II

(Atti non legislativi)

DECISIONI

DECISIONE DI ESECUZIONE (UE) 2019/419 DELLA COMMISSIONE

del 23 gennaio 2019

a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio per quanto riguarda la protezione adeguata dei dati personali da parte del Giappone a norma della legge sulla protezione delle informazioni personali

[notificata con il numero C(2019) 304]

(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,

sentito il garante europeo della protezione dei dati,

1. INTRODUZIONE

(1) Il regolamento (UE) 2016/679 stabilisce le regole per il trasferimento dei dati personali dai titolari o dai responsabili del trattamento nell'Unione ai paesi terzi e alle organizzazioni internazionali nella misura in cui tale trasferimento rientri nel suo ambito di applicazione. Le norme in materia di trasferimento internazionale di dati personali sono stabilite nel capo V di tale regolamento, in particolare agli articoli da 44 a 50. Il flusso di dati personali verso e dai paesi al di fuori dell'Unione europea è necessario all'ampliamento della cooperazione e degli scambi internazionali, garantendo al tempo stesso che il livello di protezione offerto ai dati personali nell'Unione europea non sia compromesso.

(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. In tali circostanze i trasferimenti di dati personali verso un paese terzo, un territorio, un settore o un'organizzazione internazionale possono aver luogo senza ulteriori autorizzazioni, come stabilito dall'articolo 45, paragrafo 1, e dal considerando 103 del 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 del sistema giuridico del paese terzo, per quanto riguarda sia le norme applicabili agli importatori di dati sia le limitazioni e le garanzie relative all'accesso ai dati personali da parte delle autorità pubbliche. La valutazione deve determinare se il paese terzo garantisce un livello di protezione "sostanzialmente equivalente" a quello assicurato all'interno dell'Unione [considerando 104 del regolamento (UE) 2016/679]. Come chiarito dalla Corte di giustizia dell'Unione europea, non è richiesto un livello identico di protezione ([2]). In particolare, gli strumenti dei quali il paese terzo si avvale possono essere diversi da quelli attuati all'interno dell'Unione europea, purché si rivelino efficaci, nella prassi, al fine di assicurare un livello adeguato di protezione ([3]). Lo standard di adeguatezza non comporta pertanto una duplicazione pedissequa delle norme

([1]) GU L 119 del 4.5.2016, pag. 1.
([2]) Sentenza della Corte di giustizia nella causa *Maximillian Schrems* contro *Data Protection Commissioner* («*Schrems*»), C-362/14, ECLI:EU:C:2015:650, punto 73.
([3]) *Schrems*, punto 74.

dell'UE. La prova consiste, piuttosto, nel determinare se, con la sostanza dei diritti alla riservatezza e rendendone l'attuazione, l'azionabilità e il controllo effettivi, il sistema estero, nel suo insieme, offre il necessario livello di protezione ([4]).

(4) La Commissione ha esaminato attentamente la legge e le pratiche applicate in Giappone. In base alle constatazioni illustrate nei considerando da 6 a 175 la Commissione giunge alla conclusione che il Giappone assicura un livello adeguato di protezione dei dati personali trasferiti a organizzazioni che rientrano nell'ambito di applicazione della legge giapponese sulla protezione delle informazioni personali ([5]), e che sono soggette alle condizioni aggiuntive cui rimanda la presente decisione. Tali condizioni sono stabilite dalle norme integrative (allegato I) adottate dalla Commissione per la protezione delle informazioni personali (PPC) ([6]) e dalle dichiarazioni, dalle garanzie e dagli impegni ufficiali presentati dal governo giapponese alla Commissione europea (allegato II).

(5) La presente decisione ha per effetto che i trasferimenti da un titolare o responsabile del trattamento dello Spazio economico europeo (SEE) ([7]) a dette organizzazioni in Giappone possono aver luogo senza ulteriori autorizzazioni. La presente decisione non pregiudica l'applicazione diretta del regolamento (UE) 2016/679 a tali organizzazioni quando sono rispettate le condizioni dell'articolo 3 di tale regolamento.

2. NOME APPLICABILI AL TRATTAMENTO DEI DATI DA PARTE DEGLI OPERATORI ECONOMICI

2.1. Quadro giapponese in materia di protezione dei dati

(6) Il sistema giuridico che disciplina la protezione dei dati e della vita privata in Giappone ha le sue radici nella costituzione promulgata nel 1946.

(7) L'articolo 13 della costituzione recita:

«Tutte le persone sono rispettate come individui. Il loro diritto alla vita, alla libertà e al perseguimento della felicità, purché non interferisca con il benessere pubblico, gode della più alta considerazione nella legislazione e nelle altre attività pubbliche».

(8) Sulla base di detto articolo la Corte suprema giapponese ha precisato il diritto delle persone fisiche (persone) alla protezione delle informazioni personali. In una decisione del 1969 la Corte ha infatti riconosciuto il diritto al rispetto della vita privata e alla protezione dei dati come diritto costituzionale ([8]). In particolare, la Corte ha affermato che «ogni persona fisica ha la libertà di proteggere le proprie informazioni personali dalla comunicazione a terzi o dalla divulgazione senza buona ragione». In una decisione del 6 marzo 2008 («Juki-Net» ([9])) la Corte suprema ha inoltre ritenuto che «la libertà dei cittadini nella vita privata è protetta contro l'esercizio del potere pubblico e si può considerare che ogni persona fisica abbia, tra le libertà della persona nella vita privata, la libertà di proteggere le proprie informazioni personali dalla comunicazione a terzi o dalla divulgazione senza buona ragione» ([10]).

(9) Il 30 maggio 2003 il Giappone ha adottato una serie di leggi in materia di protezione dei dati:

— la legge sulla protezione delle informazioni personali (APPI);

— la legge sulla protezione delle informazioni personali detenute da organi amministrativi (APPIHAO);

— la legge sulla protezione delle informazioni personali detenute da agenzie amministrative registrate (APPI-IAA).

([4]) Cfr. Comunicazione della Commissione al Parlamento europeo e al Consiglio - Scambio e protezione dei dati personali in un mondo globalizzato, COM(2017) 7 del 10.1.2017, sezione 3.1, pagg.7-8.
([5]) Legge sulla protezione delle informazioni personali (legge n. 57 del 2003).
([6]) Ulteriori informazioni sulla PPC sono disponibili al seguente link https://www.ppc.go.jp/en/ (compresi i contatti per le domande e i reclami: https://www.ppc.go.jp/en/contactus/access/).
([7]) La presente decisione è rilevante ai fini del SEE. L'accordo sullo Spazio economico europeo (accordo SEE) prevede l'estensione del mercato interno dell'Unione europea ai tre Stati del SEE: Islanda, Liechtenstein e Norvegia. La decisione che ha integrato il regolamento (UE) 2016/679 nell'allegato XI dell'accordo SEE è stata adottata dal Comitato misto SEE il 6 luglio 2018 ed è entrata in vigore il 20 luglio 2018. Il regolamento rientra pertanto nell'ambito di applicazione dell'accordo.
([8]) Sentenza della Corte suprema riunita come Corte costituzionale del 24 dicembre 1969, Keishu vol. 23, n. 12, pag. 1625.
([9]) Corte suprema, sentenza del 6 marzo 2008, Minshu vol. 62 n. 3, pag. 665.
([10]) Corte suprema, sentenza del 6 marzo 2008, Minshu vol. 62 n. 3, pag. 665.

(10) Le ultime due leggi (modificate nel 2016) contengono disposizioni applicabili alla protezione delle informazioni personali da parte di enti pubblici. Il trattamento dei dati che rientra nell'ambito di applicazione di tali leggi non è oggetto della constatazione di adeguatezza contenuta nella presente decisione, che si limita alla protezione delle informazioni personali da parte di «operatori economici che gestiscono informazioni personali» (PIHBO) ai sensi dell'APPI.

(11) Negli ultimi anni l'APPI è stata modificata. La versione modificata è stata promulgata il 9 settembre 2015 ed è entrata in vigore il 30 maggio 2017. È stata introdotta una serie di nuove garanzie e sono state rafforzate alcune garanzie esistenti, avvicinando il sistema di protezione dei dati giapponese a quello europeo. Esse includono, ad esempio, una serie di diritti individuali azionabili o l'istituzione di un'autorità di controllo indipendente (PPC), incaricata della vigilanza e dell'applicazione dell'APPI.

(12) Oltre all'APPI, il trattamento delle informazioni personali che rientra nell'ambito di applicazione della presente decisione è oggetto di disposizioni di attuazione emesse sulla base dell'APPI. Esse includono una modifica all'ordinanza del Gabinetto per l'attuazione della legge sulla protezione delle informazioni personali del 5 ottobre 2016 e le cosiddette disposizioni in materia di esecuzione relative alla legge sulla protezione delle informazioni personali adottate dalla PPC ([11]). Si tratta in entrambi i casi di norme giuridicamente vincolanti e azionabili che sono entrate in vigore contemporaneamente all'APPI modificata.

(13) Il 28 ottobre 2016 il Gabinetto del Giappone (comprendente il primo ministro e i ministri che formano il suo governo) ha inoltre adottato una «politica di base» al fine di «promuovere in modo globale e integrale misure riguardanti la protezione delle informazioni personali». A norma dell'articolo 7 dell'APPI, la «politica di base» è adottata sotto forma di decisione del Gabinetto e comprende orientamenti strategici riguardanti l'attuazione dell'APPI, diretti sia al governo centrale che alle amministrazioni locali.

(14) Con la decisione del Gabinetto adottata il 12 giugno 2018, il governo giapponese ha recentemente modificato la «politica di base». Per facilitare i trasferimenti di dati a livello internazionale, la decisione del Gabinetto delega alla PPC, in quanto autorità competente della gestione e dell'attuazione dell'APPI, «il potere di adottare le misure necessarie a colmare le differenze tra i sistemi e le operazioni del Giappone e quelli del paese straniero interessato sulla base dell'articolo 6 della legge, al fine di assicurare una gestione appropriata delle informazioni personali ricevute da tale paese». La decisione del Gabinetto dispone che ciò include il potere di stabilire una maggiore protezione mediante l'adozione da parte della PPC di disposizioni più rigorose che integrino e che vadano oltre quelle previste dall'APPI e dall'ordinanza del Gabinetto. A norma della decisione tali disposizioni più rigorose sono vincolanti e azionabili nei confronti degli operatori economici giapponesi.

(15) Conformemente all'articolo 6 dell'APPI e alla succitata decisione del Gabinetto, la PPC ha adottato, il 15 giugno 2018, le «Norme integrative ai sensi della legge sulla protezione delle informazioni personali per la gestione dei dati personali che sono trasferiti dall'UE in base a una decisione di adeguatezza» (le «norme integrative») al fine di rafforzare la protezione delle informazioni personali trasferite dall'Unione europea al Giappone in base alla decisione di adeguatezza attuale. Tali norme integrative sono giuridicamente vincolanti per gli operatori economici giapponesi e azionabili, da parte della PPC e degli organi giurisdizionali, al pari delle disposizioni dell'APPI che tali norme integrano con previsioni più rigorose e/o dettagliate ([12]). Poiché gli operatori economici giapponesi che ricevono e/o trattano ulteriormente i dati personali provenienti dall'Unione europea avranno l'obbligo giuridico di conformarsi alle norme integrative, essi dovranno assicurare di poter individuare tali dati personali nel corso di tutto il loro «ciclo di vita» (ad esempio mediante mezzi tecnici («etichette elettroniche») o organizzativi (conservazione in un'apposita banca dati)) ([13]). Nelle sezioni seguenti il contenuto di ciascuna norma integrativa è analizzato nel contesto della valutazione dell'articolo dell'APPI che va a completare.

(16) A differenza di quanto previsto prima della modifica del 2015, quando la competenza era attribuita a vari ministeri giapponesi in settori specifici, l'APPI autorizza la PPC ad adottare «orientamenti» «al fine di assicurare l'attuazione corretta ed efficace delle azioni che devono essere intraprese da un operatore economico nell'ambito delle norme in materia di protezione dei dati». Attraverso gli orientamenti la PPC fornisce un'interpretazione autentica delle

([11]) Consultabili al seguente indirizzo: https://www.ppc.go.jp/files/pdf/PPC_rules.pdf

([12]) Cfr. norme integrative (sezione introduttiva).

([13]) Ciò non è messo in questione dall'obbligo generale di mantenere registrazioni (soltanto) per un determinato periodo di tempo. Anche se l'origine dei dati è tra le informazioni che il PIHBO che li ha acquisiti è tenuto a confermare a norma dell'articolo 26, comma 1, dell'APPI, l'obbligo di cui all'articolo 26, comma 4, dell'APPI, in combinato disposto con l'articolo 18 delle norme della PPC, riguarda soltanto una forma specifica di registrazione (cfr. articolo 16 delle norme della PPC) e non impedisce al PIHBO di assicurare l'individuazione dei dati per periodi più lunghi. Ciò è stato confermato dalla PPC che ha dichiarato che «[l]e informazioni sull'origine dei dati provenienti dall'UE devono essere conservate dal PIHBO per il lasso di tempo necessario a potersi conformare alle norme integrative».

norme, in particolare dell'APPI. Secondo le informazioni ricevute dalla PPC, tali orientamenti formano parte integrante del quadro giuridico e sono da leggere in combinato disposto con il testo dell'APPI, l'ordinanza del Gabinetto, le norme della PPC e una serie di domande e risposte ([14]) elaborate dalla PPC. Gli ordinamenti sono pertanto «vincolanti per gli operatori economici». Quando gli orientamenti affermano che un operatore economico «deve» o «non dovrebbe» tenere una determinata condotta, la PPC considererà il mancato rispetto delle disposizioni pertinenti una violazione della normativa ([15]).

2.2. **Ambito di applicazione materiale e personale**

(17) L'ambito di applicazione dell'APPI è determinato dai concetti in essa definiti di informazioni personali, dati personali e operatori economici che gestiscono informazioni personali. Al tempo stesso l'APPI prevede alcune esenzioni importanti dal suo ambito di applicazione, in particolare per i dati personali trattati in forma anonima e per categorie specifiche di trattamento da parte di alcuni operatori. Sebbene non utilizzi il termine «trattamento», l'APPI ricorre al concetto equivalente di «gestione» che, secondo le informazioni ricevute dalla PPC, copre «qualsiasi azione riguardante i dati personali», tra cui l'acquisizione, la contribuzione, l'accumulo, l'organizzazione, la conservazione, la modifica/il trattamento, il rinnovo, la cancellazione, la produzione, l'utilizzo o la fornitura di informazioni personali.

