COMMISSIONE
EUROPEA

Bruxelles, 15.1.2024
COM(2024) 7 final

RELAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

sul primo riesame del funzionamento delle decisioni di adeguatezza adottate a norma dell'articolo 25, paragrafo 6, della direttiva 95/46/CE

{SWD(2024) 3 final}

1. IL PRIMO RIESAME – ANTEFATTI E CONTESTO

La presente relazione contiene le constatazioni della Commissione sul primo riesame delle decisioni di adeguatezza adottate sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46/CE[1] (direttiva sulla protezione dei dati).

In tali decisioni la Commissione ha constatato che 11 paesi o territori garantiscono un livello di protezione adeguato dei dati personali trasferiti dall'Unione europea (UE)[2]: Andorra[3], Argentina[4], Canada (per gli operatori commerciali)[5], isole Fær Øer[6], Guernsey[7], isola di Man[8], Israele[9], Jersey[10], Nuova Zelanda[11], Svizzera[12] e Uruguay[13]. Di conseguenza i trasferimenti di dati dall'Unione verso questi paesi o territori possono avere luogo senza ulteriori prescrizioni.

Con l'entrata in applicazione del regolamento (UE) 2016/679[14] (regolamento generale sulla protezione dei dati) il 25 maggio 2018, le decisioni di adeguatezza adottate ai sensi della

[1] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, pag. 31).
[2] In seguito alla sua integrazione nell'accordo sullo Spazio economico europeo (SEE), il regolamento generale sulla protezione dei dati si applica anche alla Norvegia, all'Islanda e al Liechtenstein. I riferimenti all'UE contenuti nella presente relazione sono da intendersi come riferimenti estesi anche agli Stati del SEE.
[3] Decisione 2010/625/UE della Commissione, del 19 ottobre 2010, ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali ad Andorra (GU L 277 del 21.10.2010, pag. 27).
[4] Decisione 2003/490/CE della Commissione, del 30 giugno 2003, conforme alla direttiva 95/46/CE del Parlamento europeo e del Consiglio e riguardante l'adeguatezza della tutela dei dati personali fornita in Argentina (GU L 168 del 5.7.2003, pag. 19).
[5] Decisione 2002/2/CE della Commissione, del 20 dicembre 2001, conforme alla direttiva 95/46/CE del Parlamento europeo e del Consiglio e riguardante l'adeguatezza della protezione fornita dalla legge canadese sulla tutela delle informazioni personali e sui documenti elettronici (Canadian Personal Information Protection and Electronic Documents Act), (GU L 2 del 4.1.2002, pag. 13).
[6] Decisione 2010/146/UE della Commissione, del 5 marzo 2010, ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguata protezione fornita dalla legge delle Isole Faer Øer sul trattamento dei dati personali (GU L 58 del 9.3.2010, pag. 17).
[7] Decisione 2003/821/CE della Commissione, del 21 novembre 2003, sull'adeguata protezione dei dati personali in Guernsey (GU L 308 del 25.11.2003, pag. 27).
[8] Decisione 2004/411/CE della Commissione, del 28 aprile 2004, sulla adeguata protezione dei dati personali nell'Isola di Man (GU L 151 del 30.4.2004, pag. 48).
[9] Decisione 2011/61/UE della Commissione, del 31 gennaio 2011, ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte dello Stato d'Israele in relazione al trattamento automatizzato di tali dati (GU L 27 dell'1.2.2011, pag. 39).
[10] Decisione 2008/393/CE della Commissione, dell'8 maggio 2008, ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali a Jersey (GU L 138 del 28.5.2008, pag. 21).
[11] Decisione di esecuzione 2013/65/UE della Commissione, del 19 dicembre 2012, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte della Nuova Zelanda (GU L 28 del 30.1.2013, pag. 12).
[12] Decisione 2000/518/CE della Commissione, del 26 luglio 2000, riguardante l'adeguatezza della protezione dei dati personali in Svizzera a norma della direttiva 95/46/CE (GU L 215 del 25.8.2000, pag. 1).
[13] Decisione di esecuzione 2012/484/UE della Commissione, del 21 agosto 2012, ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte della Repubblica orientale dell'Uruguay in relazione al trattamento automatizzato di tali dati (GU L 227 del 23.8.2012, pag. 11).
[14] 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) (GU L 119 del 4.5.2016, pag. 1).

direttiva sulla protezione dei dati sono rimaste in vigore[15]. Al contempo il regolamento generale sulla protezione dei dati ha chiarito che le constatazioni relative all'adeguatezza sono "strumenti in evoluzione", stabilendo che la Commissione deve controllare su base continuativa gli sviluppi nei paesi terzi che potrebbero incidere sul funzionamento delle decisioni di adeguatezza vigenti[16]. Inoltre l'articolo 97 del regolamento generale sulla protezione dei dati impone alla Commissione di riesaminare periodicamente tali decisioni, ogni quattro anni, per determinare se i paesi e i territori nei confronti dei quali è stata adottata una decisione di adeguatezza continuino a fornire un livello adeguato di protezione dei dati personali.

Il primo riesame delle decisioni di adeguatezza adottate a norma del precedente quadro dell'UE per la protezione dei dati è stato avviato nell'ambito di una più ampia valutazione dell'applicazione e del funzionamento del regolamento generale sulla protezione dei dati, su cui la Commissione ha presentato le proprie constatazioni nella comunicazione "La protezione dei dati come pilastro dell'autonomia dei cittadini e dell'approccio dell'UE alla transizione digitale: due anni di applicazione del regolamento generale sulla protezione dei dati"[17]. La conclusione di quest'aspetto del riesame è stata però rinviata per tener conto della sentenza della Corte di giustizia nella causa *Schrems II*[18], in cui la Corte ha fornito importanti chiarimenti su alcuni elementi essenziali del criterio di adeguatezza, oltre che su altri sviluppi correlati. Tutto questo ha poi condotto a scambi dettagliati con i paesi e i territori interessati, in merito ai pertinenti aspetti dei rispettivi quadri giuridici, meccanismi di vigilanza e sistemi di esecuzione[19]. La presente relazione tiene pienamente conto di tutti questi sviluppi, nell'UE come nei territori e paesi terzi interessati.

