protezione sostanzialmente equivalente. Tale verifica è in ogni caso obbligatoria quando la Commissione riceve informazioni che fanno sorgere un dubbio giustificato al riguardo.

(232) La Commissione dovrebbe pertanto controllare su base continuativa la situazione in Brasile per quanto riguarda il quadro giuridico e la prassi effettiva del trattamento dei dati personali valutati dalla presente decisione. Sotto questo aspetto, è opportuno prestare particolare attenzione all'applicazione pratica degli obblighi relativi alla valutazione d'impatto sulla protezione dei dati; ai requisiti in materia di trasparenza e alla loro possibile limitazione per quanto riguarda i diritti all'informazione e all'accesso; alle norme sulla notifica delle violazioni dei dati; al regime sanzionatorio e al rispetto delle limitazioni e garanzie per quanto concerne l'accesso da parte di pubbliche amministrazioni, tenendo conto di eventuali evoluzioni in questo settore.

([347]) Schrems I, punto 65: «incombe al legislatore nazionale prevedere mezzi di ricorso che consentano all'autorità nazionale di controllo di cui trattasi di far valere le censure che essa reputa fondate dinanzi ai giudici nazionali, affinché questi ultimi procedano, qualora condividano i dubbi di tale autorità in ordine alla validità della decisione della Commissione, ad un rinvio pregiudiziale inteso all'esame della validità di tale decisione».

([348]) Schrems I, punto 76.

(233) Per agevolare il processo di monitoraggio, le autorità brasiliane, compresa l'ANPD, sono invitate a informare la Commissione degli sviluppi sostanziali rilevanti ai fini della presente decisione, per quanto concerne il trattamento dei dati personali da parte degli operatori economici e delle autorità pubbliche, nonché le limitazioni e le garanzie applicabili all'accesso ai dati personali da parte delle autorità pubbliche.

(234) Inoltre, al fine di consentire alla Commissione di svolgere in modo efficace la propria funzione di monitoraggio, gli Stati membri dovrebbero informarla delle eventuali azioni intraprese dalle autorità nazionali di protezione dei dati, in particolare per quanto riguarda eventuali domande o reclami presentati da interessati dell'UE relativamente al trasferimento di dati personali dall'Unione europea verso titolari del trattamento e responsabili del trattamento in Brasile. La Commissione dovrebbe inoltre essere informata di eventuali indicazioni del fatto che le azioni delle autorità pubbliche del Brasile responsabili della prevenzione, dell'indagine, dell'accertamento o del perseguimento dei reati ovvero della sicurezza nazionale, compresi gli organismi di vigilanza, non garantiscono il necessario livello di protezione.

(235) In applicazione dell'articolo 45, paragrafo 3, del regolamento (UE) 2016/679 ([349]) e alla luce del fatto che il livello di protezione assicurato dall'ordinamento giuridico brasiliano può evolversi, la Commissione, successivamente all'adozione della presente decisione, dovrebbe riesaminare periodicamente se le constatazioni relative al livello di protezione assicurato dal Brasile continuino ad essere giustificate in fatto e in diritto.

(236) A tal fine la presente decisione dovrebbe essere oggetto di un primo riesame entro quattro anni dall'entrata in vigore. I successivi riesami periodici dovrebbero avvenire almeno ogni quattro anni ([350]). I riesami dovrebbero riguardare tutti gli aspetti del funzionamento della presente decisione, compresa la cooperazione dell'ANPD con le autorità di protezione dei dati dell'UE in merito ai reclami presentati dalle persone fisiche. Dovrebbe inoltre includere l'efficacia della vigilanza e delle attività di contrasto, nel settore delle attività di contrasto penale e della sicurezza nazionale.

(237) Per effettuare il riesame la Commissione dovrebbe incontrare l'ANPD, accompagnata, se del caso, da altre autorità brasiliane competenti per l'accesso delle pubbliche amministrazioni, compresi i pertinenti organismi di vigilanza. Alla riunione dovrebbero poter partecipare i rappresentanti dei membri del comitato europeo per la protezione dei dati. Nel quadro del riesame la Commissione dovrebbe chiedere all'ANPD di fornire informazioni complete su tutti gli aspetti pertinenti alla constatazione di adeguatezza, incluse le limitazioni e le garanzie relativamente all'accesso delle pubbliche amministrazioni. La Commissione dovrebbe inoltre chiedere delucidazioni in merito a qualsiasi informazione ricevuta risultata pertinente ai fini della presente decisione, comprese le relazioni pubbliche delle autorità brasiliane o di altri portatori di interessi in Brasile, del comitato europeo per la protezione dei dati, delle singole autorità di protezione dei dati e dei gruppi della società civile, le informazioni dei mezzi di comunicazione o qualsiasi altra fonte di informazioni disponibile.

(238) La Commissione dovrebbe elaborare, sulla base del riesame, una relazione pubblica da presentare al Parlamento europeo e al Consiglio.

(239) Se dalle informazioni disponibili, in particolare da quelle risultanti dal monitoraggio della presente decisione o fornite dalle autorità brasiliane o degli Stati membri, risulta che il livello di protezione offerto dal Brasile potrebbe non essere più adeguato, la Commissione dovrebbe informare le autorità brasiliane competenti e richiedere che adottino misure adeguate entro un periodo di tempo specificato e ragionevole.