2.2.1. *Definizione di informazioni personali*

(18) Innanzitutto, per quanto riguarda l'ambito di applicazione materiale, l'APPI distingue tra informazioni personali e dati personali, e soltanto alcune sue disposizioni si applicano alla prima categoria. Ai sensi dell'articolo 2, comma 1, dell'APPI, il concetto di «informazioni personali» include qualsiasi informazione relativa a una persona vivente che ne consenta l'identificazione. La definizione distingue due categorie di informazioni personali: i) codici identificativi individuali e ii) altre informazioni personali che consentano l'identificazione di una persona specifica. Quest'ultima categoria include anche informazioni che di per sé non consentono l'identificazione ma che, quando «facilmente collegabili» ad altre informazioni, permettono l'identificazione di una persona specifica. Secondo gli orientamenti della PPC ([16]), si dovrà valutare caso per caso se le informazioni possono essere ritenute «facilmente collegabili», tenendo in considerazione la situazione effettiva («condizione») dell'operatore economico. Esse saranno ritenute tali se il collegamento è (o può essere) effettuato da un operatore economico medio («normale») con i mezzi a sua disposizione. Ad esempio, le informazioni non sono «facilmente collegabili» ad altre informazioni se un operatore economico deve fare uno sforzo straordinario o commettere atti illeciti per ottenere da uno o più operatori economici le informazioni da collegare.

2.2.2. *Definizione di dati personali*

(19) A norma dell'APPI soltanto alcune forme di informazioni personali rientrano nella nozione di «dati personali». I dati personali sono definiti, infatti, come «informazioni personali che costituiscono una banca dati di informazioni personali», ossia un «corpus di informazioni» che comprende informazioni personali «organizzate sistematicamente così da permettere la ricerca di informazioni personali specifiche mediante computer» ([17]) o «per cui un'ordinanza del Gabinetto dispone l'organizzazione sistematica così da permettere una ricerca agevole delle singole informazioni personali», ma «ad esclusione di quelle per cui un'ordinanza del Gabinetto ritiene poco probabile che pregiudichino i diritti e gli interessi di una persona tenuto conto del metodo con cui sono utilizzate» ([18]).

(20) Tale eccezione è ulteriormente specificata nell'articolo 3, comma 1, dell'ordinanza del Gabinetto secondo cui devono essere soddisfatte contemporaneamente tutte e tre le condizioni seguenti: i) il corpus di informazioni deve essere stato «creato al fine di essere venduto a un gran numero di persone indeterminate e l'emissione di tale corpus non è avvenuta in violazione delle disposizioni di leggi o dei regolamenti basati su di esse»; ii) il corpus di informazioni deve poter essere «acquistato in qualsiasi momento da un gran numero di persone indeterminate» e

([14]) PPC, Domande e risposte, 16 febbraio 2017 (modificate il 30 maggio 2017), consultabile al seguente link: https://www.ppc.go.jp/files/pdf/kojouhouQA.pdf. Le domande e risposte trattano una serie di questioni affrontate negli orientamenti e forniscono esempi pratici, tra l'altro, di che cosa costituisca dati personali sensibili, dell'interpretazione del consenso individuale, dei trasferimenti che implicano terzi nel contesto del cloud computing o dell'obbligo del registro applicato ai trasferimenti transfrontalieri, ecc. Le domande e risposte sono disponibili solo in lingua giapponese.

([15]) A seguito di una domanda specifica la PPC ha comunicato all'EDPB che «gli organi giurisdizionali giapponesi basano la [propria] interpretazione dell'APPI/delle norme della PPC sugli orientamenti quando devono applicare dette norme ai singoli casi loro sottoposti, e hanno quindi fatto direttamente riferimento al testo degli orientamenti della PPC nelle sentenze. Anche da questo punto di vista gli orientamenti della PPC sono vincolanti per gli operatori economici. La PPC non è a conoscenza di casi in cui l'organo giurisdizionale si sia discostato dagli orientamenti». A tal proposito la PPC ha indicato alla Commissione una sentenza in materia di protezione dei dati in cui le conclusioni dell'organo giurisdizionale sono basate esplicitamente sugli orientamenti (cfr. tribunale distrettuale di Osaka, decisione del 19 maggio 2006, Hanrei Jiho, vol. 1948, pag. 122, in cui il giudice ha stabilito che l'operatore economico aveva l'obbligo di effettuare un controllo di sicurezza in base agli orientamenti).

([16]) Orientamenti della PPC (edizione norme generali), pag. 6.

([17]) Ciò include qualsiasi sistema di archiviazione elettronica. Gli orientamenti della PPC (edizione generale, pag. 17) forniscono esempi specifici di informazioni in proposito, ad esempio un elenco di indirizzi e-mail conservato in un software client di posta elettronica.

([18]) Articolo 2, commi 4 e 6, dell'APPI.

iii) i dati personali in esso contenuti devono essere «forniti per il loro scopo originario senza aggiungere ulteriori informazioni relative a una persona vivente». Secondo le spiegazioni ricevute dalla PPC, tale eccezione di applicazione limitata è stata introdotta al fine di escludere gli elenchi telefonici o altri elenchi simili.

(21) Detta distinzione tra «informazioni personali» e «dati personali» è importante per le informazioni raccolte in Giappone, in quanto esse non fanno sempre parte di una «banca dati di informazioni personali» (ad esempio, un insieme unico di dati raccolti e trattati manualmente) e le disposizioni dell'APPI relative soltanto ai dati personali non trovano pertanto applicazione ([19]).

(22) Per contro, tale distinzione non sarà importante per i dati personali importati dall'Unione europea in Giappone sulla base di una decisione di adeguatezza. Poiché di norma i dati provenienti dall'UE saranno trasferiti per via elettronica (dato che nell'era digitale si tratta del modo comune di scambiare dati, specialmente su grandi distanze come nel caso dell'UE e del Giappone), e diventeranno quindi parte dei sistemi di archiviazione elettronica dell'importatore di dati, essi saranno considerati «dati personali» ai sensi dell'APPI. Nel caso eccezionale in cui i dati personali siano trasferiti dall'UE con altri mezzi (ad esempio in formato cartaceo), essi saranno comunque coperti dall'APPI se a seguito del trasferimento saranno inseriti in un «corpus di informazioni» organizzato sistematicamente in modo da consentire facilmente la ricerca delle informazioni specifiche (articolo 2, comma 4, punto ii), dell'APPI). A norma dell'articolo 3, comma 2, dell'ordinanza del Gabinetto, è il caso quando le informazioni sono predisposte «secondo un determinato criterio» e la banca dati contiene strumenti come un sommario o un indice per facilitare la ricerca. Ciò corrisponde alla definizione di «archivio» ai sensi dell'articolo 2, paragrafo 1, del regolamento generale sulla protezione dei dati.

2.2.3. *Definizione di dati personali conservati*

(23) Alcune disposizioni dell'APPI, in particolare gli articoli da 27 a 30 relativi ai diritti individuali, si applicano soltanto a una categoria specifica di dati personali, ossia ai «dati personali conservati». L'articolo 2, comma 7, dell'APPI li definisce come dati personali diversi da quelli che i) «un'ordinanza del Gabinetto ritiene probabile che danneggino l'interesse pubblico o altri interessi nel caso in cui ne sia resa nota la presenza o l'assenza» o ii) «sono destinati a essere cancellati entro un periodo non superiore a un anno, disposto da un'ordinanza del Gabinetto».

(24) La prima delle due categorie è precisata nell'articolo 4 dell'ordinanza del Gabinetto e riguarda quattro diverse eccezioni ([20]). Le esenzioni citate perseguono obiettivi analoghi a quelli elencati nell'articolo 23, paragrafo 1, del regolamento (UE) 2016/679, in particolare la tutela dell'interessato («titolare» nella terminologia dell'APPI) e della libertà altrui, della sicurezza nazionale, della sicurezza pubblica, dell'attività di contrasto nella sfera penale o di altri importanti obiettivi di interesse pubblico generale. Dalla formulazione dell'articolo 4, comma 1, punti da i) a iv), dell'ordinanza del Gabinetto risulta inoltre che la loro applicazione presuppone sempre un rischio specifico per uno degli importanti interessi tutelati ([21]).

(25) La seconda categoria è stata precisata ulteriormente nell'articolo 5 dell'ordinanza del Gabinetto. Tale articolo, in combinato disposto con l'articolo 2, comma 7, dell'APPI, esclude dall'ambito di applicazione della nozione di dati personali conservati, e quindi dai diritti individuali tutelati dall'APPI, i dati personali che sono «destinati a essere cancellati» entro un periodo di sei mesi. La PPC ha spiegato che l'esenzione mira a incentivare gli operatori economici a conservare e trattare i dati per il più breve tempo possibile. Ciò significherebbe tuttavia che gli interessati dell'UE non potrebbero beneficiare di diritti importanti unicamente a causa della durata della conservazione dei loro dati da parte degli operatori economici interessati.

(26) Per far fronte a questa situazione, la norma integrativa (2) stabilisce che i dati personali trasferiti dall'Unione europea «siano gestiti come dati personali conservati ai sensi dell'articolo 2, comma 7, della legge, indipendentemente dal periodo entro il quale sono destinati a essere cancellati». Il periodo di conservazione non avrà pertanto conseguenze sui diritti riconosciuti agli interessati dell'UE.

([19]) Ad esempio, l'articolo 23 dell'APPI sulle condizioni di condivisione dei dati personali con terzi.

([20]) In particolare i dati personali i) «in grado, qualora ne fosse resa nota la presenza o l'assenza, di pregiudicare la vita, l'integrità fisica o il patrimonio del titolare o di un terzo»; ii) i dati «in grado, qualora ne fosse resa nota la presenza o l'assenza, di incoraggiare o causare un atto illegale o ingiusto»; iii) i dati «in grado, qualora ne fosse resa nota la presenza o l'assenza, di compromettere la sicurezza nazionale, distruggere un rapporto di fiducia con un paese straniero o un' organizzazione internazionale, o arrecare svantaggio nei negoziati con un paese straniero o un'organizzazione internazionale»; iv) i dati «in grado, qualora ne fosse resa nota la presenza o l'assenza, di ostacolare il mantenimento della sicurezza e dell'ordine pubblici, ad esempio la prevenzione, la lotta o le indagini relative a un reato».

([21]) A tali condizioni non occorre una comunicazione alla persona. Ciò è conforme all'articolo 23, paragrafo 2, lettera h), del regolamento generale sulla protezione dei dati, che stabilisce che gli interessati non devono essere informati della limitazione qualora «ciò possa compromettere la finalità della stessa».

2.2.4. *Definizione di informazioni personali trattate in forma anonima*

(27) Le disposizioni applicabili alle informazioni personali trattate in forma anonima, definite nell'articolo 2, comma 9, dell'APPI, sono previste nel capo 4, sezione 2, della legge («Obblighi dell'operatore economico che gestisce informazioni trattate in forma anonima»). A tali informazioni non si applicano invece le previsioni del capo IV, sezione 1, dell'APPI, che comprende gli articoli che prevedono le garanzie di protezione dei dati e i diritti che si applicano al trattamento dei dati personali ai sensi della legge medesima. Di conseguenza, sebbene non siano soggette alle norme «standard» in materia di protezione dei dati (specificate nel capo IV, sezione 1, e nell'articolo 42 dell'APPI), le «informazioni personali trattate in forma anonima» rientrano comunque nell'ambito di applicazione dell'APPI, in particolare degli articoli da 36 a 39.

(28) Secondo l'articolo 2, comma 9, dell'APPI le «informazioni personali trattate in forma anonima» sono informazioni relative a una persona che sono state «ottenute dal trattamento di informazioni personali» mediante le misure stabilite nell'APPI (articolo 36, comma 1) e specificate nelle norme della PPC (articolo 19) e che, di conseguenza, rendono impossibile l'identificazione di una persona specifica o il ripristino delle informazioni personali.

(29) Tali disposizioni specificano, come confermato anche dalla PPC, che il processo per rendere le informazioni personali «anonime» non deve necessariamente essere tecnicamente irreversibile. Ai sensi dell'articolo 36, comma 2, dell'APPI, gli operatori economici che gestiscono «informazioni personali trattate in forma anonima» sono semplicemente tenuti a prevenire la reidentificazione mediante l'adozione di misure volte a garantire la sicurezza «delle descrizioni ecc., dei codici di identificazione individuali rimossi dalle informazioni personali utilizzate per ottenere le informazioni trattate in forma anonima e delle informazioni relative al metodo di trattamento applicato».

(30) Poiché, come definite dall'APPI, le «informazioni personali trattate in forma anonima» comprendono dati che consentono ancora la reidentificazione della rispettiva persona, ciò potrebbe significare che i dati personali trasferiti dall'Unione europea potrebbero perdere un parte delle protezioni disponibili a causa di un procedimento che, ai sensi del regolamento (UE) 2016/679, sarebbe considerato una forma di «pseudonimizzazione» piuttosto che un' «anonimizzazione» (non cambiando pertanto la loro natura di dati personali).

(31) Per far fronte a detta situazione, le norme integrative stabiliscono disposizioni aggiuntive applicabili soltanto ai dati personali trasferiti dall'Unione europea nell'ambito della presente decisione. Secondo la norma (5) delle norme integrative, le informazioni personali sono considerate «informazioni personali trattate in forma anonima» ai sensi dell'APPI unicamente «se l'operatore economico che gestisce le informazioni personali adotta misure che rendono l'anonimizzazione della persona irreversibile per chiunque, in particolare mediante la cancellazione delle informazioni relative al metodo di trattamento ecc.». Le norme integrative definiscono nello specifico queste ultime come le informazioni relative a descrizioni e codici di identificazione individuali che sono stati cancellati dalle informazioni personali utilizzate per ottenere «informazioni personali trattate in forma anonima» nonché le informazioni relative al metodo di trattamento applicato per la cancellazione di tali descrizioni e codici di identificazione individuali. In altri termini le norme integrative impongono all'operatore economico che produce informazioni personali trattate in forma anonima di distruggere la «chiave» che consente la reidentificazione dei dati. I dati personali originari dell'Unione europea rientreranno nelle disposizioni dell'APPI relative alle «informazioni personali trattate in forma anonima» soltanto nel caso in cui essi siano considerati informazioni anonime anche a norma del regolamento (UE) 2016/679 ([22]).