È importante ricordare che il primo riesame si svolge nel contesto di uno sviluppo esponenziale delle tecnologie digitali. Nel corso dei decenni passati l'importanza delle decisioni di adeguatezza si è sensibilmente accentuata, giacché i flussi di dati sono diventati parte integrante della trasformazione digitale della società e della globalizzazione dell'economia. Il trasferimento transfrontaliero di dati fa ormai parte delle operazioni quotidiane delle imprese europee di tutte le dimensioni, in tutti i settori. Oggi più che mai il rispetto della vita privata rappresenta una condizione per la stabilità, la sicurezza e la competitività dei flussi commerciali. In tale contesto le decisioni di adeguatezza svolgono sotto molti punti di vista un ruolo sempre più importante. Facendo sì che i trasferimenti di dati siano accompagnati dalla

[15] Cfr. l'articolo 45, paragrafo 9, del regolamento generale sulla protezione dei dati, il quale stabilisce che le decisioni adottate dalla Commissione in base all'articolo 25, paragrafo 6, della direttiva 95/46/CE restano in vigore fino a quando non sono modificate, sostituite o abrogate da una decisione della Commissione adottata conformemente all'articolo 45, paragrafi 3 o 5.

[16] Articolo 45, paragrafo 4, del regolamento generale sulla protezione dei dati. Cfr. anche la sentenza della Corte di giustizia dell'Unione europea del 6 ottobre 2015, nella causa C-362/14, Maximillian Schrems/Data Protection Commissioner (*Schrems I*), ECLI:EU:C:2015:650, punto 76.

[17] La comunicazione, pubblicata nel giugno 2020, è disponibile al link seguente:https://ec.europa.eu/info/law/law-topic/data-protection/communication-two-years-application-general-data-protection-regulation_en.

[18] Sentenza della Corte di giustizia dell'Unione europea, del 16 luglio 2020, nella causa C-311/18, Data Protection Commissioner/Facebook Ireland Ltd. e Maximilian Schrems (*Schrems II*), ECLI:EU:C:2020:559.

[19] La decisione di adeguatezza riguardante il Giappone è stata adottata sulla base del regolamento generale sulla protezione dei dati e prevede un riesame periodico separato. Il primo riesame è stato portato a termine nell'aprile 2023 con la relazione della Commissione al Parlamento europeo e al Consiglio sul primo riesame del funzionamento della decisione di adeguatezza relativa al Giappone (COM(2023) 275 final), disponibile al link seguente: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=COM:2023:275:FIN.

protezione degli stessi, tali decisioni garantiscono la sicurezza dei flussi di dati nel rispetto dei diritti degli individui, in linea con l'approccio alla trasformazione digitale incentrato sulla persona, adottato dall'UE. In quanto comportano il riconoscimento che il quadro di tutela della vita privata dei paesi terzi offre un livello di protezione essenzialmente equivalente a quello dell'UE, le decisioni di adeguatezza promuovono la convergenza tra sistemi di tutela della vita privata basati su rigorose norme di protezione. Inoltre, come si illustra nella presente relazione, anziché costituire un punto di arrivo le decisioni di adeguatezza hanno gettato le basi di una collaborazione più stretta e di un'ulteriore convergenza normativa tra l'Unione europea e i suoi partner che adottano un'impostazione analoga. Consentendo il libero flusso dei dati personali, queste decisioni hanno aperto canali commerciali agli operatori dell'Unione, tra l'altro integrando e ampliando i benefici degli accordi commerciali, e hanno favorito la cooperazione con i partner stranieri in un ampio ventaglio di settori normativi. Esse hanno offerto una soluzione diretta e globale ai trasferimenti di dati, senza che l'esportatore dei dati debba fornire ulteriori garanzie o ottenere alcuna autorizzazione; in tal modo rendono più facile, soprattutto alle piccole e medie imprese, rispettare i requisiti previsti dal regolamento generale sulla protezione dei dati per il trasferimento internazionale. Infine, grazie al loro "effetto rete", le decisioni di adeguatezza adottate dalla Commissione europea acquistano rilevanza sempre maggiore anche al di fuori dell'UE, poiché consentono il libero flusso di dati non solo con le 30 economie dell'UE, ma anche con molte altre giurisdizioni nel mondo[20] che riconoscono nei paesi, per cui esiste una decisione di adeguatezza dell'UE, "destinazioni sicure" ai sensi delle proprie norme di protezione dei dati.

Per tutti questi motivi - come conferma anche l'intenso e proficuo dialogo con i territori e i paesi terzi interessati, su cui si basa il riesame - le decisioni di adeguatezza sono diventate una componente strategica delle relazioni complessive dell'UE con questi partner stranieri e sono considerate un importante fattore che consente di intensificare la cooperazione in una vasta gamma di settori. È dunque particolarmente importante che tali decisioni possano superare la prova del tempo e affrontare nuovi sviluppi e nuove sfide.

2. OGGETTO E METODOLOGIA DEL RIESAME

Le decisioni di adeguatezza che sono oggetto del riesame sono state adottate a norma del quadro dell'UE per la protezione dei dati che precedeva il regolamento generale sulla protezione dei dati. Le decisioni più recenti risalgono circa a un decennio fa (ad esempio quelle su Nuova Zelanda e Uruguay, adottate entrambe nel 2012), mentre altre sono in vigore da oltre 20 anni (ad esempio quella sul Canada, adottata nel 2001, e quella sulla Svizzera, adottata nel 2000). Da allora in tutti gli 11 paesi e territori i quadri per la protezione dei dati si sono evoluti, ad esempio tramite riforme legislative o normative, sviluppi nelle pratiche di applicazione delle autorità di protezione dei dati o la giurisprudenza.

Nello svolgimento della valutazione la Commissione si è pertanto concentrata sull'evoluzione dei quadri per la protezione dei dati che, nei paesi e nei territori interessati, ha avuto luogo dopo l'adozione della decisione di adeguatezza. La Commissione ha valutato come tale evoluzione abbia ulteriormente plasmato il panorama della protezione dei dati nel paese o nel territorio in

[20] Come per esempio Argentina, Colombia, Israele, Marocco, Svizzera e Uruguay.

questione, e se - alla luce di tale evoluzione - i vari regimi continuino a garantire un livello di protezione adeguato.

A tal fine si è tenuto pienamente conto dell'evoluzione del regime di protezione dei dati vigente nella stessa Unione europea, soprattutto con l'entrata in applicazione del regolamento generale sulla protezione dei dati. In particolare, dall'adozione di queste decisioni di adeguatezza in poi, la norma giuridica applicabile a tali decisioni e gli elementi pertinenti per valutare se un sistema straniero garantisca un livello di protezione adeguato sono stati ulteriormente chiariti tramite la giurisprudenza della Corte di giustizia dell'Unione europea e gli orientamenti adottati dal gruppo di lavoro Articolo 29 e dal suo successore, il comitato europeo per la protezione dei dati[21] (EDPB).