(240) Laddove alla scadenza di tale periodo di tempo specificato le autorità brasiliane competenti non abbiano adottato tali misure o non dimostrino altrimenti in modo soddisfacente che la presente decisione continua ad essere basata su un livello di protezione adeguato, la Commissione avvierà la procedura di cui all'articolo 93, paragrafo 2, del regolamento (UE) 2016/679 al fine di sospendere o abrogare parzialmente o completamente la presente decisione.

(241) In alternativa, la Commissione avvierà tale procedura al fine di modificare la presente decisione, in particolare imponendo ulteriori condizioni per i trasferimenti di dati o limitando il riconoscimento dell'adeguatezza soltanto ai trasferimenti di dati per cui continua ad essere garantito un livello di protezione adeguato.

([349]) Conformemente all'articolo 45, paragrafo 3, del regolamento (UE) 2016/679, «[l]'atto di esecuzione prevede un meccanismo di riesame periodico, […] che tenga conto di tutti gli sviluppi pertinenti nel paese terzo o nell'organizzazione internazionale».

([350]) L'articolo 45, paragrafo 3, del regolamento (UE) 2016/679 dispone che il riesame periodico abbia luogo almeno ogni quattro anni. Cfr. anche comitato europeo per la protezione dei dati, Criteri di riferimento per l'adeguatezza, WP 254 rev. 01.

(242) La Commissione dovrebbe inoltre valutare l'opportunità di avviare la procedura di modifica, sospensione o abrogazione della presente decisione se, nel contesto del riesame o in altro contesto, le autorità brasiliane competenti non forniscano le informazioni o i chiarimenti necessari alla valutazione del livello di protezione offerto ai dati personali trasferiti dall'Unione europea al Brasile o per quanto concerne la conformità alla presente decisione. A tale riguardo, la Commissione dovrebbe tener conto della misura in cui le informazioni pertinenti possono essere ottenute da altre fonti.

(243) In ragione di motivi imperativi d'urgenza debitamente giustificati, la Commissione farà ricorso alla possibilità di adottare, conformemente alla procedura di cui all'articolo 93, paragrafo 3, del regolamento (UE) 2016/679, atti di esecuzione immediatamente applicabili destinati a sospendere, abrogare o modificare la presente decisione.

7. **CONSIDERAZIONI FINALI**

(244) Il comitato europeo per la protezione dei dati ha pubblicato il proprio parere ([351]), del quale si è tenuto conto nell'elaborazione della presente decisione.

(245) Le misure di cui alla presente decisione sono conformi al parere del comitato istituito a norma dell'articolo 93, paragrafo 1, del regolamento (UE) 2016/679,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Ai fini dell'articolo 45 del regolamento (UE) 2016/679, il Brasile garantisce un livello di protezione adeguato dei dati personali trasferiti dall'Unione europea a titolari del trattamento e responsabili del trattamento in Brasile soggetti alla legge generale sulla protezione dei dati (LGPD).

Articolo 2

Quando, al fine di proteggere le persone con riguardo al trattamento dei loro dati personali, le autorità competenti degli Stati membri esercitano i poteri di cui all'articolo 58 del regolamento (UE) 2016/ 679 in relazione ai trasferimenti di dati che rientrano nell'ambito di applicazione di cui all'articolo 1, lo Stato membro interessato ne informa senza indugio la Commissione.

Articolo 3

1. La Commissione monitora costantemente l'applicazione del quadro giuridico su cui si basa la presente decisione al fine di valutare se il Brasile continui a garantire un livello di protezione adeguato ai sensi dell'articolo 1.

2. Gli Stati membri e la Commissione si informano reciprocamente dei casi in cui l'autorità brasiliana di protezione dei dati (Agência Nacional de Proteção de Dados - ANPD) o qualsiasi altra autorità brasiliana competente non garantisce il rispetto del quadro giuridico su cui si basa la presente decisione.

3. Gli Stati membri e la Commissione si informano reciprocamente di qualsiasi indicazione del fatto che le ingerenze delle autorità pubbliche brasiliane nel diritto delle persone alla protezione dei loro dati personali vanno oltre quanto strettamente necessario o che contro tali ingerenze non esiste una tutela giuridica efficace.

4. Dopo quattro anni dalla data di notifica della presente decisione agli Stati membri, e successivamente almeno ogni quattro anni, la Commissione verifica la constatazione enunciata all'articolo 1 in base a tutte le informazioni disponibili, comprese quelle ricevute nell'ambito del riesame effettuato congiuntamente con le autorità brasiliane pertinenti.

([351]) Comitato europeo per la protezione dei dati, parere sulla decisione di adeguatezza relativa al Brasile, novembre 2025, disponibile all'indirizzo: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-282025-regarding-european-commission-draft_en.

5. In presenza di indicazioni del fatto che non è più assicurato un livello di protezione adeguato la Commissione informa le autorità brasiliane competenti e può sospendere, abrogare o modificare la presente decisione.

6. La Commissione può inoltre sospendere, abrogare o modificare la presente decisione se la mancanza di collaborazione da parte del governo del Brasile le impedisce di stabilire se la constatazione di cui all'articolo 1 della presente decisione risulti compromessa.

Articolo 4

Gli Stati membri sono destinatari della presente decisione.

Fatto a Bruxelles, il 26 gennaio 2026

Per la Commissione
Michael McGRATH
Membro della Commissione