2.2.5. *Definizione di operatore economico che gestisce informazioni personali*

(32) Per quanto riguarda il campo di applicazione personale, l'APPI si applica soltanto agli operatori economici che trattano informazioni personali (PIHBO). A norma dell'articolo 2, comma 5, dell'APPI, per PIHBO si intende «una persona che fornisce banche dati di informazioni personali ecc. a scopi commerciali», ad esclusione delle agenzie governative e amministrative a livello centrale e locale.

(33) Gli orientamenti della PPC definiscono un'"attività commerciale" qualsiasi «condotta volta ad esercitare un'impresa socialmente riconosciuta, per il raggiungimento di un determinato oggetto, con o senza scopo di lucro, in modo ripetuto e continuato». Le organizzazioni prive di personalità giuridica (quali le associazioni di fatto) o le persone fisiche sono considerate PIHBO se forniscono (l'uso di) banche dati di informazioni personali ecc. nell'ambito della propria attività commerciale ([23]). Ai sensi dell'APPI la nozione di «attività commerciale» è pertanto molto ampia, in quanto include non soltanto le attività esercitate da qualsiasi organizzazione o persona con scopo di lucro ma anche quelle che ne sono prive. L'uso «a scopi commerciali» include inoltre le informazioni personali che non sono utilizzate nei rapporti commerciali (esterni) dell'operatore, ma internamente, ad esempio per il trattamento dei dati dei dipendenti.

([22]) Cfr. considerando 26 del regolamento (UE) 2016/679.
([23]) Orientamenti della PPC (edizione norme generali), pag. 18.

(34) Per quanto riguarda i beneficiari della protezione prevista dall'APPI, la legge non opera alcuna distinzione sulla base della cittadinanza, della residenza o dell'ubicazione della persona. Lo stesso vale per le possibilità delle persone di presentare ricorso, dinanzi alla PPC o alle autorità giurisdizionali.

2.2.6. *Concetti di titolare del trattamento e di responsabile del trattamento*

(35) L'APPI non effettua una distinzione specifica tra gli obblighi dei titolari del trattamento e quelli dei responsabili del trattamento. La mancanza di tale distinzione non pregiudica tuttavia il livello di protezione, in quanto tutti i PIHBO sono soggetti alle disposizioni dell'APPI nella sua interezza. Se affida la gestione dei dati a un fiduciario (l'equivalente del responsabile del trattamento ai sensi del regolamento generale sulla protezione dei dati), il PIHBO rimane soggetto agli obblighi previsti dall'APPI e dalle norme integrative per quanto riguarda i dati affidati. L'articolo 22 della legge prevede inoltre che il PIHBO è tenuto a «esercitare il controllo necessario e opportuno» sul fiduciario. Come confermato dalla PPC, il fiduciario è poi a sua volta vincolato da tutti gli obblighi contenuti nell'APPI e nelle norme integrative.

2.2.7. *Esclusioni settoriali*

(36) L'articolo 76 dell'APPI esclude alcuni tipi di trattamento dei dati dall'applicazione del capo IV della legge, che contiene le disposizioni principali in materia di protezione dei dati (principi di base, obblighi degli operatori economici, diritti individuali, controllo da parte della PPC). Il trattamento coperto dall'esclusione settoriale di cui all'articolo 76 è escluso anche dai poteri di esecuzione della PPC previsti dall'articolo 43, comma 2, dell'APPI ([24]).

(37) Per quanto riguarda l'esclusione settoriale di cui all'articolo 76 dell'APPI, le categorie pertinenti sono definite utilizzando un doppio criterio basato sul tipo di PIHBO che effettua il trattamento delle informazioni personali e sulla finalità del trattamento. Più in particolare, l'esclusione si applica a: i) emittenti radiotelevisive, case editrici di giornali, agenzie di comunicazione e altre organizzazioni della stampa (comprese le persone che svolgono attività di stampa per professione) purché trattino informazioni personali a fini di stampa; ii) persone che svolgono un'attività di scrittura professionale, purché questa preveda l'utilizzo di informazioni personali; iii) università e qualsiasi altra organizzazione o gruppo che svolge studi accademici o qualsiasi persona appartenente a tale organizzazione, purché trattino informazioni personali ai fini di studi accademici; iv) istituzioni religiose purché trattino informazioni personali ai fini di attività religiose (comprese tutte le attività connesse); v) organizzazioni politiche purché trattino informazioni personali ai fini dell'attività politica (comprese tutte le attività connesse). Il trattamento delle informazioni personali per uno degli scopi elencati nell'articolo 76 da parte degli altri tipi di PIHBO e il trattamento di informazioni personali da parte di uno dei PIHBO elencati per altri motivi, ad esempio nel contesto lavorativo, rientrano nelle disposizioni del capo IV.

(38) Al fine di garantire un adeguato livello di protezione dei dati personali trasferiti dall'Unione europea a operatori economici in Giappone, è opportuno che la presente decisione copra soltanto il trattamento di informazioni personali che rientra nell'ambito di applicazione del capo IV dell'APPI (ossia da parte di un PIHBO, purché la tipologia di trattamento non corrisponda a una delle esclusioni settoriali). L'ambito di applicazione della presente decisione dovrebbe pertanto essere allineato con quello dell'APPI. Secondo le informazioni ricevute dalla PPC, se un PIHBO oggetto della presente decisione modificasse successivamente la finalità di utilizzo (nella misura consentita) e fosse poi soggetto a una delle esclusioni settoriali di cui all'articolo 76 dell'APPI, ciò sarebbe considerato un trasferimento internazionale (dato che, in tali casi, il trattamento delle informazioni personali non rientrerebbe più nel capo IV dell'APPI ed esulerebbe quindi dall'ambito di applicazione di tale norma). Lo stesso varrebbe nel caso in cui un PIHBO fornisse informazioni personali a un soggetto di cui all'articolo 76 dell'APPI ad uso di una delle finalità di trattamento indicate in tale disposizione. Per quanto riguarda i dati personali trasferiti dall'Unione europea, tale caso si configurerebbe pertanto come trasferimento successivo soggetto alle garanzie pertinenti (in particolare a quelle specificate nell'articolo 24 dell'APPI e nella norma integrativa (4)). Quando ha bisogno del consenso dell'interessato ([25]), il PIHBO dovrebbe fornirgli tutte le informazioni necessarie, compreso il fatto che le informazioni personali non sarebbero più protette dall'APPI.

([24]) Per quanto riguarda gli altri operatori la PPC, nell'esercizio dei propri poteri di indagine e di esecuzione, non ne impedisce l'esercizio del diritto alla libertà di espressione, alla libertà accademica, alla libertà di religione e alla libertà di attività politica (articolo 43, comma 1, dell'APPI).

([25]) Come spiegato dalla PPC, gli orientamenti della PPC interpretano il consenso come «[l'] espressione dell'intenzione del titolare di accettare che le sue informazioni personali possano essere gestite con un metodo indicato da un operatore economico che gestisce informazioni personali». Gli orientamenti della PPC (edizione norme generali, pag. 24) elencano i metodi per prestare il consenso considerati «prassi commerciali correnti in Giappone», quali dare il consenso orale, riconsegnare moduli o altri documenti, fornire il consenso a mezzo posta elettronica, spuntare un'apposita casella in una pagina internet, cliccare sulla home page, utilizzare un pulsante di consenso, toccare uno schermo tattile. Tali metodi costituiscono tutti una forma di consenso esplicito.

2.3. **Garanzie, diritti e obblighi**

2.3.1. *Limitazione delle finalità*

(39) I dati personali dovrebbero essere trattati per una finalità specifica e, di conseguenza, dovrebbero essere utilizzati soltanto nella misura in cui l'uso non sia incompatibile con la finalità del trattamento. Tale principio di protezione dei dati è garantito dagli articoli 15 e 16 dell'APPI.

(40) L'APPI si basa sul principio che un operatore economico deve specificare la finalità dell'utilizzo «nel modo più esplicito possibile» (articolo 15, comma 1) ed è poi vincolato da tale finalità quando tratta i dati.

(41) A tal proposito, l'articolo 15, comma 2, dell'APPI stabilisce che la finalità iniziale non può essere modificata dal PIHBO «al di là di un ambito ritenuto ragionevolmente pertinente alla finalità dell'utilizzo precedente la modifica». Nell'interpretazione degli orientamenti della PPC ciò corrisponde a quanto possa essere previsto oggettivamente dall'interessato sulla base delle «normali convenzioni sociali» ([26]).

(42) L'articolo 16, comma 1, dell'APPI vieta ai PIHBO di gestire informazioni personali al di là dell'"ambito necessario per conseguire la finalità di utilizzo" specificata a norma dell'articolo 15 senza il previo consenso dell'interessato, a meno che non si applichi una delle deroghe di cui all'articolo 16, comma 3 ([27]).

(43) Quando si tratta di informazioni personali acquisite da un altro operatore commerciale, in linea di principio il PIHBO è libero di stabilire una nuova finalità di utilizzo ([28]). Al fine di garantire che, nel caso di un trasferimento di dati dall'Unione europea, tale destinatario sia vincolato dalla finalità per la quale i dati sono stati trasferiti, la norma integrativa (3) impone che, nei casi «in cui [il PIHBO] riceva dati personali dall'UE sulla base di una decisione di adeguatezza» o tale operatore «riceva da un altro [PIHBO] dati personali trasferiti in precedenza dall'UE sulla base di una decisione di adeguatezza» (condivisione successiva), il destinatario debba «indicare la finalità d'uso di detti dati personali, che deve rientrare nell'ambito della finalità di utilizzo per la quale i dati sono stati originariamente o successivamente ricevuti». In altre parole la norma garantisce che in caso di trasferimento la finalità definita ai sensi del regolamento (UE) 2016/679 continui a determinare il trattamento e che una modifica di tale finalità in una qualsiasi fase della catena del trattamento in Giappone richieda il consenso dell'interessato dell'UE. Sebbene l'ottenimento di tale consenso preveda che il PIHBO contatti l'interessato, quando ciò non è possibile ne consegue semplicemente l'obbligo di mantenere la finalità originaria.

2.3.2. *Liceità e correttezza del trattamento*

(44) La protezione supplementare di cui al considerando 43 è tanto più pertinente in quanto il sistema giapponese assicura la liceità e la correttezza del trattamento dei dati personali anche attraverso il principio di limitazione della finalità.

(45) A norma dell'APPI, quando il PIHBO raccoglie informazioni personali deve specificarne dettagliatamente la finalità di utilizzo ([29]) e informarne prontamente l'interessato (o comunicare la finalità al pubblico) ([30]). L'articolo 17 dell'APPI stabilisce inoltre che il PIHBO non possa acquisire informazioni personali con l'inganno o altri mezzi impropri. Per quanto riguarda alcune categorie di dati, quali le informazioni personali particolarmente sensibili, la loro acquisizione richiede il consenso dell'interessato (articolo 17, comma 2, dell'APPI).

([26]) Le domande e risposte pubblicate dalla PPC contengono una serie di esempi che illustrano tale nozione. Esempi di situazioni in cui la modifica resta entro un ambito ragionevolmente pertinente includono, in particolare, l'uso di informazioni personali ottenute dagli acquirenti di merci o servizi nell'ambito di un'operazione commerciale al fine di informarli di altre merci o servizi d'interesse disponibili (ad esempio il gestore di una palestra che registra gli indirizzi di posta elettronica dei membri per informarli dei corsi e dei programmi). Allo stesso tempo le domande e risposte includono un esempio di un caso in cui la modifica della finalità di utilizzo non è consentita, ossia di una società che invia informazioni sulle merci e i servizi offerti agli indirizzi di posta elettronica che ha raccolto al fine di segnalare frodi o furti delle tessere di iscrizione.

([27]) Dette esenzioni possono risultare da altre leggi o regolamenti oppure riguardare situazioni in cui la gestione delle informazioni personali è necessaria per i) la «tutela della vita umana, dell'integrità fisica o del patrimonio», ii) «migliorare l'igiene pubblica o promuovere la crescita di bambini sani», o iii) «cooperare con le agenzie o gli organismi governativi o i loro rappresentanti» nello svolgimento dei loro compiti ufficiali. Le categorie i) e ii) si applicano soltanto se è difficile ottenere il consenso dell'interessato e la categoria iii) soltanto se vi è il rischio che l'ottenimento del consenso dell'interessato interferisca con lo svolgimento di tali compiti.

([28]) Ciò premesso, l'articolo 23, comma 1, dell'APPI stabilisce che, in linea di principio, la comunicazione di dati a un terzo richiede il consenso della persona interessata. In tal modo la persona è in grado di esercitare un certo controllo sull'uso dei propri dati da parte di un operatore economico.

([29]) Ai sensi dell'articolo 15, comma 1, dell'APPI, l'indicazione deve essere «il più esplicita possibile».

([30]) Articolo 18, comma 1, dell'APPI.

(46) Di conseguenza, come spiegato nei considerando 41 e 42, al PIHBO è fatto divieto di trattare le informazioni personali per altre finalità, ad eccezione del caso in cui l'interessato presti il proprio consenso o dell'applicazione di una delle deroghe di cui all'articolo 16, comma 3, dell'APPI.

(47) Infine, per quanto riguarda l'ulteriore trasferimento delle informazioni personali a un terzo ([31]), l'articolo 23, comma 1, dell'APPI limita tale comunicazione a casi specifici, in genere previo consenso dell'interessato ([32]). L'articolo 23, commi 2, 3 e 4, dell'APPI, stabilisce eccezioni all'obbligo di ottenere il consenso. Tuttavia le eccezioni si applicano solamente ai dati non sensibili e prevedono che l'operatore economico informi preventivamente le persone interessate dell'intenzione di comunicare a un terzo le informazioni personali che le riguardano e della possibilità di opporsi a qualsiasi ulteriore comunicazione ([33]).

(48) Per quanto riguarda i trasferimenti dall'Unione europea, i dati personali saranno stati necessariamente raccolti e trattati prima nell'UE in conformità al regolamento (UE) 2016/679. Ciò prevederà sempre, da un lato, la raccolta e il trattamento dei dati, anche per il trasferimento dall'Unione europea al Giappone, sulla base di uno dei motivi leciti elencati nell'articolo 6, paragrafo 1, del regolamento e, dall'altro, la raccolta dei dati per una finalità determinata, esplicita e legittima nonché il divieto di ulteriore trattamento, anche mediante trasferimento, con una modalità incompatibile con tale finalità come disposto dall'articolo 5, paragrafo 1, lettera b), e dall'articolo 6, paragrafo 4, del regolamento.