Segnatamente, nella sentenza del 6 ottobre 2015 nella causa *Schrems I*, la Corte di giustizia ha stabilito che, mentre non può esigersi che un paese terzo assicuri un livello di protezione identico a quello garantito nell'ordinamento giuridico dell'Unione, la verifica dell'adeguatezza deve essere intesa nel senso che esige un livello di protezione "sostanzialmente equivalente"[22]. 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[23]. La verifica dell'adeguatezza richiede pertanto una valutazione globale del sistema del paese terzo nel suo complesso, estesa alla sostanza delle tutele della vita privata, alla loro effettiva attuazione e all'applicazione.

La Corte di giustizia ha chiarito inoltre che la valutazione della Commissione non dovrebbe limitarsi al quadro generale per la protezione dei dati del paese terzo, ma dovrebbe comprendere pure le norme che disciplinano l'accesso ai dati personali da parte delle autorità pubbliche, segnatamente a fini di amministrazione della giustizia e sicurezza nazionale[24]. Impiegando come parametro la Carta dei diritti fondamentali, la Corte di giustizia ha individuato vari requisiti che tali norme dovrebbero rispettare per soddisfare il criterio dell'"equivalenza sostanziale". La legislazione in questo settore dovrebbe ad esempio prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura de qua e impongano requisiti minimi in modo che le persone i cui dati personali sono interessati dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati contro il rischio di abusi nonché contro eventuali accessi e usi illeciti dei suddetti dati[25]. Dovrebbe altresì prevedere la possibilità per il singolo di avvalersi di rimedi giuridici al fine di accedere a dati personali che lo riguardano, oppure di ottenere la rettifica o la soppressione di tali dati[26].

[21] Il comitato europeo per la protezione dei dati riunisce le autorità di controllo per la protezione dei dati degli Stati membri e il garante europeo della protezione dei dati.
[22] *Schrems I*, punti 73, 74 e 96. Si veda anche il considerando 104 del regolamento (UE) 2016/679, che fa riferimento al criterio dell'equivalenza sostanziale.
[23] *Schrems I*, punto 74.
[24] *Schrems I*, punto 90.
[25] *Schrems I*, punto 91.
[26] *Schrems I*, punto 95.

Il regolamento generale sulla protezione dei dati si è basato sui chiarimenti forniti dalla Corte di giustizia stabilendo un dettagliato catalogo di elementi che la Commissione deve prendere in considerazione nel valutare l'adeguatezza[27]. Inoltre, nella sentenza *Schrems II* del 16 luglio 2020, la Corte di giustizia ha approfondito il criterio dell'"equivalenza sostanziale", in particolare per quanto riguarda le norme sull'accesso ai dati personali da parte delle autorità pubbliche a fini di amministrazione della giustizia e sicurezza nazionale. In particolare, secondo quanto ha chiarito la Corte di giustizia, il criterio dell'"equivalenza sostanziale" esige che i quadri giuridici pertinenti da cui sono vincolate le autorità pubbliche nei territori e nei paesi terzi interessati includano requisiti minimi tali da garantire che tali autorità non possano accedere ai dati oltre quanto è necessario e proporzionato per perseguire obiettivi legittimi, e che gli interessati godano di diritti effettivi e azionabili nei confronti di tali autorità[28].

L'evoluzione del criterio di adeguatezza si riflette altresì negli orientamenti originariamente adottati dal gruppo di lavoro Articolo 29 e successivamente approvati dall'EDPB[29]. Questi orientamenti, e in particolare i cosiddetti "criteri di riferimento per l'adeguatezza", chiariscono ulteriormente gli elementi di cui la Commissione deve tener conto nell'effettuare una valutazione dell'adeguatezza, anche offrendo una panoramica delle "garanzie essenziali" per l'accesso ai dati personali da parte delle autorità pubbliche. I criteri di riferimento per l'adeguatezza si basano in particolare sulla giurisprudenza della Corte europea dei diritti dell'uomo e sono stati aggiornati dall'EDPB per tener conto dei chiarimenti forniti dalla Corte di giustizia dell'Unione europea nella sentenza *Schrems II*[30]. È importante notare che anche secondo i criteri di riferimento per l'adeguatezza il criterio dell'"equivalenza sostanziale" non comporta una duplicazione pedissequa (una "fotocopia") delle norme dell'Unione, dal momento che i mezzi per assicurare un livello di protezione comparabile possono variare tra i diversi sistemi di tutela della vita privata, che spesso rispecchiano tradizioni giuridiche differenti.

Per determinare quindi se le 11 decisioni di adeguatezza adottate ai sensi delle norme precedenti continuino a soddisfare i criteri stabiliti dal regolamento generale sulla protezione dei dati, la Commissione ha tenuto conto non soltanto dell'evoluzione dei quadri per la protezione dei dati nei paesi e nei territori interessati, ma anche dell'evoluzione che l'interpretazione del criterio di adeguatezza ha registrato nel diritto dell'Unione europea. Ciò comporta altresì una valutazione del quadro giuridico che regola l'accesso ai dati personali (o l'utilizzo di tali dati) trasferiti dall'Unione europea dalle autorità pubbliche dei paesi o territori per cui è stato accertato un livello di protezione adeguato ai sensi dell'articolo 25, paragrafo 6, della direttiva sulla protezione dei dati.

[27] Articolo 45, paragrafo 2, del regolamento generale sulla protezione dei dati.
[28] *Schrems II*, punti 180-182.
[29] Criteri di riferimento per l'adeguatezza, WP 254 rev. 01, 6 febbraio 2018 (disponibile all'indirizzo:https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108).
[30] Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza (disponibile all'indirizzo:https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_en).

3. PROCESSO DI RIESAME

Come si è illustrato in precedenza, per ciascun paese o territorio interessato la valutazione delle decisioni di adeguatezza vigenti riguarda il quadro per la protezione dei dati ed eventuali sviluppi concernenti tale quadro giuridico, verificatisi dopo l'adozione della constatazione di adeguatezza, nonché le norme che disciplinano l'accesso ai dati da parte del governo, segnatamente a fini di contrasto e sicurezza nazionale. Negli anni passati i servizi della Commissione hanno adottato varie misure per effettuare tale valutazione, in stretta cooperazione con ciascuno dei paesi o territori interessati.

Per coadiuvare la Commissione nei suoi obblighi di monitoraggio, ciascuno degli 11 paesi o territori ha fornito alla Commissione informazioni esaustive sugli sviluppi del proprio regime di protezione dei dati verificatisi dopo l'adozione della decisione di adeguatezza. La Commissione ha chiesto inoltre a ciascuno degli 11 paesi o territori informazioni dettagliate riguardanti le norme che disciplinano l'accesso ai dati personali da parte del governo, segnatamente a fini di contrasto e sicurezza nazionale, applicabili nel rispettivo paese o territorio. La Commissione ha chiesto informazioni anche a fonti pubbliche, autorità di vigilanza e di contrasto nonché esperti locali, in merito al funzionamento delle decisioni e ai pertinenti sviluppi in termini di diritto e di pratica in ciascuno dei paesi e dei territori interessati, per quanto riguarda sia le norme sulla protezione dei dati applicabili agli operatori privati, sia l'accesso del governo. Se del caso, infine, si è tenuto conto degli impegni internazionali sottoscritti da questi paesi/territori nel quadro di strumenti regionali o universali.

Su questa base la Commissione ha avviato con ciascuno dei paesi e dei territori interessati un intenso dialogo, nell'ambito del quale molti di questi paesi e territori hanno aggiornato e potenziato la propria legislazione in materia di tutela della vita privata tramite riforme globali o parziali (ad esempio Andorra, Canada, isole Fær Øer, Svizzera, Nuova Zelanda), spinti tra l'altro dall'esigenza di garantire la continuità delle decisioni di adeguatezza. In alcuni di questi paesi le autorità di protezione dei dati hanno adottato normative e/o orientamenti volti a introdurre nuovi requisiti in materia di protezione dei dati (ad esempio Israele e Uruguay) oppure a chiarire determinate norme di tutela della vita privata (ad esempio Argentina, Canada, Guernsey, Jersey, isola di Man, Israele, Nuova Zelanda), sulla base della pratica di applicazione o della giurisprudenza. Inoltre per superare le differenze nel livello di protezione, con alcuni paesi e territori interessati sono state negoziate e concordate ulteriori garanzie per i dati personali trasferiti dall'Europa, qualora ciò fosse necessario per assicurare la continuità della decisione di adeguatezza. Ad esempio il governo canadese ha esteso i diritti di accesso e rettifica per i dati personali trattati dal settore pubblico a tutte le persone, indipendentemente dalla cittadinanza o dal luogo di residenza (mentre in passato tali diritti erano garantiti soltanto ai cittadini canadesi, a coloro che risiedevano stabilmente nel paese o alle persone presenti in Canada)[31]. Un altro esempio: il governo israeliano ha introdotto garanzie specifiche per rafforzare la protezione dei dati personali trasferiti dallo Spazio economico europeo; in particolare si creano così nuovi obblighi in materia di esattezza e conservazione dei dati, si

[31] Sezione 12 della legge sulla tutela della vita privata, ordinanza di estensione della legge sulla tutela della vita privata, n. 1 e ordinanza di estensione della legge sulla tutela della vita privata, n. 2.

rafforzano i diritti all'informazione e alla cancellazione e si introducono categorie supplementari di dati sensibili[32].

Parallelamente i servizi della Commissione hanno raccolto le opinioni del Parlamento europeo (commissione per le libertà civili, la giustizia e gli affari interni)[33], del Consiglio (tramite il gruppo per la tutela dei dati personali)[34], dell'EDPB[35] e del gruppo multilaterale di esperti sul regolamento generale sulla protezione dei dati[36] (composto da rappresentanti della società civile, delle imprese, del mondo accademico e degli operatori della giustizia) sui progressi della valutazione; hanno poi regolarmente informato tutti questi organi e istituzioni.

La presente relazione e il documento di lavoro dei servizi della Commissione (SWD) che l'accompagna costituiscono pertanto il risultato di una stretta cooperazione con ciascuno dei paesi e territori interessati, oltre che della consultazione con le istituzioni e gli organismi dell'UE competenti e del feedback che questi hanno fornito. Si basano su un'ampia gamma di fonti: legislazione, atti regolamentari, giurisprudenza, decisioni e orientamenti redatti dalle autorità di protezione dei dati, relazioni degli organismi di vigilanza (indipendenti) e contributi dei portatori di interessi. Prima dell'adozione della presente relazione, a tutti i paesi e territori menzionati è stata offerta l'opportunità di verificare l'esattezza materiale delle informazioni comunicate sul proprio sistema nel documento di lavoro dei servizi della Commissione.

4. PRINCIPALI RISULTATI E CONCLUSIONI

Il primo riesame ha dimostrato che, dopo l'adozione delle decisioni di adeguatezza, è aumentata la convergenza dei quadri di protezione dei dati vigenti in ciascuno degli 11 paesi o territori con il quadro dell'UE. Per quanto riguarda l'accesso dei governi ai dati personali, il primo riesame ha indicato che il diritto di questi paesi o territori impone garanzie e limitazioni appropriate e prevede meccanismi di vigilanza e ricorso in questo settore.

Le constatazioni dettagliate per ciascuno degli 11 paesi o territori sono presentate nel documento di lavoro dei servizi della Commissione che accompagna la presente relazione. Sulla base di tali constatazioni la Commissione conclude che ciascuno degli 11 paesi e territori continua a garantire un livello adeguato di protezione per i dati personali trasferiti dall'Unione europea ai sensi del regolamento generale sulla protezione dei dati, secondo l'interpretazione

[32] Normative sulla tutela della vita privata (Istruzioni per i dati trasferiti verso Israele dallo Spazio economico europeo), 5783-2023, pubblicate nella Gazzetta ufficiale di Israele (*Reshumut*) il 7 maggio 2023.
[33] Cfr. ad esempio la risoluzione del Parlamento europeo, del 25 marzo 2021, sulla relazione di valutazione della Commissione concernente l'attuazione del regolamento generale sulla protezione dei dati due anni dopo la sua applicazione (2020/2717(RSP), disponibile al link seguente:https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_EN.html.
[34] Cfr. ad esempio il documento "Posizione e conclusioni del Consiglio in merito all'applicazione del regolamento generale sulla protezione dei dati (GDPR)", adottato il 19 dicembre 2019, disponibile al link seguente:https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-1/en/pdf.
[35] Cfr. ad esempio il contributo dell'EDPB per la valutazione del regolamento generale sulla protezione dei dati a norma dell'articolo 97 (non disponibile in IT), adottato il 18 febbraio 2020, disponibile al link seguente:https://edpb.europa.eu/sites/default/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf.
[36] Cfr. ad esempio la relazione del gruppo multilaterale di esperti sulla valutazione del regolamento generale sulla protezione dei dati, disponibile al link seguente: https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=en&do=groupDetail.groupMeeting&meetingId=21356

della Corte di giustizia. Le constatazioni per ciascuno dei paesi e territori adeguati sono sintetizzate di seguito.

4.1. Andorra

La Commissione apprezza gli sviluppi registrati nel quadro giuridico di Andorra dopo l'adozione della decisione di adeguatezza, comprese le modifiche legislative e le attività delle autorità di controllo. In particolare l'adozione della legge qualificata 29/2021 sulla protezione dei dati personali, entrata in vigore nel maggio 2022, ha contribuito ad accrescere il livello di protezione dei dati, giacché è strettamente allineata al regolamento generale sulla protezione dei dati in termini di struttura e componenti principali.