(49) Dopo il trasferimento, in conformità alla norma integrativa (3) il PIHBO che riceva i dati dovrà «confermare» la o le finalità determinate su cui si fonda il trasferimento (ossia la finalità determinata a norma del regolamento (UE) 2016/679) e trattare successivamente i dati in linea con tale o tali finalità ([34]). Ciò significa che la o le finalità determinate a norma del regolamento vincolano non soltanto colui che per primo ha acquisito i dati personali in Giappone ma anche i futuri destinatari di tali dati (compresi i fiduciari).

(50) Inoltre, nel caso in cui il PIHBO desideri modificare la finalità precedentemente determinata a norma del regolamento (UE) 2016/679, l'articolo 16, comma 1, dell'APPI stabilisce che, in linea di principio, debba ottenere il consenso dell'interessato. In mancanza di tale consenso qualsiasi trattamento che vada oltre l'ambito necessario al raggiungimento di tale finalità di utilizzo costituirebbe una violazione dell'articolo 16, comma 1, che può essere fatta valere dalla PPC e dagli organi giurisdizionali.

(51) Pertanto, dato che a norma del regolamento (UE) 2016/679 un trasferimento necessita di una base giuridica valida e di una finalità determinata, che siano rispecchiate nella finalità di utilizzo «confermata» in conformità all'APPI, la combinazione delle disposizioni pertinenti dell'APPI e della norma integrativa (3) assicura che la liceità del trattamento dei dati dell'UE continui anche in Giappone.

2.3.3. *Esattezza e minimizzazione dei dati*

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

(53) I principi enunciati sono garantiti nel diritto giapponese dall'articolo 16, comma 1, dell'APPI, che vieta la gestione delle informazioni personali oltre «l'ambito necessario per conseguire la finalità di utilizzo». Come spiegato dalla PPC, ciò esclude non solo l'utilizzo di dati che non siano adeguati e l'utilizzo eccessivo di dati (oltre quanto necessario al raggiungimento della finalità di utilizzo), ma comporta anche il divieto di gestire i dati non pertinenti per il raggiungimento della finalità di utilizzo.

([31]) Sebbene, ai fini dell'applicazione dell'articolo 23 (cfr. comma 5), i fiduciari siano esclusi dalla nozione di «terzo», tale esclusione si applica purché il fiduciario gestisca le informazioni personali entro i limiti dell'affidamento («nell'ambito necessario per conseguire la finalità di utilizzo»), ossia agisca in qualità di responsabile del trattamento.

([32]) Gli altri motivi (eccezionali) sono: i) la fornitura di informazioni personali «sulla base di disposizioni legislative e regolamentari», ii) casi «in cui è necessario tutelare la vita umana, l'integrità fisica o il patrimonio e quando è difficile ottenere il consenso del titolare», iii) casi «in cui è particolarmente necessario migliorare l'igiene pubblica o incoraggiare la promozione della salute dei minori e quando è difficile ottenere il consenso del titolare», iv) nei casi «in cui sia necessario cooperare con un organismo del governo centrale o un'amministrazione locale o con un soggetto da questi incaricato di svolgere attività previste da leggi e regolamenti e quando vi è la possibilità che l'ottenimento del consenso del titolare interferisca con lo svolgimento di tali attività».

([33]) Le informazioni da fornire includono, in particolare, le categorie di dati personali da condividere con un terzo e i metodi di trasmissione. Il PIHBO deve inoltre informare l'interessato della possibilità di opporsi alla trasmissione dei dati e delle modalità con cui fare opposizione.

([34]) A norma dell'articolo 26, comma 1, punto ii), dell'APPI, quando riceve dati personali da un terzo il PIHBO è tenuto a «confermare» (verificare) i «dettagli dell'acquisizione dei dati personali da parte del terzo», compresa la finalità dell'acquisizione. Sebbene l'articolo 26 non specifichi espressamente che il PIHBO debba quindi rispettare tale finalità, ciò è esplicitamente previsto dalla norma integrativa (3).

(54) Per quanto concerne l'obbligo di mantenere i dati esatti e aggiornati, l'articolo 19 dell'APPI prevede che il PIHBO «si sforzi di mantenere i dati personali esatti e aggiornati nell'ambito necessario al raggiungimento della finalità di utilizzo». Tale disposizione dovrebbe essere letta in combinato disposto con l'articolo 16, comma 1, dell'APPI. Secondo le spiegazioni ricevute dalla PPC, se il PIHBO non soddisfa i requisiti di esattezza, si riterrà che la gestione delle informazioni personali non raggiunga la finalità di utilizzo e che sia quindi illecita ai sensi dell'articolo 16, comma 1.

2.3.4. *Limitazione della conservazione*

(55) 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.

(56) Ai sensi dell'articolo 19 dell'APPI, i PIHBO sono tenuti a «adoperarsi[…] per cancellare prontamente i dati personali quando tale utilizzo non sia più necessario». Occorre leggere tale disposizione in combinato disposto con l'articolo 16, comma 1, dell'APPI che vieta la gestione delle informazioni personali oltre «l'ambito necessario per conseguire la finalità di utilizzo». Una volta raggiunta la finalità di utilizzo, il trattamento delle informazioni personali non può più considerarsi necessario e, pertanto, non può continuare (a meno che il PIHBO non ottenga il consenso dell'interessato in tal senso).

2.3.5. *Sicurezza dei dati*

(57) 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 economici dovrebbero adottare misure tecniche o organizzative per proteggere i dati personali da possibili minacce. Tali misure dovrebbero essere valutate tenendo conto dello stato dell'arte e dei costi connessi.

(58) Detto principio è attuato nel diritto giapponese dall'articolo 20 dell'APPI che stabilisce che il PIHBO «adotta le misure necessarie e appropriate per controllare la sicurezza dei dati personali, anche per prevenire le fughe o le perdite di dati personali da lui gestiti o i danni agli stessi». Gli orientamenti della PPC spiegano le misure da adottare, compresi i metodi per definire politiche di base, norme per la gestione dei dati e varie «azioni di controllo» (relative alla sicurezza organizzativa e alla sicurezza umana, fisica e tecnologica) ([35]). Gli orientamenti della PPC e l'apposita comunicazione (appendice 8 sui «Contenuti delle misure di gestione della sicurezza da adottare») pubblicati dalla PPC stabiliscono, nel quadro delle misure di gestione della sicurezza che devono adottare i PIHBO, ulteriori dettagli sulle misure in caso di incidenti di sicurezza che comportano, ad esempio, la fuga di informazioni personali ([36]).

(59) Inoltre, a norma degli articoli 20 e 21 dell'APPI, ogniqualvolta le informazioni personali sono gestite da dipendenti o subappaltatori, deve essere garantita, per motivi di controllo della sicurezza, una «supervisione necessaria e adeguata». Infine, a norma dell'articolo 83 dell'APPI, la fuga intenzionale o il furto di informazioni personali sono punibili con una pena detentiva fino a un anno.

2.3.6. *Trasparenza*

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

(61) L'articolo 18, comma 1, dell'APPI stabilisce che il PIHBO è tenuto a mettere a disposizione dell'interessato le informazioni sulla finalità di utilizzo delle informazioni personali acquisite, ad eccezione dei «casi in cui la finalità di utilizzo è stata comunicata in anticipo al pubblico». Lo stesso obbligo vale anche nel caso di una modifica lecita della finalità autorizzata (articolo 18, comma 3). In questo modo si garantisce inoltre che l'interessato sia informato anche del fatto che sono stati raccolti dati che lo riguardano. Sebbene l'APPI non preveda in genere che il PIHBO sia tenuto a informare l'interessato dei possibili destinatari delle informazioni personali al momento della raccolta, tali elementi sono una condizione necessaria per qualsiasi comunicazione successiva delle informazioni a un terzo (destinatario) sulla base dell'articolo 23, comma 2, pertanto nei casi in cui ciò avviene senza il previo consenso dell'interessato.

([35]) Orientamenti della PPC (edizione norme generali), pag. 41 e pagg. 86-98.

([36]) A norma della sezione 3-3-2 degli orientamenti della PPC, nel caso in cui si verifichino fughe, danni o perdite, il PIHBO è tenuto a svolgere le indagini necessarie e in particolare valutare l'entità della violazione dei diritti e degli interessi dell'interessato nonché la natura e la quantità delle informazioni personali in questione.

(62) Per quanto riguarda i «dati personali conservati», l'articolo 27 dell'APPI prevede che il PIHBO comunichi all'interessato la sua identità (contatti), la finalità di utilizzo e le procedure per rispondere a una richiesta concernente i diritti individuali dell'interessato ai sensi degli articoli 28, 29 e 30 dell'APPI.

(63) Ai sensi delle norme integrative i dati personali trasferiti dall'Unione europea saranno considerati «dati personali conservati» a prescindere dal loro periodo di conservazione (a meno che non rientrino nelle eccezioni) e saranno sempre soggetti agli obblighi di trasparenza previsti dalle due disposizioni summenzionate.

(64) Sia i requisiti dell'articolo 18 che l'obbligo di informare circa la finalità di utilizzo ai sensi dell'articolo 27 dell'APPI sono soggetti alle stesse eccezioni, principalmente basate su considerazioni di interesse generale e sulla tutela dei diritti e degli interessi dell'interessato, dei terzi e del titolare del trattamento ([37]). Secondo l'interpretazione elaborata negli orientamenti della PPC, tali eccezioni si applicano in situazioni molto specifiche, ad esempio nel caso in cui le informazioni sulla finalità di utilizzo rischino di compromettere le misure legittime adottate dall'operatore economico al fine di tutelare determinati interessi (ad esempio, la lotta contro le frodi, lo spionaggio industriale e il sabotaggio).

2.3.7. *Categorie particolari di dati*

(65) Garanzie specifiche dovrebbero essere applicate al trattamento di «categorie speciali di dati».

(66) Le «informazioni personali particolarmente sensibili» sono definite all'articolo 2, comma 3, dell'APPI. Tale disposizione riguarda le «informazioni personali del titolare concernenti, tra l'altro, razza, credo, status sociale, storia clinica, precedenti penali e danni subiti a causa di un reato o altre descrizioni per cui un'ordinanza del Gabinetto impone una gestione particolarmente attenta al fine di non causare ingiustamente discriminazioni, pregiudizi o altri svantaggi al titolare». Tali categorie coincidono in larga parte con quelle contenute nell'elenco dei dati sensibili di cui agli articoli 9 e 10 del regolamento (UE) 2016/679. In particolare, la «storia clinica» corrisponde ai dati sanitari mentre i «precedenti penali» e i «danni subiti a causa di un reato» sono sostanzialmente identici alle categorie di cui all'articolo 10 del regolamento (UE) 2016/679. Le categorie di cui all'articolo 2, comma 3, dell'APPI sono oggetto di ulteriore interpretazione nell'ordinanza del Gabinetto e negli orientamenti della PPC. A norma della sezione 2.3, punto 8), degli orientamenti della PPC, nell'interpretazione delle sottocategorie della «storia clinica» di cui all'articolo 2, punti ii) e iii), dell'ordinanza del Gabinetto, rientrano anche i dati genetici e biometrici. Inoltre, anche se l'elenco non contiene espressamente i termini «origine etnica» e «opinione politica», include comunque riferimenti a «razza» e «credo». Come spiegato nella sezione 2.3, punti 1) e 2), degli orientamenti della PPC, il riferimento alla «razza» riguarda «legami di tipo etnico o legami a una determinata parte del mondo» mentre nel «credo» rientrano sia la religione che le opinioni politiche.

(67) Come si evince chiaramente dal testo della disposizione, non si tratta di un elenco esaustivo, in quanto possono essere aggiunte ulteriori categorie di dati se il loro trattamento rischia di causare «ingiustamente discriminazioni, pregiudizi o altri svantaggi al titolare».

(68) Sebbene il concetto di dati «sensibili» sia di per sé un costrutto sociale, in quanto si fonda, tra l'altro, su tradizioni culturali e giuridiche, considerazioni di ordine morale e scelte politiche di una determinata società, vista l'importanza di offrire garanzie adeguate per dati sensibili in caso di trasferimento verso operatori economici in Giappone, la Commissione ha ottenuto che le tutele concesse alle «informazioni personali particolarmente sensibili» a norma della legislazione giapponese siano estese a tutte le categorie riconosciute come «dati sensibili» dal regolamento (UE) 2016/679. A tal fine, la norma integrativa (1) prevede che i dati trasferiti dall'Unione europea relativi alla vita sessuale, all'orientamento sessuale e all'appartenenza sindacale di una persona siano trattati dai «PIHBO allo stesso modo delle informazioni personali particolarmente sensibili di cui all'articolo 2, comma 3, dell'APPI».

([37]) Si tratta i) dei casi in cui la comunicazione della finalità di utilizzo all'interessato o al pubblico potrebbe «danneggiare la vita, l'integrità fisica, il patrimonio o altri diritti e interessi di un titolare o di un terzo» o «i diritti e gli interessi legittimi del […] PIHBO»; ii) dei casi in cui «è necessario cooperare con un organismo governativo centrale o un'amministrazione» nello svolgimento dei loro compiti ufficiali, e tali informazioni o la loro comunicazione potrebbe interferire con tali «attività»; iii) dei casi in cui la finalità di utilizzo è chiaramente deducibile dalla situazione in cui i dati sono stati acquisiti.

(69) Per quanto riguarda le ulteriori garanzie sostanziali che si applicano alle informazioni personali particolarmente sensibili, i PIHBO non sono autorizzati, ai sensi dell'articolo 17, comma 2, dell'APPI, ad acquisire tale tipologia di dati senza il previo consenso dell'interessato in questione, fatto salvo soltanto un numero limitato di eccezioni ([38]). Per tale categoria di informazioni personali è inoltre esclusa la possibilità di comunicazione a terzi in base alla procedura di cui all'articolo 23, comma 2, dell'APPI (che consente la trasmissione di dati a terzi senza il previo consenso dell'interessato in questione).

2.3.8. *Responsabilizzazione*

(70) Secondo il principio di responsabilizzazione, i soggetti che trattano dati sono tenuti a mettere in atto misure tecniche e organizzative adeguate per rispettare effettivamente 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.