Per quanto riguarda l'accesso del governo ai dati personali, le autorità pubbliche andorrane sono soggette a norme chiare, precise e accessibili in base alle quali possono accedere ai dati trasferiti dall'UE (e successivamente utilizzarli) per obiettivi di interesse pubblico, in particolare a fini di contrasto in materia penale e di sicurezza nazionale. Tali limitazioni e garanzie derivano dal quadro giuridico generale e da impegni internazionali: in particolare la Costituzione andorrana, la Convenzione europea dei diritti dell'uomo (CEDU) e la Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale (Convenzione 108 e protocollo di modifica, che ha dato luogo alla Convenzione 108+ aggiornata), oltre a specifiche norme di protezione dei dati, che si applicano al trattamento dei dati personali per finalità di contrasto e sostanzialmente riproducono gli elementi essenziali della direttiva (UE) 2016/680[37]. La legislazione di Andorra impone inoltre una serie di condizioni e limitazioni specifiche sull'accesso ai dati personali, e sull'utilizzo di tali dati, da parte delle autorità pubbliche; prevede anche meccanismi di vigilanza e ricorso in questo settore.

Sulla base delle constatazioni complessive esposte nel documento di lavoro dei servizi della Commissione, la Commissione conclude che Andorra continua a fornire un livello adeguato di protezione dei dati personali trasferiti dall'UE.

Per quanto riguarda le specifiche norme di protezione dei dati che attualmente si applicano al trattamento di dati da parte delle autorità competenti per l'applicazione della legge, la Commissione accoglie con favore l'intenzione del legislatore andorrano di sostituire queste norme con un regime più generale che sarà allineato in maniera ancora più stretta alle norme vigenti nell'UE. La Commissione sorveglierà attentamente gli sviluppi futuri in questo settore.

4.2. Argentina

La Commissione apprezza gli sviluppi registrati nel quadro giuridico dell'Argentina dopo l'adozione della decisione di adeguatezza, comprese le modifiche legislative, la giurisprudenza e le attività degli organismi di vigilanza, che hanno contribuito ad accrescere il livello di

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

protezione dei dati. In particolare l'indipendenza dell'autorità di controllo argentina per la protezione dei dati è stata sensibilmente rafforzata con il decreto n. 746/17, che ha affidato all'*Agencia de Acceso a la Información Pública* (AAIP) la responsabilità di controllare il rispetto della legge sulla protezione dei dati. L'AAIP ha inoltre emanato una serie di normative e pareri vincolanti che chiariscono le modalità di interpretazione e di applicazione pratica del quadro di protezione dei dati, e contribuiscono in tal modo a mantenere aggiornata la legge sulla protezione dei dati. L'Argentina ha rafforzato i propri impegni internazionali in materia di protezione dei dati aderendo alla Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale e al suo protocollo addizionale nel 2019, e ratificando nel 2023 il protocollo di modifica che ha dato luogo alla Convenzione 108+ aggiornata.

Per quanto riguarda l'accesso del governo ai dati personali, le autorità pubbliche argentine sono soggette a norme chiare, precise e accessibili, in base alle quali possono accedere ai dati trasferiti dall'UE (e successivamente utilizzarli) per obiettivi di interesse pubblico, in particolare a fini di applicazione del diritto penale e di sicurezza nazionale. Tali limitazioni e garanzie derivano dal quadro giuridico generale e da impegni internazionali: in particolare la Costituzione argentina, la Convenzione americana dei diritti dell'uomo, la Convenzione 108 e la Convenzione 108+, oltre alle norme argentine sulla protezione dei dati (legge 25.326 sulla protezione dei dati personali del 4 ottobre 2000) che sono anch'esse applicabili al trattamento dei dati personali da parte delle autorità pubbliche argentine, anche per finalità di contrasto e sicurezza nazionale. La legislazione argentina impone inoltre una serie di condizioni e limitazioni specifiche sull'accesso ai dati personali, e sull'utilizzo di tali dati, a fini di applicazione del diritto penale e di sicurezza nazionale; prevede anche meccanismi di vigilanza e ricorso in questo settore.

Sulla base delle constatazioni complessive esposte nel documento di lavoro dei servizi della Commissione, la Commissione conclude che l'Argentina continua a fornire un livello adeguato di protezione dei dati personali trasferiti dall'UE.

Al contempo la Commissione raccomanda di includere in atti legislativi le misure di protezione che sono state adottate a livello sublegislativo, per potenziare la certezza giuridica e consolidare tali prescrizioni. Il progetto di legge sulla protezione dei dati recentemente presentato al Congresso argentino potrebbe offrire l'occasione di codificare tali sviluppi, rafforzando perciò ulteriormente il quadro argentino di tutela della vita privata. La Commissione sorveglierà attentamente gli sviluppi futuri in questo settore.

4.3. Canada

La Commissione apprezza gli sviluppi registrati nel quadro giuridico del Canada dopo l'adozione della decisione di adeguatezza, comprese le numerose modifiche legislative, la giurisprudenza e le attività degli organismi di vigilanza, che hanno contribuito ad accrescere il livello di protezione dei dati. In particolare la legge sulla tutela delle informazioni personali e sui documenti elettronici (PIPEDA) è stata ulteriormente rafforzata mediante varie modifiche (riguardanti ad esempio le condizioni di efficacia del consenso e le notifiche di violazione dei dati), mentre le principali prescrizioni in materia di protezione dei dati (ad esempio sul

trattamento dei dati sensibili) sono state ulteriormente chiarite tramite la giurisprudenza e per mezzo di orientamenti emanati dall'autorità federale canadese per la protezione dei dati (il Commissariato per la protezione della vita privata del Canada). La Commissione raccomanda di inserire in atti legislativi alcune delle misure di protezione che sono state adottate a livello sublegislativo, per potenziare la certezza giuridica e consolidare tali prescrizioni. La riforma legislativa di PIPEDA attualmente in corso potrebbe offrire l'occasione di codificare tali sviluppi, rafforzando perciò ulteriormente il quadro canadese di tutela della vita privata. La Commissione sorveglierà attentamente gli sviluppi futuri in questo settore.