(71) Come indicato nella nota a piè di pagina 34 (considerando 49), i PIHBO sono tenuti, ai sensi dell'articolo 26, comma 1, dell'APPI, a verificare l'identità del terzo che fornisce loro dati personali e le «circostanze» in cui i dati sono stati acquisiti dal terzo (nel caso di dati personali oggetto della presente decisione, l'APPI e la norma integrativa (3) prevedono che tali circostanze includano il fatto che i dati siano originari dell'Unione europea e la finalità della trasmissione originaria). Tale misura è intesa, tra l'altro, a garantire la liceità del trattamento lungo tutta la catena dei PIHBO che gestiscono i dati personali. Inoltre, ai sensi dell'articolo 26, comma 3, dell'APPI, i PIHBO sono tenuti a registrare la data di ricevimento e le informazioni (obbligatorie) ricevute dal terzo ai sensi del comma 1, nonché il nome della persona in questione (interessato), le categorie di dati trattati e, nella misura necessaria, il consenso dell'interessato alla condivisione dei suoi dati personali. Come specificato all'articolo 18 delle norme della PPC, tali registrazioni devono essere conservate per un periodo che va da almeno uno a tre anni, a seconda delle circostanze. Nell'esercizio delle sue funzioni, la PPC può esigere la presentazione di tali registrazioni ([39]).

(72) I PIHBO devono occuparsi prontamente e adeguatamente dei reclami presentati dalle persone interessate in merito al trattamento delle loro informazioni personali. Per agevolare la gestione dei reclami, essi istituiscono un «sistema necessario per conseguire [tale] finalità», il che implica che dovrebbero porre in essere procedure adeguate all'interno della loro organizzazione (ad esempio, per assegnare responsabilità o fornire un punto di contatto).

(73) L'APPI definisce infine un quadro per la partecipazione delle organizzazioni settoriali al fine di garantire un livello elevato di conformità (cfr. capo IV, sezione 4). Il ruolo di tali organizzazioni accreditate per la protezione delle informazioni personali ([40]) è di promuovere la protezione delle informazioni personali, mettendo le competenze di cui dispongono al servizio delle imprese, ma anche contribuendo all'attuazione di garanzie, in particolare con la gestione di singoli reclami e con il sostegno alla risoluzione dei conflitti connessi. A tal fine le organizzazioni possono chiedere ai PIHBO partecipanti, se del caso, di adottare le misure necessarie ([41]). Inoltre, in caso di violazione dei dati o altri incidenti di sicurezza, i PIHBO devono, in linea di principio, informare la PPC nonché l'interessato (o il pubblico) e adottare le misure necessarie, comprese le misure per ridurre al minimo i danni ed evitare il ripetersi di incidenti simili ([42]). Sebbene si tratti di regimi volontari, il 10 agosto 2017 la PPC aveva elencato 44 organizzazioni, di cui la più grande, *Japan Information Processing and Development Center* (JIPDEC),

([38]) Le eccezioni sono le seguenti: i) «casi fondati su disposizioni legislative e regolamentari»; ii) «casi in cui è necessario tutelare la vita umana, l'integrità fisica o il patrimonio e quando è difficile ottenere il consenso del titolare»; iii) «casi in cui è particolarmente necessario migliorare l'igiene pubblica o incoraggiare la promozione della salute dei bambini e quando è difficile ottenere il consenso del titolare»; iv) «in cui sia necessario cooperare con un organismo governativo centrale o un'amministrazione locale o con un soggetto da questi incaricato di svolgere attività previste da leggi e regolamenti e quando vi è la possibilità che l'ottenimento del consenso del titolare interferisca con lo svolgimento di tali attività»; v) i casi in cui le informazioni personali particolarmente sensibili sono comunicate al pubblico da un interessato, un'organizzazione governativa, un'amministrazione locale, una persona rientrante in una delle categorie di cui all'articolo 76, comma 1, o da altre persone previste dalle norme della PPC. Un'ulteriore categoria riguarda «gli altri casi che l'ordinanza del Gabinetto ritiene equivalenti a quelli indicati in ciascuna voce precedente» e, nell'ambito dell'attuale ordinanza del Gabinetto, concerne, in particolare, caratteristiche visibili di una persona (ad esempio, condizioni di salute visibili) nel caso in cui i dati sensibili siano stati acquisiti (involontariamente) mediante osservazione visiva, riprese video o fotografie dell'interessato, ad esempio mediante telecamere a circuito chiuso.

([39]) A norma dell'articolo 40, comma 1, dell'APPI, la PPC può, se necessario all'attuazione delle disposizioni dell'APPI, richiedere al PIHBO di presentare le informazioni o i materiali necessari concernenti la gestione delle informazioni personali.

([40]) L'APPI stabilisce, tra l'altro, norme per l'accreditamento di tali organizzazioni; cfr. articoli da 47 a 50 dell'APPI.

([41]) Articolo 52 dell'APPI.

([42]) Notifica n. 1/2017 della PPC «concernente le misure da adottare in caso di violazione di dati personali o di altro incidente».

contava da sola 15 436 operatori economici partecipanti ([43]). I regimi accreditati comprendono associazioni di settore, quali l'associazione giapponese degli operatori in titoli, l'associazione giapponese delle scuole guida o l'associazione giapponese dei mediatori di matrimoni ([44]).

(74) Le organizzazioni accreditate per la protezione delle informazioni personali presentano relazioni annuali sulle loro attività. Secondo la «Sintesi sullo stato di attuazione dell'APPI nell'esercizio finanziario 2015», pubblicato dalla PPC, le organizzazioni accreditate per la protezione delle informazioni personali hanno ricevuto un totale di 442 reclami; hanno chiesto 123 spiegazioni agli operatori economici soggetti alla loro giurisdizione; hanno chiesto a tali operatori documenti in 41 casi; hanno impartito 181 istruzioni e hanno formulato due raccomandazioni ([45]).

2.3.9. *Restrizioni ai trasferimenti successivi*

(75) Il livello di protezione offerto ai dati personali trasferiti dall'Unione europea verso gli operatori economici in Giappone non deve essere compromesso da ulteriori trasferimenti di tali dati a destinatari che si trovano in un paese terzo al di fuori del Giappone. Tali «trasferimenti successivi», che dal punto di vista dell'operatore economico giapponese costituiscono trasferimenti internazionali dal Giappone, dovrebbero essere autorizzati soltanto nel caso in cui anche il destinatario successivo al di fuori del Giappone sia soggetto a norme che garantiscono un livello di protezione analogo a quello garantito dall'ordinamento giuridico giapponese.

(76) L'articolo 24 dell'APPI prevede una prima protezione, vietando, in linea di principio, il trasferimento di dati personali a terzi al di fuori del territorio del Giappone senza il previo consenso dell'interessato. La norma integrativa (4) garantisce che tale consenso, nel caso di trasferimenti di dati dall'Unione europea, sia particolarmente ben informato, in quanto impone che all'interessato siano «fornite le informazioni sulle circostanze relative al trasferimento che sono necessarie al titolare per decidere in merito al consenso». Su tale base gli interessati sono informati del trasferimento dei dati all'estero (al di fuori dell'ambito di applicazione dell'APPI) e del paese di destinazione specifico. Ciò consentirà loro di valutare il rischio per la privacy che tale trasferimento comporta. Come si può quindi evincere dall'articolo 23 dell'APPI (cfr. considerando 47), le informazioni fornite al titolare dovrebbero riguardare gli elementi obbligatori previsti dal comma 2 del medesimo articolo, ossia le categorie di dati personali fornite a un terzo e il metodo di comunicazione.

(77) L'articolo 24 dell'APPI, in combinato disposto con l'articolo 11-2 delle norme della PPC, prevede diverse eccezioni alla regola del consenso. Inoltre, conformemente all'articolo 24, le stesse deroghe applicabili ai sensi dell'articolo 23, comma 1, dell'APPI valgono anche per i trasferimenti internazionali di dati ([46]).

(78) Per garantire la continuità di protezione nel caso dei dati personali trasferiti dall'Unione europea al Giappone nel quadro della presente decisione, la norma integrativa (4) rafforza il livello di protezione per i trasferimenti successivi di tali dati da parte dei PIHBO verso un destinatario situato in un paese terzo. A tal fine limita e inquadra le basi per i trasferimenti internazionali cui possono ricorrere i PIHBO in alternativa al consenso. Più in particolare, e fatte salve le deroghe di cui all'articolo 23, comma 1, dell'APPI, i dati personali trasferiti ai sensi della presente decisione possono essere soggetti a trasferimenti (successivi) senza consenso solo in due casi: i) se i dati sono inviati a un paese terzo che secondo la PPC fornisce, ai sensi dell'articolo 24 dell'APPI, un livello di protezione equivalente a quello garantito in Giappone ([47]); o ii) se il PIHBO e il destinatario terzo hanno attuato misure concordate che garantiscono un livello di protezione equivalente a quello dell'APPI, in combinato disposto con le norme integrative, mediante un contratto, altre forme di accordi vincolanti o modalità vincolanti stabilite all'interno di un gruppo societario. La seconda categoria corrisponde agli strumenti utilizzati a norma del regolamento (UE) 2016/679 per assicurare garanzie adeguate (in particolare, clausole contrattuali e norme vincolanti d'impresa). Inoltre, come confermato dalla PPC, persino in tali casi il trasferimento rimane soggetto alle disposizioni generali applicabili a qualsiasi fornitura di dati personali a terzi conformemente all'APPI (ossia all'obbligo di ottenere il consenso a norma dell'articolo 23, comma 1, o, in alternativa, all'obbligo di informare con possibilità di rifiuto del consenso conformemente all'articolo 23, comma 2, dell'APPI). Nel caso in cui non sia possibile

([43]) Secondo i dati pubblicati sul sito web PrivacyMark della JIPDEC, consultato il 2 ottobre 2017.

([44]) PPC, elenco delle organizzazioni accreditate per la protezione delle informazioni personali, consultabile al seguente indirizzo internet: https://www.ppc.go.jp/personal/nintei/list/ o https://www.ppc.go.jp/files/pdf/nintei_list.pdf

([45]) PPC, Sintesi sullo stato di attuazione dell'APPI nell'esercizio finanziario 2015 (ottobre 2016), consultabile (solo in giapponese) al seguente indirizzo internet: https://www.ppc.go.jp/files/pdf/personal_sekougaiyou_27ppc.pdf

([46]) Cfr. nota 32.

([47]) A norma dell'articolo 11 delle norme della PPC, ciò richiede non solo la vigenza di norme sostanziali equivalenti all'APPI effettivamente soggette alla vigilanza di un'autorità indipendente incaricata dell'esecuzione, ma anche la garanzia dell'attuazione delle norme pertinenti nel paese terzo.

contattare l'interessato per chiedergli il consenso o per fornirgli le informazioni preventive di cui all'articolo 23, comma 2, dell'APPI, il trasferimento non può aver luogo.

(79) Pertanto, al di fuori dei casi in cui la PPC ha constatato che il paese terzo garantisce un livello di protezione equivalente a quello garantito dall'APPI ([48]), le disposizioni di cui alla norma integrativa (4) escludono l'utilizzo di strumenti che non istituiscano un rapporto vincolante tra l'esportatore di dati giapponesi e l'importatore di dati del paese terzo e che non garantiscano il necessario livello di protezione. È il caso, ad esempio, del sistema di norme transfrontaliere in materia di privacy (CBPR) dell'APEC, di cui il Giappone è un'economia partecipante ([49]), in quanto in tale sistema le protezioni non risultano da un'intesa vincolante nell'ambito delle relazioni bilaterali tra l'esportatore e l'importatore e la protezione è chiaramente inferiore a quella garantita dalla combinazione dell'APPI e delle norme integrative ([50]).

(80) Infine, un'ulteriore garanzia in caso di trasferimenti (successivi) discende dagli articoli 20 e 22 dell'APPI. Secondo tali disposizioni, qualora un operatore di un paese terzo (importatore di dati) agisca per conto del PIHBO (esportatore di dati), quindi in qualità di (sub)responsabile del trattamento, il secondo deve assicurare il controllo sul primo per quanto riguarda la sicurezza del trattamento dei dati.

2.3.10. *Diritti delle persone*

(81) Analogamente alla normativa UE sulla protezione dei dati, l'APPI accorda alle persone alcuni diritti azionabili, fra cui il diritto di accesso («comunicazione»), il diritto di rettifica e il diritto di cancellazione, nonché il diritto di opposizione («cessazione dell'utilizzo»).

(82) In primo luogo, ai sensi dell'articolo 28, commi 1 e 2, dell'APPI, l'interessato ha il diritto di chiedere al PIHBO di «comunicare i dati personali conservati che possono consentirne l'identificazione»; al ricevimento di una tale richiesta, il PIHBO «[…] comunica i dati personali conservati» all'interessato. Gli articoli 29 (diritto di rettifica) e 30 (diritto di cessazione dell'utilizzo) hanno la stessa struttura dell'articolo 28.

(83) L'articolo 9 dell'ordinanza del Gabinetto specifica che la comunicazione di informazioni personali, di cui all'articolo 28, comma 2, dell'APPI, è effettuata per iscritto, a meno che il PIHBO e l'interessato non abbiano convenuto diversamente.

(84) Detti diritti sono soggetti a tre tipi di limitazioni, relative ai diritti e agli interessi della persona o dei terzi ([51]), alle gravi interferenze con l'attività commerciale del PIHBO ([52]) e ai casi in cui la comunicazione costituirebbe una violazione di altre disposizioni legislative o regolamentari ([53]). Le situazioni in cui tali limitazioni sarebbero

([48]) Ad oggi la PPC non ha ancora adottato alcuna decisione ai sensi dell'articolo 24 dell'APPI per riconoscere che un paese terzo fornisce un livello di protezione equivalente a quello garantito dal Giappone. La sola decisione che attualmente sta valutando di adottare riguarda il SEE. Per quanto riguarda eventuali altre decisioni future, la Commissione monitorerà da vicino la situazione e, se necessario, adotterà misure appropriate per eliminare eventuali effetti negativi sulla continuità della protezione (cfr. i considerando 176, 177 e 184 e l'articolo 3, paragrafo 1).

([49]) Tuttavia solo due società giapponesi sono certificate nell'ambito del sistema CBPR dell'APEC (cfr. https://english.jipdec.or.jp/sp/protection_org/cbpr/list.html). Gli unici altri operatori economici al di fuori del Giappone che sono certificati nell'ambito del sistema sono un numero limitato (23) di imprese degli Stati Uniti d'America (cfr. https://www.trustarc.com/consumer-resources/trusted-directory/#apec-list).

([50]) Mancano, ad esempio, una definizione di dati sensibili e la relativa protezione specifica, nonché l'obbligo di conservazione limitata dei dati. Cfr. Gruppo di lavoro Articolo 29, parere 02/2014 relativo a un repertorio dei requisiti relativi alle norme vincolanti di impresa presentate alle autorità nazionali di protezione dei dati dell'Unione europea e alle norme transfrontaliere in materia di privacy presentate agli agenti responsabili delle CBPR dei paesi dell'APEC, del 6 marzo 2014.