Per quanto riguarda l'accesso del governo ai dati personali, le autorità pubbliche canadesi sono soggette a norme chiare, precise e accessibili, in base alle quali possono accedere ai dati trasferiti dall'UE (e successivamente utilizzarli) per obiettivi di interesse pubblico, in particolare a fini di applicazione del diritto penale e di sicurezza nazionale. Tali limitazioni e garanzie derivano dal quadro costituzionale generale (la Carta dei diritti e delle libertà del Canada), dalla giurisprudenza, dalla legislazione specifica che disciplina l'accesso ai dati, nonché dalle norme sulla protezione dei dati (cioè la legge sulla tutela della vita privata e leggi analoghe vigenti a livello provinciale) che si applicano altresì al trattamento dei dati personali da parte delle autorità pubbliche canadesi, anche per finalità di contrasto e di sicurezza nazionale. Il sistema giuridico canadese inoltre prevede meccanismi efficaci di vigilanza e ricorso in questo settore, tra l'altro grazie a una recente estensione dei diritti degli interessati e delle possibilità di ricorso per chi non soggiorna in Canada o non è cittadino canadese.

Sulla base delle constatazioni complessive esposte nel documento di lavoro dei servizi della Commissione, la Commissione stessa conclude che il Canada continua a fornire un livello adeguato di protezione dei dati personali trasferiti dall'UE ai destinatari soggetti a PIPEDA. Come si è osservato in precedenza PIPEDA è attualmente oggetto di una riforma legislativa che potrebbe rafforzare ulteriormente le misure di tutela della vita privata, anche in settori pertinenti per la constatazione di adeguatezza.

4.4. Isole Fær Øer

La Commissione apprezza gli sviluppi registrati nel quadro giuridico delle isole Fær Øer dopo l'adozione della decisione di adeguatezza, comprese le modifiche legislative, la giurisprudenza e le attività degli organismi di vigilanza, che hanno contribuito ad accrescere il livello di protezione dei dati. In particolare le isole Fær Øer hanno notevolmente aggiornato il proprio quadro di protezione dei dati con l'adozione della legge sulla protezione dei dati, che è entrata in vigore nel 2021 e ha strettamente allineato il regime delle isole Fær Øer al regolamento generale sulla protezione dei dati.

Per quanto riguarda l'accesso del governo ai dati personali, le autorità pubbliche delle isole Fær Øer sono soggette a norme chiare, precise e accessibili, in base alle quali possono accedere ai dati trasferiti dall'UE (e successivamente utilizzarli) per obiettivi di interesse pubblico, in particolare a fini di applicazione del diritto penale e di sicurezza nazionale. Tali limitazioni e garanzie derivano dal quadro giuridico generale e da impegni internazionali: in particolare il quadro costituzionale e la CEDU, oltre a leggi specifiche che disciplinano l'accesso del governo ai dati e a norme di protezione dei dati che si applicano al trattamento di dati personali a fini di

applicazione del diritto penale (la legge sul trattamento dei dati personali da parte delle autorità di contrasto che è entrata in vigore nelle isole Fær Øer nel 2022 e recepisce la legislazione adottata dalla Danimarca per attuare la direttiva (UE) 2016/680 nelle isole Fær Øer) e di sicurezza nazionale (contenute nella legge sui servizi di sicurezza e di intelligence). In questo settore esistono inoltre meccanismi efficaci di vigilanza e ricorso.

Sulla base delle constatazioni complessive esposte nel documento di lavoro dei servizi della Commissione, la Commissione conclude che le isole Fær Øer continuano a fornire un livello adeguato di protezione dei dati personali trasferiti dall'UE.

4.5. Guernsey

La Commissione apprezza gli sviluppi registrati nel quadro giuridico di Guernsey dopo l'adozione della decisione di adeguatezza, comprese le modifiche legislative e le attività degli organismi di vigilanza, che hanno contribuito ad accrescere il livello di protezione dei dati. In particolare Guernsey ha decisamente aggiornato il proprio quadro di protezione dei dati adottando la legge sulla protezione dei dati (del Baliato di Guernsey) del 2017, che si applica dal 2019 e allinea strettamente il regime di Guernsey al regolamento generale sulla protezione dei dati.

Per quanto riguarda l'accesso del governo ai dati personali, le autorità pubbliche di Guernsey sono soggette a norme chiare, precise e accessibili, in base alle quali possono accedere ai dati trasferiti dall'UE (e successivamente utilizzarli) per obiettivi di interesse pubblico, in particolare a fini di applicazione del diritto penale e di sicurezza nazionale. Tali limitazioni e garanzie derivano dal quadro giuridico generale e da impegni internazionali: in particolare la CEDU e la Convenzione 108, oltre alle norme di Guernsey sulla protezione dei dati, tra cui le disposizioni specifiche per il trattamento di dati personali per finalità di contrasto contenute nell'ordinanza sulla protezione dei dati (Applicazione della legge e questioni correlate) (Baliato di Guernsey), 2018. La legislazione di Guernsey impone inoltre una serie di condizioni e limitazioni specifiche sull'accesso ai dati personali, e sull'utilizzo di tali dati, a fini di applicazione del diritto penale e di sicurezza nazionale; prevede anche meccanismi di vigilanza e ricorso in questo settore.

Sulla base delle constatazioni complessive esposte nel documento di lavoro dei servizi della Commissione, la Commissione conclude che Guernsey continua a fornire un livello adeguato di protezione dei dati personali trasferiti dall'UE.

4.6. Isola di Man

La Commissione apprezza gli sviluppi registrati nel quadro giuridico dell'isola di Man dopo l'adozione della decisione di adeguatezza, comprese le modifiche legislative e le attività degli organismi di vigilanza, che hanno contribuito ad accrescere il livello di protezione dei dati. In particolare nel 2018 l'isola di Man ha adottato una nuova legislazione: la legge sulla protezione dei dati del 2018, integrata dall'ordinanza sulla protezione dei dati del 2018 (applicazione del regolamento generale sulla protezione dei dati), che incorpora gran parte delle disposizioni del quadro di protezione dei dati dell'UE nell'ordinamento giuridico dell'isola di Man, operando

soltanto adattamenti di secondaria importanza su aspetti specifici, in particolare per adattare il quadro al contesto locale.

Per quanto riguarda l'accesso del governo ai dati personali, le autorità pubbliche dell'isola di Man sono soggette a norme chiare, precise e accessibili, in base alle quali possono accedere ai dati trasferiti dall'UE (e successivamente utilizzarli) per obiettivi di interesse pubblico, in particolare a fini di applicazione del diritto penale e di sicurezza nazionale. Tali limitazioni e garanzie derivano dal quadro giuridico generale e da impegni internazionali: in particolare la CEDU e la Convenzione 108, oltre alle norme dell'isola di Man sulla protezione dei dati, tra cui le disposizioni specifiche per il trattamento di dati personali per finalità di contrasto contenute nell'ordinanza sulla protezione dei dati (applicazione della LED) del 2018 e nei regolamenti di esecuzione della LED del 2018. La legislazione dell'isola di Man impone inoltre una serie di limitazioni specifiche sull'accesso ai dati personali, e sull'utilizzo di tali dati, a fini di applicazione del diritto penale e di sicurezza nazionale; prevede anche meccanismi di vigilanza e ricorso in questo settore.