([51]) Secondo la PPC, una limitazione può essere giustificata solo da interessi «tali da meritare protezione giuridica». La valutazione a tal fine deve essere svolta caso per caso «tenendo conto dell'interferenza nel diritto fondamentale al rispetto della vita privata, compresa la protezione dei dati riconosciuta dalla costituzione e dalla giurisprudenza». Gli interessi tutelati possono includere, ad esempio, i segreti relativi agli scambi o i segreti commerciali di altra natura.

([52]) Gli orientamenti della PPC illustrano il concetto di «interferenza grave con il corretto svolgimento dell'attività dell'operatore» attraverso casi specifici, ad esempio l'invio ripetuto da parte della medesima persona di richieste complesse identiche, laddove tali richieste comportino un onere significativo per l'operatore economico tale da comprometterne la capacità di rispondere ad altre richieste (orientamenti della PPC (edizione norme generali), pag. 62). Più in generale, la PPC ha confermato che tale categoria si limita a casi eccezionali che vanno al di là di un semplice inconveniente. In particolare, il PIHBO non può rifiutare la comunicazione soltanto perché è stata richiesta una grande quantità di dati.

([53]) Come confermato dalla PPC, tali leggi devono tenere conto del diritto al rispetto della vita privata garantito dalla costituzione e quindi «rispecchiare una limitazione necessaria e ragionevole».

applicabili sono analoghe ad alcune eccezioni applicabili ai sensi dell'articolo 23, paragrafo 1, del regolamento (UE) 2016/679, che consente di limitare i diritti delle persone per motivi concernenti «la tutela dell'interessato o dei diritti e delle libertà altrui» o «altri importanti obiettivi di interesse pubblico generale». Sebbene la categoria dei casi in cui la comunicazione violerebbe «altre disposizioni legislative o regolamentari» possa apparire ampia, le leggi e i regolamenti che prevedono limitazioni a tale riguardo devono rispettare il diritto costituzionale alla riservatezza e possono imporre limitazioni solo nella misura in cui l'esercizio di tale diritto «interferisca con il benessere pubblico» ([54]). Occorre pertanto un bilanciamento degli interessi in gioco.

(85) A norma dell'articolo 28, comma 3, dell'APPI, se i dati richiesti non esistono, o se il PIHBO interessato decide di non concedere l'accesso ai dati conservati, questo è tenuto a informare la persona senza indugio.

(86) In secondo luogo, a norma dell'articolo 29, commi 1 e 2, dell'APPI, l'interessato ha il diritto di richiedere la rettifica, l'aggiunta o la cancellazione dei propri dati personali conservati qualora non siano esatti. Al ricevimento della richiesta, il PIHBO «svolge […] le indagini necessarie» e, sulla base dei risultati, «rettifica ecc. i contenuti dei dati conservati».

(87) In terzo luogo, ai sensi dell'articolo 30, commi 1 e 2, dell'APPI, l'interessato ha il diritto di chiedere al PIHBO di cessare l'utilizzo di informazioni personali o di cancellarle quando siano gestite in violazione dell'articolo 16 (sulla limitazione di finalità) o siano state acquisite indebitamente in violazione dell'articolo 17 dell'APPI (sull'acquisizione con frode o altri mezzi impropri o, in caso di dati sensibili, senza autorizzazione). Allo stesso modo, a norma dell'articolo 30, commi 3 e 4, dell'APPI, la persona ha il diritto di chiedere al PIHBO di cessare la fornitura di informazioni a terzi quando ciò viola le disposizioni dell'articolo 23, comma 1, o dell'articolo 24 dell'APPI (sulla fornitura a terzi, compresi i trasferimenti internazionali).

(88) Quando la richiesta è fondata, il PIHBO interrompe senza indugio l'utilizzo dei dati, o la loro fornitura a un terzo, nella misura necessaria per porre rimedio alla violazione o, se il caso rientra in un'eccezione (in particolare se la cessazione dell'utilizzo comportasse costi particolarmente elevati) ([55]), attua le misure alternative necessarie a tutelare i diritti e gli interessi della persona interessata.

(89) Diversamente dal diritto dell'UE, l'APPI e le pertinenti disposizioni regolamentari non contengono previsioni riguardanti specificamente la possibilità di opporsi al trattamento per finalità di marketing diretto. La presente decisione prevede tuttavia che tale trattamento avvenga nel contesto di un trasferimento di dati personali precedentemente raccolti nell'Unione europea. A norma dell'articolo 21, paragrafo 2, del regolamento (UE) 2016/679, l'interessato ha sempre la possibilità di opporsi quando i dati sono trasferiti per essere trattati per finalità di marketing diretto. Inoltre, come spiegato al considerando 43, ai sensi della norma integrativa (3) il PIHBO è tenuto a trattare i dati ricevuti a norma della presente decisione per la stessa finalità per la quale sono stati trasferiti dall'Unione europea, a meno che l'interessato non acconsenta a modificare la finalità di utilizzazione. Pertanto, se il trasferimento è stato effettuato per finalità diverse dal marketing diretto, al PIHBO in Giappone sarà vietato il trattamento dei dati a finalità di marketing diretto senza il consenso dell'interessato dell'UE.

(90) In tutti i casi di cui agli articoli 28 e 29 dell'APPI il PIHBO è tenuto a comunicare alla persona l'esito della sua richiesta senza indugio e, peraltro, a giustificare l'eventuale rifiuto (parziale) sulla base delle eccezioni di legge previste agli articoli da 27 a 30 (articolo 31 dell'APPI).

([54]) Secondo l'interpretazione della Corte suprema l'articolo 13 della costituzione prevede il diritto al rispetto della vita privata (cfr. sopra i considerando 7 e 8). Sebbene tale diritto possa essere limitato nei casi in cui «interferisce nel benessere pubblico», nella sentenza del 6 marzo 2008 (cfr. considerando 8) la Corte suprema ha chiarito che qualsiasi limitazione (che consenta, in tal caso, a un'autorità pubblica di raccogliere e trattare dati personali) deve essere valutata alla luce del diritto al rispetto della vita privata, tenendo conto di fattori quali la natura dei dati, i rischi che il trattamento dei dati crea per le persone, le garanzie applicabili e i vantaggi per il pubblico interesse derivanti dal trattamento. Si tratta di un tipo di valutazione molto simile a quella richiesta dal diritto dell'UE, basata sui principi di necessità e di proporzionalità, per l'autorizzazione di limitazioni dei diritti e delle garanzie concernenti la protezione dei dati.

([55]) Per ulteriori spiegazioni su tali eccezioni cfr. professor Katsuya Uga, «Commento articolo per articolo della nuova legge sulla protezione delle informazioni personali», 2015, pag. 217. Ad esempio, il caso di una domanda che comporta un «importo elevato di spese» si verifica quando soltanto alcuni nomi contenuti in un elenco lungo (per esempio un repertorio) sono stati trattati in violazione del principio della limitazione di finalità ma il repertorio è già in vendita, cosicché il ritiro delle copie o la loro sostituzione con nuovi esemplari risulterebbero molto costosi. Nello stesso esempio, se fossero già state vendute copie del repertorio a molte persone, non sarebbe possibile ritirarle tutte e sarebbe quindi «difficile adempiere la cessazione di utilizzo». In queste ipotesi le «misure alternative necessarie» potrebbero includere, ad esempio, la pubblicazione o la distribuzione di un avviso di rettifica. Tale azione non esclude altre forme di ricorso giurisdizionale per la violazione del diritto alla vita privata, per danni alla reputazione (diffamazione) causati dalla pubblicazione o per la violazione di altri interessi.

(91) Per quanto riguarda le condizioni per la presentazione di una richiesta, l'articolo 32 dell'APPI (in combinato disposto con l'ordinanza del Gabinetto) consente al PIHBO di determinare procedure ragionevoli, anche in termini di informazioni necessarie a identificare i dati personali conservati. Tuttavia, a norma del comma 4, del medesimo articolo, i PIHBO non devono imporre un «onere eccessivo sul titolare». In taluni casi i PIHBO possono anche imporre il pagamento di un contributo purché l'importo sia di «entità ritenuta ragionevole in considerazione dei costi reali» (articolo 33 dell'APPI).

(92) Infine la persona può opporsi alla fornitura delle proprie informazioni personali a un terzo ai sensi dell'articolo 23, comma 2, dell'APPI, o rifiutare il consenso ai sensi dell'articolo 23, comma 1 (impedendo così la comunicazione nel caso in cui non sia applicabile nessun'altra base giuridica). Analogamente la persona può impedire, a norma dell'articolo 16, comma 1, dell'APPI, il trattamento dei dati per una finalità diversa rifiutando di dare il proprio consenso.

(93) Diversamente dal diritto dell'UE, l'APPI e le pertinenti disposizioni regolamentari non contengono previsioni generali sulle decisioni riguardanti l'interessato basate unicamente sul trattamento automatizzato di dati personali. La questione è affrontata tuttavia in alcune norme settoriali applicabili in Giappone che sono particolarmente pertinenti per tale tipo di trattamento. Si tratta in particolare dei settori in cui è maggiormente probabile che le imprese ricorrano al trattamento automatizzato dei dati personali per prendere decisioni relative alle persone (ad esempio, nel settore finanziario). Ad esempio, gli «orientamenti completi per la vigilanza sulle grandi banche», riveduti nel giugno 2017, impongono che la persona riceva spiegazioni specifiche sui motivi del rifiuto della richiesta di concludere un contratto di prestito. Tali norme offrono quindi protezione nei casi, presumibilmente assai limitati, in cui un operatore economico «importatore» giapponese (invece del titolare del trattamento «esportatore» dell'UE) prenda una decisione con procedura automatizzata.

(94) In ogni caso, per quanto riguarda i dati personali raccolti nell'Unione europea, qualsiasi decisione basata sul trattamento automatizzato sarà generalmente presa dal titolare del trattamento nell'Unione (che ha un rapporto diretto con l'interessato) ed è, di conseguenza, soggetta al regolamento (UE) 2016/679 ([56]). Ciò comprende i casi di trasferimento in cui il trattamento è effettuato da un operatore economico straniero (ad esempio, giapponese) che agisce in qualità di agente (responsabile del trattamento) per conto del titolare del trattamento dell'UE (o come responsabile del trattamento in seconda battuta che agisce per conto del responsabile del trattamento dell'UE, che ha ricevuto i dati dal titolare del trattamento dell'UE che li ha raccolti) che, su questa base, prende la decisione. È pertanto improbabile che l'assenza di norme specifiche relative al processo decisionale automatizzato nell'APPI incida sul livello di protezione dei dati personali trasferiti ai sensi della presente decisione.

2.4. **Vigilanza ed esecuzione**

2.4.1. *Vigilanza indipendente*

(95) Al fine di garantire anche nella pratica un adeguato livello di protezione dei dati, 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.

(96) In Giappone l'autorità incaricata di monitorare e assicurare il rispetto dell'APPI è la PPC. Questa è composta di un presidente e otto commissari nominati dal primo ministro con il consenso delle due camere della Dieta. La durata del mandato del presidente e dei commissari è di cinque anni, con possibilità di rinnovo (articolo 64 dell'APPI). I commissari possono essere revocati solo per giusta causa in una serie limitata di circostanze eccezionali ([57]) e non devono essere impegnati attivamente in attività politiche. Conformemente all'APPI, i commissari a tempo pieno devono altresì astenersi da qualsiasi altra attività remunerata o commerciale. Tutti i commissari sono soggetti anche a norme interne che impediscono loro di partecipare alle deliberazioni in caso di un possibile conflitto di interessi. La PPC è assistita da un segretariato, diretto da un segretario generale, che è stato istituito al fine di eseguire i compiti assegnati alla PPC (articolo 70 dell'APPI). I commissari e i funzionari del segretariato sono tenuti a rispettare rigorose norme di riservatezza (articoli 72 e 82 dell'APPI).

([56]) Per contro, nel caso eccezionale in cui l'operatore giapponese abbia un rapporto diretto con l'interessato dell'UE, ciò sarà di norma una conseguenza del fatto che si sia rivolto a persone nell'Unione europea offrendo loro beni o servizi o monitorandone il comportamento. In questo scenario, l'operatore giapponese stesso rientrerà nell'ambito di applicazione dell'articolo 3, paragrafo 2, del regolamento (UE) 2016/679 ed è perciò tenuto a rispettare direttamente la normativa UE in materia protezione dei dati.

([57]) A norma dell'articolo 65 dell'APPI, un commissario può essere revocato contro la sua volontà solo per uno dei seguenti motivi: i) apertura di una procedura fallimentare; ii) condanna per violazione dell'APPI o della legge in materia di uso della numerazione; iii) condanna a una pena detentiva senza possibilità di lavoro o a una pena ancora più severa; iv) incapacità di eseguire i compiti ha causa di un disturbo mentale o fisico o di condotta irregolare.

(97) I poteri della PPC, che essa esercita in piena indipendenza ([58]), sono stabiliti soprattutto dagli articoli 40, 41 e 42 dell'APPI. Ai sensi dell'articolo 40, la PPC può chiedere al PIHBO di presentare una relazione o documentazione sulle operazioni di trattamento dei dati e può anche svolgere ispezioni, sia in loco che di registri o altri documenti. Se necessario a far rispettare l'APPI, la PPC può fornire ai PIHBO anche orientamenti o consulenza per quanto riguarda la gestione delle informazioni personali. La PPC si è già avvalsa di tale potere a norma dell'articolo 41 dell'APPI emettendo orientamenti destinati a Facebook a seguito delle rivelazioni del caso Facebook/Cambridge Analytica.

(98) Massimamente importante è il fatto che la PPC abbia il potere (a seguito di un reclamo o di propria iniziativa) di formulare, in singoli casi, raccomandazioni ed emettere ordinanze al fine di far rispettare l'APPI e le altre norme vincolanti (comprese le norme integrative). Tali poteri sono stabiliti dall'articolo 42 dell'APPI. Sebbene i commi 1 e 2 prevedano un meccanismo in due fasi per cui la PPC può emettere un'ordinanza (solo) a seguito di una precedente raccomandazione, il comma 3 consente l'adozione diretta di un'ordinanza in casi di urgenza.