Sulla base delle constatazioni complessive esposte nel documento di lavoro dei servizi della Commissione, la Commissione conclude che l'isola di Man continua a fornire un livello adeguato di protezione dei dati personali trasferiti dall'UE.

4.7. Israele

La Commissione apprezza gli sviluppi registrati nel quadro giuridico di Israele dopo l'adozione della decisione di adeguatezza, comprese le modifiche legislative, la giurisprudenza e le attività degli organismi di vigilanza, che hanno contribuito ad accrescere il livello di protezione dei dati. In particolare Israele ha introdotto garanzie specifiche per rafforzare la protezione dei dati personali trasferiti dallo Spazio economico europeo, adottando normative sulla tutela della vita privata (Istruzioni per i dati trasferiti verso Israele dallo Spazio economico europeo), 5783-2023. Israele ha altresì rafforzato le prescrizioni in materia di sicurezza dei dati adottando le normative sulla tutela della vita privata (sicurezza dei dati), 5777-2017, e ha consolidato l'indipendenza della propria autorità di controllo competente per la protezione dei dati con una risoluzione vincolante del governo.

Per quanto riguarda l'accesso del governo ai dati personali, le autorità pubbliche di Israele sono soggette a norme chiare, precise e accessibili, in base alle quali possono accedere ai dati trasferiti dall'UE (e successivamente utilizzarli) per obiettivi di interesse pubblico, in particolare a fini di applicazione del diritto penale e di sicurezza nazionale. Tali limitazioni e garanzie derivano dal quadro giuridico generale, segnatamente dalla Legge fondamentale di Israele, nonché dalla legge sulla tutela della vita privata, 5741-1981, e dalle normative adottate ai sensi della medesima, che si applicano al trattamento dei dati personali da parte delle autorità pubbliche israeliane, anche per finalità di contrasto e sicurezza nazionale. La legislazione di Israele impone inoltre una serie di limitazioni specifiche sull'accesso ai dati personali, e sull'utilizzo di tali dati, a fini di applicazione del diritto penale e di sicurezza nazionale; prevede anche meccanismi di vigilanza e ricorso in questo settore.

Sulla base delle constatazioni complessive esposte nel documento di lavoro dei servizi della Commissione, la Commissione conclude che Israele continua a fornire un livello adeguato di protezione dei dati personali trasferiti dall'UE.

Al contempo la Commissione raccomanda di inserire in atti legislativi le misure di protezione che sono state adottate a livello sublegislativo e dalla giurisprudenza, per potenziare la certezza giuridica e consolidare tali prescrizioni. Il disegno di legge sulla tutela della vita privata (emendamento n. 14), 5722-2022, che è stato recentemente presentato al parlamento israeliano, offre un'importante opportunità per consolidare e codificare tali sviluppi, rafforzando così ulteriormente il quadro della tutela della vita privata in Israele. La Commissione sorveglierà attentamente gli sviluppi futuri in questo settore.

4.8. Jersey

La Commissione apprezza gli sviluppi registrati nel quadro giuridico di Jersey dopo l'adozione della decisione di adeguatezza, comprese le modifiche legislative, la giurisprudenza e le attività degli organismi di vigilanza, che hanno contribuito ad accrescere il livello di protezione dei dati. In particolare Jersey ha decisamente aggiornato il proprio quadro di protezione dei dati adottando la legge sulla protezione dei dati (di Jersey) del 2018 e la legge sull'autorità di protezione dei dati (di Jersey) del 2018, che sono entrate in vigore nel 2018 e allineano strettamente il regime di Jersey al regolamento generale sulla protezione dei dati.

Per quanto riguarda l'accesso del governo ai dati personali, le autorità pubbliche di Jersey sono soggette a norme chiare, precise e accessibili, in base alle quali possono accedere ai dati trasferiti dall'UE (e successivamente utilizzarli) per obiettivi di interesse pubblico, in particolare a fini di applicazione del diritto penale e di sicurezza nazionale. Tali limitazioni e garanzie derivano dal quadro giuridico generale e da impegni internazionali: in particolare la CEDU e la Convenzione 108, oltre alle norme di Jersey sulla protezione dei dati, tra cui le disposizioni specifiche per il trattamento di dati personali per finalità di contrasto contenute nella legge sulla protezione dei dati (di Jersey) del 2018 modificata dalla relativa appendice 1. La legislazione di Jersey impone inoltre una serie di limitazioni specifiche sull'accesso ai dati personali, e sull'utilizzo di tali dati, a fini di applicazione del diritto penale e di sicurezza nazionale; prevede anche meccanismi di vigilanza e ricorso in questo settore.

Sulla base delle constatazioni complessive esposte nel documento di lavoro dei servizi della Commissione, la Commissione conclude che Jersey continua a fornire un livello adeguato di protezione dei dati personali trasferiti dall'UE.

4.9. Nuova Zelanda

La Commissione apprezza gli sviluppi registrati nel quadro giuridico della Nuova Zelanda dopo l'adozione della decisione di adeguatezza, comprese le modifiche legislative, la giurisprudenza e le attività degli organismi di vigilanza, che hanno contribuito ad accrescere il livello di protezione dei dati. In particolare il regime di protezione dei dati è stato sottoposto a una riforma globale con l'adozione della legge sulla tutela della vita privata del 2020 che ha accentuato ulteriormente la convergenza con il quadro della protezione dei dati dell'UE, soprattutto per

quanto riguarda le norme sui trasferimenti internazionali di dati personali e i poteri dell'autorità di protezione dei dati (Commissariato per la protezione della vita privata).

Per quanto riguarda l'accesso del governo ai dati personali, le autorità pubbliche della Nuova Zelanda sono soggette a norme chiare, precise e accessibili, in base alle quali possono accedere ai dati trasferiti dall'UE (e successivamente utilizzarli) per obiettivi di interesse pubblico, in particolare a fini di applicazione del diritto penale e di sicurezza nazionale. Tali limitazioni e garanzie derivano dal quadro costituzionale generale (ad esempio il Bill of Rights Act) e dalla giurisprudenza, oltre che da leggi specifiche che disciplinano l'accesso del governo ai dati e alle disposizioni della legge sulla tutela della vita privata che si applicano altresì al trattamento dei dati personali da parte delle autorità competenti per l'applicazione del diritto penale e per la sicurezza nazionale. Il sistema giuridico della Nuova Zelanda prevede inoltre diversi meccanismi di vigilanza e ricorso in questo settore.