(99) Anche se non tutte le disposizioni del capo IV, sezione 1, dell'APPI, sono elencate all'articolo 42, comma 1 (che stabilisce anche l'ambito di applicazione dell'articolo 42, comma 2), ciò può essere spiegato dal fatto che alcune di queste disposizioni non riguardano gli obblighi del PIHBO ([59]) e che tutte le protezioni essenziali sono già garantite da altre disposizioni incluse in tale elenco. Ad esempio, sebbene non sia menzionato l'articolo 15 (secondo il quale il PIHBO è tenuto a fissare la finalità di utilizzo delle informazioni personali e a trattarle esclusivamente in tale ambito), l'inosservanza di tale disposizione può essere motivo di una raccomandazione per violazione dell'articolo 16, comma 1 (che proibisce al PIHBO di trattare le informazioni personali al di là di quanto sia necessario a conseguire la finalità di utilizzo, a meno di non ottenere il consenso dell'interessato) ([60]). Un'altra disposizione non elencata all'articolo 42, comma 1, è l'articolo 19 dell'APPI sull'esattezza dei dati e la loro conservazione. Il mancato rispetto di tale disposizione può essere fatto valere come violazione dell'articolo 16, comma 1, o come violazione dell'articolo 29, comma 2, laddove la persona interessata chieda la rettifica o la cancellazione di dati errati o eccessivi e il PIHBO rifiuti di soddisfare tale richiesta. Quanto ai diritti dell'interessato ai sensi dell'articolo 28, comma 1, dell'articolo 29, comma 1, e dell'articolo 30, comma 1, la vigilanza della PPC è garantita conferendole poteri di esecuzione per quanto riguarda i corrispondenti obblighi del PIHBO stabiliti in tali articoli.

(100) A norma dell'articolo 42, comma 1, dell'APPI, la PPC, se ritiene che vi sia «necessità di proteggere i diritti e gli interessi di una persona nei casi in cui [il PIHBO] abbia violato» disposizioni specifiche dell'APPI, può emettere una raccomandazione al fine di «interrompere la violazione o di adottare le altre misure necessarie a porre rimedio alla violazione stessa». Tale raccomandazione non è vincolante, ma apre la strada a un'ordinanza vincolante a norma dell'articolo 42, comma 2, dell'APPI. In base a tale disposizione, se la raccomandazione non è seguita «senza motivi legittimi» e la PPC «ritiene che sia imminente una grave violazione dei diritti e degli interessi di una persona», la PPC può ordinare al PIHBO di adottare misure in linea con la raccomandazione.

(101) Le norme integrative chiariscono e rafforzano ulteriormente i poteri esecutivi della PPC. Più specificamente, nei casi riguardanti dati importati dall'Unione europea, se il PIHBO omette, senza motivo legittimo, di adottare misure per conformarsi a una raccomandazione emessa dalla PPC a norma dell'articolo 42, comma 1, dell'APPI, la PPC riterrà sempre che ciò costituisca una grave violazione di natura imminente dei diritti e degli interessi di una persona ai sensi dell'articolo 42, paragrafo 2, e, di conseguenza, una violazione che giustifica l'emissione di un'ordinanza vincolante. La PPC accetterà inoltre come «motivo legittimo» per non conformarsi a una raccomandazione esclusivamente un «evento di carattere straordinario [che impedisce di conformarsi alla raccomandazione] al di fuori del controllo [del PIHBO] che non può essere ragionevolmente previsto (ad esempio, catastrofi naturali)» o casi in cui la necessità di adottare misure riguardanti una raccomandazione «è venuta meno poiché [il PIHBO] ha adottato misure alternative che costituiscono un rimedio integrale della violazione».

([58]) Cfr. articolo 62 dell'APPI.

([59]) Ad esempio, alcune disposizioni riguardano le azioni facoltative del PIHBO (articoli 32 e 33 dell'APPI) o gli obblighi di mezzi che non sono, in quanto tali, eseguibili (articoli 31 e 35, articolo 36, comma 6, e articolo 39 dell'APPI). Talune disposizioni non sono rivolte al PIHBO ma ad altri soggetti. È questo il caso, ad esempio, dell'articolo 23, comma 4, dell'articolo 26, comma 2, e dell'articolo 34 dell'APPI (il rispetto dell'articolo 26, comma 2, dell'APPI è garantito tuttavia dalla possibilità di sanzioni penali ai sensi dell'articolo 88, punto i), dell'APPI).

([60]) Inoltre, come spiegato nel considerando 48, nel contesto di un trasferimento la finalità di utilizzo sarà indicata dall'esportatore di dati dell'UE, che, a tal riguardo, è vincolato dall'obbligo di cui all'articolo 5, paragrafo 1, lettera b), del regolamento (UE) 2016/679. Tale obbligo può essere fatto rispettare dalla competente autorità di protezione dei dati nell'Unione europea.

(102) L'inosservanza di un'ordinanza della PPC è considerata reato ai sensi dell'articolo 84 dell'APPI e, se ritenuto colpevole, il PIHBO è punito con pena detentiva con obbligo di lavoro fino a sei mesi oppure con una pena pecuniaria fino a 300 000 yen. Inoltre, ai sensi dell'articolo 85, punto i), dell'APPI, la mancanza di cooperazione con la PPC o l'intralcio delle indagini da essa condotte è punibile con una pena pecuniaria fino a 300 000 yen. Tali sanzioni penali si applicano in aggiunta a quelle che possono essere imposte per violazioni sostanziali dell'APPI (cfr. considerando 108).

2.4.2. *Ricorso giurisdizionale*

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

(104) Prima di presentare ricorso in sede amministrativa o giudiziaria, o in alternativa al ricorso, la persona può decidere di presentare reclamo per il trattamento dei propri dati personali al titolare del trattamento stesso. In conformità all'articolo 35 dell'APPI i PIHBO si adoperano a trattare tali reclami «in modo adeguato e prontamente» e a istituire sistemi interni di gestione dei reclami per conseguire tale obiettivo. Inoltre, a norma dell'articolo 61, punto ii), dell'APPI, la PPC è responsabile della «mediazione necessaria relativamente ai reclami presentati e della cooperazione offerta agli operatori commerciali che trattano i reclami», il che include, in entrambi i casi, i reclami presentati dagli stranieri. A tal proposito il legislatore ha affidato inoltre al governo centrale il compito di adottare le «misure necessarie» a consentire e ad agevolare la risoluzione dei reclami da parte dei PIHBO (articolo 9); in tali casi le amministrazioni locali devono adoperarsi ad assicurare la mediazione (articolo 13). A tale riguardo, le persone possono presentare un reclamo sia presso uno degli oltre 1 700 centri per i consumatori, istituiti dalle amministrazioni locali in base alla legge sulla sicurezza dei consumatori ([61]), che presso il Centro nazionale per gli affari dei consumatori del Giappone. I reclami possono essere presentati anche per violazione dell'APPI. A norma dell'articolo 19 della legge di base sui consumatori ([62]), le amministrazioni locali si adoperano a mediare in caso di reclami e a mettere a disposizione delle parti le competenze necessarie. Tali meccanismi di risoluzione delle controversie sembrano essere molto efficaci, con un tasso di risoluzione del 91,2 % per gli oltre 75 000 casi di reclamo del 2015.

(105) Le violazioni delle disposizioni dell'APPI da parte di un PIHBO possono dar luogo ad azioni civili e ad azioni penali con le relative sanzioni. In primo luogo, la persona che reputa violati i diritti di cui gode a norma degli articoli 28, 29 e 30 dell'APPI può chiedere al giudice un'ingiunzione che ordini al PIHBO di soddisfare la richiesta presentata ai sensi di una di tali disposizioni, ossia di comunicare i dati personali conservati (articolo 28), di rettificare i dati conservati che non sono corretti (articolo 29) o di cessare il trattamento illecito o la fornitura a terzi (articolo 30). Tale ricorso potrebbe essere proposto senza la necessità di basarsi sull'articolo 709 del codice civile ([63]) o su altre disposizioni di legge sugli illeciti civili ([64]). Ciò significa, in particolare, che la persona non ha l'onere di provare il danno.

(106) In secondo luogo, qualora una presunta violazione non riguardi diritti individuali di cui agli articoli 28, 29 e 30, bensì principi o obblighi generali del PIHBO relativi alla protezione dei dati, la persona interessata può promuovere un'azione civile nei confronti dell'operatore economico sulla base delle disposizioni sugli illeciti civili del codice civile giapponese, in particolare dell'articolo 709. Sebbene una causa ai sensi dell'articolo 709 preveda, oltre all'elemento soggettivo (dolo o colpa), una dimostrazione del danno, l'articolo 710 del codice civile dispone che tale danno possa essere sia materiale che immateriale. L'importo dell'indennizzo non è soggetto a limitazioni.

(107) Per quanto riguarda i rimedi disponibili, l'articolo 709 del codice civile fa riferimento a un risarcimento pecuniario. Secondo l'interpretazione della giurisprudenza giapponese, tale articolo conferisce tuttavia anche il diritto di ottenere un'ingiunzione ([65]). Pertanto, qualora l'interessato avvii un'azione ai sensi dell'articolo 709 del codice civile sostenendo che i suoi diritti o interessi sono stati lesi dalla violazione di una disposizione dell'APPI da parte del convenuto, tale pretesa può includere, oltre al risarcimento del danno, la richiesta di un provvedimento inibitorio, in particolare al fine di porre termine a qualsiasi trattamento illecito.

([61]) Legge n. 50 del 5 giugno 2009.
([62]) Legge n. 60 del 22 agosto 2012.
([63]) L'articolo 709 del codice civile è il principale fondamento dei contenziosi civili per il risarcimento dei danni. In base a tale disposizione «una persona che ha leso, in modo doloso o colposo, un diritto altrui o un interesse altrui giuridicamente tutelato è responsabile del risarcimento dei danni che ne conseguono».
([64]) Alta Corte di Tokyo, sentenza del 20 maggio 2015 (non pubblicata); tribunale distrettuale di Tokyo, sentenza dell'8 settembre 2014, Westlaw Japan 2014WLJPCA09088002. Cfr. anche articolo 34, commi 1 e 3, dell'APPI.
([65]) Cfr. Corte suprema, sentenza del 24 settembre 2002 (Hanrei Times vol. 1106, pag. 72).

(108) In terzo luogo, oltre ai mezzi di ricorso di diritto civile (risarcimento danni per illeciti civili), l'interessato può presentare denuncia alla magistratura o alla polizia giudiziaria per violazione dell'APPI, il che può condurre a sanzioni penali. Il capo VII dell'APPI contiene una serie di disposizioni penali. La più importante (articolo 84) riguarda il mancato rispetto da parte del PIHBO delle ordinanze della PPC a norma dell'articolo 42, commi 2 e 3. Se un operatore economico non rispetta l'ordinanza emessa dalla PPC, il presidente della PPC (nonché qualsiasi altro funzionario governativo) ([66]) può trasmettere il caso alla magistratura o alla polizia giudiziaria determinando l'avvio dell'azione penale. La violazione di un'ordinanza della PPC è punita con una pena detentiva con obbligo di lavoro fino a sei mesi o una pena pecuniaria fino a 300 000 yen. Altre disposizioni dell'APPI che prevedono sanzioni in caso di violazioni dell'APPI che ledono i diritti e gli interessi degli interessati comprendono l'articolo 83 (per quanto riguarda «la fornitura o l'uso a seguito di furto» di una banca dati di informazioni personali «al fine di trarne […] profitti illeciti») e l'articolo 88, punto i) (per quanto riguarda il mancato adempimento da parte di un terzo dell'obbligo di informare correttamente il PIHBO quando quest'ultimo riceve dati personali a norma dell'articolo 26, paragrafo 1, dell'APPI, con particolare riguardo ai dettagli delle precedenti acquisizioni di tali dati da parte del terzo medesimo). Le sanzioni applicabili a tali violazioni dell'APPI sono, rispettivamente, una pena detentiva con obbligo di lavoro fino a un anno o una pena pecuniaria fino a 500 000 yen (nel caso dell'articolo 83) o una sanzione amministrativa fino a 100 000 yen (nel caso dell'articolo 88, punto i)). Sebbene la minaccia di una sanzione penale possa già avere un forte effetto deterrente sulla direzione dell'impresa che conduce le operazioni di trattamento del PIHBO e sulle persone che gestiscono i dati, l'articolo 87 dell'APPI chiarisce che, quando un rappresentante, un dipendente o un altro collaboratore di una persona giuridica ha commesso una violazione a norma degli articoli da 83 a 85 dell'APPI,«il soggetto è punito e la sanzione stabilita negli articoli corrispondenti è inflitta a detta persona giuridica». In tal caso sia al dipendente che all'impresa possono essere imposte sanzioni fino all'intero importo massimo.

(109) Infine le persone possono anche presentare ricorso contro l'azione o l'inerzia della PPC. A tal fine la normativa giapponese prevede varie vie di ricorso in sede amministrativa e giudiziaria.

(110) La persona che non è soddisfatta della linea di azione seguita dalla PPC ha la facoltà di depositare un ricorso amministrativo ai sensi della legge per il riesame dei ricorsi amministrativi ([67]). Per contro, la persona che ritiene che la PPC sia rimasta inerte quando avrebbe invece dovuto agire può chiedere che quest'ultima, a norma dell'articolo 36-3 di tale legge, emani una disposizione o linee guida amministrative se, a suo parere, «non sono state fornite o imposte le disposizioni o linee guida amministrative necessarie alla correzione della violazione».

(111) Per quanto riguarda la possibilità di presentare ricorso giurisdizionale, ai sensi della legge in materia di contenzioso amministrativo, la persona che non è soddisfatta di una disposizione amministrativa emanata dalla PPC può avviare un'azione *mandamus* ([68]) con cui chiede all'organo giurisdizionale di ordinare alla PPC di adottare ulteriori misure ([69]). In determinati casi, l'organo giurisdizionale può emettere anche un'ordinanza *mandamus* provvisoria al fine di prevenire danni irreversibili ([70]). Ai sensi della medesima legge la persona può chiedere anche la revoca di una decisione di PPC ([71]).

(112) Una persona può infine avviare anche un'azione di risarcimento da parte dello Stato contro la PPC, a norma dell'articolo 1, comma 1, della legge sul ricorso avverso lo Stato, nel caso in cui abbia subito danni a causa di un'ordinanza illegittima emessa dalla PPC nei confronti di un operatore economico o del mancato esercizio dei propri poteri da parte della PPC.

3. ACCESSO E USO DEI DATI PERSONALI TRASFERITI DALL'UNIONE EUROPEA DA PARTE DELLE AUTORITÀ PUBBLICHE GIAPPONESI

(113) La Commissione ha valutato le limitazioni e le garanzie, compresi i meccanismi di vigilanza e di ricorso individuale disponibili nella normativa giapponese per quanto riguarda la raccolta e il successivo utilizzo dei dati personali trasferiti verso operatori economici in Giappone da parte di autorità pubbliche per motivi di interesse pubblico, in particolare per motivi di contrasto penale e di sicurezza nazionale («accesso da parte di pubbliche amministrazioni»). A tale riguardo il governo giapponese ha fornito alla Commissione le dichiarazioni, le garanzie e gli impegni ufficiali, firmati al più alto livello dei ministeri e delle agenzie, che figurano nell'allegato II della presente decisione.