Sulla base delle constatazioni complessive esposte nel documento di lavoro dei servizi della Commissione, la Commissione conclude che la Nuova Zelanda continua a fornire un livello adeguato di protezione dei dati personali trasferiti dall'UE. La Commissione accoglie inoltre con favore la recente presentazione in parlamento, da parte del governo della Nuova Zelanda, di un progetto di legge volto a modificare la legge sulla tutela della vita privata del 2020 per rafforzare ulteriormente le vigenti prescrizioni in materia di trasparenza. La Commissione sorveglierà attentamente gli sviluppi futuri in questo settore.

4.10. Svizzera

La Commissione apprezza gli sviluppi registrati nel quadro giuridico della Svizzera dopo l'adozione della decisione di adeguatezza, comprese le modifiche legislative, la giurisprudenza e le attività degli organismi di vigilanza, che hanno contribuito ad accrescere il livello di protezione dei dati. In particolare l'aggiornamento della legge federale sulla protezione dei dati ha accentuato ulteriormente la convergenza con il quadro della protezione dei dati dell'UE, soprattutto per quanto riguarda le misure di protezione per i dati sensibili e le norme sui trasferimenti internazionali di dati. La Svizzera ha inoltre rafforzato i propri impegni internazionali in materia di protezione dei dati ratificando la Convenzione 108+ nel settembre 2023.

Per quanto riguarda l'accesso del governo ai dati personali, le autorità pubbliche della Svizzera sono soggette a norme chiare, precise e accessibili, in base alle quali possono accedere ai dati trasferiti dall'UE (e successivamente utilizzarli) per obiettivi di interesse pubblico, in particolare a fini di applicazione del diritto penale e di sicurezza nazionale. Tali limitazioni e garanzie derivano dal quadro giuridico generale e da impegni internazionali: in particolare la Costituzione federale svizzera, la CEDU e la Convenzione 108+, oltre alle norme svizzere sulla protezione dei dati, tra cui la legge federale sulla protezione dei dati e le specifiche norme sulla protezione dei dati che disciplinano l'applicazione del diritto penale (ad esempio il codice di procedura penale) e le autorità di sicurezza nazionale (ad esempio la legge sui servizi di intelligence). La legislazione della Svizzera impone inoltre una serie di limitazioni specifiche sull'accesso ai dati personali, e sull'utilizzo di tali dati, a fini di applicazione del diritto penale e di sicurezza nazionale; prevede anche meccanismi di vigilanza e ricorso in questo settore.

Sulla base delle constatazioni complessive esposte nel documento di lavoro dei servizi della Commissione, la Commissione conclude che la Svizzera continua a fornire un livello adeguato di protezione dei dati personali trasferiti dall'UE.

4.11. Uruguay

La Commissione apprezza gli sviluppi registrati nel quadro giuridico dell'Uruguay dopo l'adozione della decisione di adeguatezza, comprese le numerose modifiche legislative, la giurisprudenza e le attività degli organismi di vigilanza, che hanno contribuito ad accrescere il livello di protezione dei dati. In particolare l'Uruguay ha aggiornato e potenziato la propria legge 18.331 sulla protezione dei dati personali e l'azione Habeas Data del 2008 mediante modifiche legislative che, nel 2018 e nel 2020, hanno ampliato la portata territoriale della legislazione sulla protezione dei dati, hanno stabilito nuovi obblighi in materia di responsabilità (come le valutazioni d'impatto, la protezione dei dati fin dalla progettazione e per impostazione predefinita, la notifica di una violazione dei dati e la nomina dei responsabili della protezione dei dati) e hanno introdotto ulteriori misure di protezione per i dati biometrici. L'Uruguay ha potenziato i propri impegni internazionali nel campo della protezione dei dati aderendo alla Convenzione 108 nel 2019 e ratificando la Convenzione 108+ nel 2021.

Per quanto riguarda l'accesso del governo ai dati personali, le autorità pubbliche dell'Uruguay sono soggette a norme chiare, precise e accessibili, in base alle quali possono accedere ai dati trasferiti dall'UE (e successivamente utilizzarli) per obiettivi di interesse pubblico, in particolare a fini di applicazione del diritto penale e di sicurezza nazionale. Tali limitazioni e garanzie derivano dal quadro giuridico generale e da impegni internazionali: in particolare la Costituzione uruguayana, la Convenzione americana dei diritti dell'uomo, la Convenzione 108 e la Convenzione 108+, oltre alle norme sulla protezione dei dati contenute nella legge 18.331 sulla protezione dei dati personali e nell'azione Habeas Data che sono applicabili al trattamento dei dati personali da parte delle autorità pubbliche uruguayane, segnatamente per finalità di contrasto e di sicurezza nazionale. La legislazione dell'Uruguay impone inoltre una serie di condizioni e limitazioni specifiche sull'accesso ai dati personali, e sull'utilizzo di tali dati, da parte delle autorità pubbliche; prevede anche meccanismi di vigilanza e ricorso in questo settore.

Sulla base delle constatazioni complessive formulate nel quadro del primo riesame, la Commissione conclude che l'Uruguay continua a fornire un livello adeguato di protezione dei dati personali trasferiti dall'UE.

5. MONITORAGGIO E COOPERAZIONE IN FUTURO

La Commissione riconosce e apprezza vivamente l'ottima cooperazione con le autorità competenti in ciascuno dei paesi e territori interessati, che si è registrata nel corso del riesame. La Commissione continuerà a monitorare attentamente gli sviluppi dei quadri di protezione e la pratica effettiva nei paesi e nei territori interessati. Qualora in un paese o territorio per il quale è stata formulata una decisione di adeguatezza si verifichino sviluppi tali da incidere negativamente sul livello di protezione dei dati giudicato adeguato, la Commissione ricorrerà, se necessario, ai poteri di cui dispone ai sensi dell'articolo 45, paragrafo 5, del regolamento

generale sulla protezione dei dati, per sospendere, modificare o revocare una decisione di adeguatezza.

Il riesame conferma che l'adozione di una decisione di adeguatezza non è un punto di arrivo ma offre l'occasione di intensificare ulteriormente il dialogo e la cooperazione con partner internazionali che adottano un'impostazione analoga in materia di flussi di dati e più in generale sulle questioni digitali. A tale proposito la Commissione guarda con interesse ai futuri scambi con le autorità competenti per intensificare la cooperazione a livello internazionale sulla promozione di flussi di dati liberi e sicuri, anche mediante una cooperazione rafforzata in materia di contrasto. Per accelerare questo dialogo e promuovere lo scambio di informazioni e di esperienze, la Commissione intende organizzare nel 2024 una riunione ad alto livello tra i rappresentanti dell'Unione europea e quelli di tutti i paesi per i quali è stata formulata una decisione di adeguatezza.