([66]) Articolo 239, comma 2, del codice di procedura penale.
([67]) Legge n. 160 del 2014.
([68]) Articolo 37-2 della legge in materia di contenzioso amministrativo.
([69]) A norma dell'articolo 3, comma 6, della legge in materia di contenzioso amministrativo, per «azione *mandamus*» si intende un'azione volta a ottenere un'ordinanza dell'organo giurisdizionale nei confronti di un'agenzia amministrativa affinché questa emetta la disposizione amministrativa che avrebbe dovuto emettere in origine ma non ha emesso.
([70]) Articolo 37-5 della legge in materia di contenzioso amministrativo.
([71]) Capo II, sezione 1, della legge in materia di contenzioso amministrativo.

3.1. **Quadro giuridico generale**

(114) In quanto esercizio di pubblici poteri, in Giappone l'accesso da parte delle pubbliche amministrazioni deve essere effettuato nel pieno rispetto della legge (principio di legittimità). A tal proposito, la costituzione giapponese contiene disposizioni che limitano e inquadrano la raccolta dei dati personali da parte delle autorità pubbliche. Come già indicato relativamente al trattamento dei dati da parte di operatori economici, la Corte suprema del Giappone, basandosi sull'articolo 13 della costituzione, che tutela tra l'altro il diritto alla libertà, ha riconosciuto il diritto al rispetto della vita privata e alla protezione dei dati ([72]). Un elemento importante di tale diritto è la libertà di impedire la comunicazione delle proprie informazioni personali a terzi senza autorizzazione ([73]). Ciò implica il diritto alla protezione effettiva dei dati personali dagli abusi e (in particolare) dall'accesso illecito. Un'ulteriore protezione è garantita dall'articolo 35 della costituzione che sancisce il diritto di ognuno all'inviolabilità del domicilio, dei propri documenti e degli effetti personali, che impone alle autorità pubbliche di ottenere un mandato del giudice per un «motivo adeguato» ([74]) in tutti i casi di «perquisizioni e sequestri». Nella sentenza del 15 marzo 2017 (causa GPS) la Corte suprema ha chiarito che l'obbligo di mandato si applica ogniqualvolta il governo fa intrusione (entra) nella sfera privata in modo che la volontà della persona risulti repressa e conduce un'«indagine obbligatoria». Un giudice può emettere tale mandato soltanto sulla base di un sospetto concreto di reato, ossia quando gli siano state fornite prove documentali sulla base delle quali si può ritenere che la persona sottoposta a indagine abbia commesso un reato ([75]). Di conseguenza, le autorità giapponesi non hanno legalmente il potere di raccogliere informazioni personali con mezzi forzosi in situazioni in cui non si è ancora verificata alcuna violazione della legge ([76]), ad esempio al fine di prevenire un reato o un'altra minaccia per la sicurezza (come nel caso di indagini per motivi di sicurezza nazionale).

(115) Secondo il principio della riserva di legge, qualsiasi raccolta di dati nell'ambito di un'indagine coercitiva deve essere autorizzata specificamente dalla legge (come indicato, ad esempio, nell'articolo 197, comma 1, del codice di procedura penale in riferimento alla raccolta forzosa di informazioni a fini di indagine penale). Tale obbligo si applica anche all'accesso alle informazioni in formato elettronico.

(116) È importante osservare che l'articolo 21, comma 2, della costituzione garantisce la segretezza di tutti i mezzi di comunicazione, consentendo limitazioni solo nella normativa per motivi di interesse pubblico. L'articolo 4 della legge sulle imprese di telecomunicazione, secondo cui la segretezza delle comunicazioni gestite da un operatore di telecomunicazioni non deve essere violata, dà attuazione nella legge a tale obbligo costituzionale di riservatezza. L'obbligo è stato interpretato come un divieto di comunicazione delle informazioni sulle comunicazioni, a meno che l'utente presti il proprio consenso o in base a una delle esenzioni esplicite dalla responsabilità penale previste dal codice penale ([77]).

(117) La costituzione garantisce inoltre il diritto di accesso alla giustizia (articolo 32) e il diritto di citare in giudizio lo Stato per ottenere un risarcimento nel caso in cui una persona abbia subito danni a causa dell'atto illecito di un pubblico ufficiale (articolo 17).

(118) Per quanto riguarda in particolare il diritto alla protezione dei dati, il capo III, sezioni 1, 2 e 3, dell'APPI stabilisce principi generali relativamente a tutti i settori, compreso il settore pubblico. In particolare, l'articolo 3 dell'APPI prevede che tutte le informazioni personali debbano essere gestite in conformità al principio del rispetto della personalità delle persone. Una volta che le informazioni personali, contenute anche in registri elettronici, sono state raccolte («ottenute») dalle autorità pubbliche ([78]), la loro gestione è disciplinata dalla legge sulla protezione delle

([72]) Cfr., ad esempio, Corte suprema, sentenza del 12 settembre 2003, causa n. 1656 (2002 (Ju)). In particolare la Corte suprema ha affermato che «ognuno ha la libertà di proteggere le proprie informazioni personali dalla comunicazione a terzi o dalla divulgazione pubblica senza buona ragione».

([73]) Corte suprema, sentenza del 6 marzo 2008, (Juki-net).

([74]) Un «motivo adeguato» sussiste soltanto laddove si ritenga che la persona (indagato, imputato) abbia commesso un reato e che la perquisizione e il sequestro siano necessari per l'indagine penale. Cfr. Corte suprema, sentenza del 18 marzo 1969, causa n. 100 (1968 (Shi)).

([75]) Cfr. articolo 156, comma 1, delle norme di procedura penale.

([76]) Va osservato, tuttavia, che la legge sulla repressione della criminalità organizzata e il controllo dei proventi della criminalità del 15 giugno 2017 istituisce il nuovo reato di preparazione di atti di terrorismo e di altre forme di criminalità organizzata. Le indagini possono essere avviate soltanto in caso di sospetto concreto, basato su prove, che siano presenti tutti e tre gli elementi costitutivi del reato («coinvolgimento di un gruppo criminale organizzato», «azione di pianificazione» e «azione di preparazione per la messa in pratica del reato»). Cfr., ad esempio, anche gli articoli da 38 a 40 della legge sulla prevenzione delle attività sovversive (legge n. 240 del 21 luglio 1952).

([77]) Articolo 15, comma 8, degli orientamenti sulla protezione delle informazioni personali nel settore delle telecomunicazioni.

([78]) Organi amministrativi quali definiti all'articolo 2, comma 1, dell'APPIHAO. In base alle informazioni trasmesse dal governo giapponese, tutte le autorità pubbliche, ad eccezione della polizia prefetturale, rientrano nella nozione di «organi amministrativi». La polizia prefetturale opera tuttavia nel quadro giuridico fissato dalle ordinanze prefetturali sulla protezione delle informazioni personali (cfr. articolo 11 dell'APPI e politica di base) che stabiliscono disposizioni per la protezione delle informazioni personali equivalenti a quelle dell'APPIHAO. Cfr. allegato II, sez. I.B. Come spiegato dalla PPC, secondo la «politica di base» tali ordinanze devono essere adottate sulla base del contenuto dell'APPIHAO e il MIC emette comunicazioni al fine di impartire alle amministrazioni locali le istruzioni necessarie al riguardo. Come sottolineato dalla PPC «[e]ntro tali limiti si dovrà emettere, in ciascuna prefettura, un'ordinanza in materia di protezione delle informazioni personali […] basata sulla politica di base e sul contenuto delle comunicazioni».

informazioni personali detenute da organi amministrativi («APPIHAO») ([79]). Ciò comprende ([80]), in linea di principio, anche il trattamento delle informazioni personali per motivi di contrasto penale o di sicurezza nazionale. L'APPIHAO prevede, tra l'altro, che le autorità pubbliche: i) possano conservare le informazioni personali solo se è necessario allo svolgimento delle loro funzioni; ii) non usino tali informazioni per una finalità «ingiusta» né le comunichino a terzi senza giustificazione; iii) specifichino la finalità e non la modifichino al di là di quanto possa essere considerato ragionevolmente pertinente per la finalità originaria (limitazione delle finalità); iv) in linea di principio, non usino né forniscano a terzi le informazioni personali conservate per altre finalità e, qualora lo ritengano necessario, impongano restrizioni alla finalità o alla modalità di utilizzo da parte di terzi; v) si adoperino per garantire la correttezza delle informazioni (qualità dei dati); vi) adottino le misure necessarie per la corretta gestione delle informazioni e per prevenire fughe, perdite o danni (sicurezza dei dati); vii) si adoperino per elaborare in modo corretto e rapido gli eventuali reclami concernenti il trattamento delle informazioni ([81]).

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

(119) La normativa giapponese prevede una serie di limitazioni all'accesso e all'uso dei dati personali per motivi di contrasto penale, così come meccanismi di vigilanza e di ricorso, tali da costituire garanzie sufficienti che permettono di proteggere efficacemente detti dati dall'ingerenza illecita e dal rischio di abusi.

3.2.1. *Base giuridica e limitazioni/garanzie applicabili*

(120) Il quadro giuridico giapponese prevede che la raccolta di informazioni in formato elettronico per motivi di contrasto penale è ammissibile sulla base di un mandato (raccolta obbligatoria) o di una richiesta di comunicazione volontaria.

3.2.1.1. Indagine obbligatoria sulla base di un mandato del giudice

(121) Come indicato al considerando 115, la raccolta di dati nell'ambito di un'indagine coercitiva deve essere autorizzata specificamente dalla normativa e può essere effettuata solo sulla base di un mandato del giudice «emesso per un motivo adeguato» (articolo 35 della costituzione). Per quanto riguarda l'indagine sui reati, tale obbligo si rispecchia nelle disposizioni del codice di procedura penale. A norma dell'articolo 197, comma 1, del codice di procedura penale, le misure obbligatorie «non si applicano a meno che il presente codice non preveda disposizioni speciali». Per quanto riguarda la raccolta di informazioni in formato elettronico, le uniche basi giuridiche ([82]) pertinenti sono l'articolo 218 del codice di procedura penale (perquisizioni e sequestri) e articolo 222-2 del codice di procedura penale, secondo il quale le misure obbligatorie per l'intercettazione delle comunicazioni elettroniche senza il consenso di una delle parti sono eseguite sulla base di altre leggi, in particolare della legge sulle intercettazioni delle comunicazioni ai fini delle indagini giudiziarie («legge sulle intercettazioni»). In entrambi i casi vige l'obbligo di mandato.

(122) Più specificamente, a norma dell'articolo 218, comma 1, del codice di procedura penale, un pubblico ministero, un assistente di un pubblico ministero o un ufficiale di polizia giudiziaria possono, se necessario ai fini dell'indagine sul reato, effettuare una perquisizione o un sequestro (anche ordinando registrazioni) in base a un mandato precedentemente emesso da un giudice ([83]). Tale mandato deve contenere, tra l'altro, il nome dell'indagato o dell'imputato, l'imputazione ([84]), le registrazioni elettromagnetiche da sequestrare e il «luogo o gli elementi» da ispezionare (articolo 219, comma 1, del codice di procedura penale).

([79]) Le informazioni personali ottenute dagli operatori di un organo amministrativo nell'esercizio delle loro funzioni e detenute da detto organo amministrativo a uso organizzativo rientrano nella definizione di «informazioni personali conservate», ai sensi dell'articolo 2, comma 3, dell'APPIHAO, purché siano registrate in «documenti amministrativi». Sono incluse le informazioni in formato elettronico raccolte e successivamente trattate da tali organi, in quanto la definizione di «documenti amministrativi» di cui all'articolo 2, comma 2, della legge sull'accesso alle informazioni detenute da organi amministrativi (legge n. 42 del 1999) comprende i dati elettromagnetici.

([80]) Tuttavia, a norma dell'articolo 53-2 del codice di procedura penale, il capo IV dell'APPIHAO è escluso per i «documenti relativi ai processi»; secondo le informazioni ricevute sono incluse le informazioni in formato elettronico ottenute sulla base di un mandato o di una richiesta di collaborazione volontaria nell'ambito di un'indagine penale. Allo stesso modo, per quanto riguarda le informazioni raccolte nel settore della sicurezza nazionale, le persone non possono far valere i diritti di cui all'APPIHAO se il responsabile dell'autorità pubblica ha «fondati motivi» di ritenere che la comunicazione «possa causare danni alla sicurezza nazionale» (cfr. articolo 14, punto iv)). Detto ciò, le autorità pubbliche sono tenute a concedere la comunicazione almeno parziale ogniqualvolta sia possibile (articolo 15).

([81]) Cfr. i riferimenti specifici all'APPIHAO nell'allegato II, sez. II.A.1), lettera b), punto 2.

([82]) Sebbene l'articolo 220 del codice di procedura penale autorizzi perquisizioni e sequestri «in loco» senza mandato allorché un pubblico ministero, l'assistente di un pubblico ministero o un ufficiale di polizia giudiziaria arresti un indagato/un trasgressore in flagranza di reato, ciò non si applica nel contesto di un trasferimento né quindi ai fini della presente decisione.

([83]) In conformità all'articolo 222, comma 1, in combinato disposto con l'articolo 110 del codice di procedura penale, il mandato di perquisizione/sequestro relativo alle registrazioni deve essere mostrato alla persona soggetta alla misura.

([84]) Cfr. anche articolo 189, comma 2, del codice di procedura penale, secondo il quale un ufficiale di polizia giudiziaria indaga sull'autore di un reato e cerca le relative prove «quando ritiene che sia stato commesso un reato». Analogamente, l'articolo 155, comma 1, delle norme di procedura penale, dispone che una richiesta scritta di mandato contenga, tra l'altro l'"imputazione" e una «sintesi dei fatti del reato».

(123) Per quanto riguarda l'intercettazione delle comunicazioni, l'articolo 3 della legge sulle intercettazioni la autorizza solo nel rispetto di rigorose condizioni. In particolare, le autorità pubbliche devono ottenere preventivamente un mandato del giudice che può essere emesso solo per l'indagine su gravi reati specifici (elencati nell'allegato della legge) ([85]) e quando è «estremamente difficile individuare l'autore del reato o chiarire le situazioni/i dettagli della perpetrazione in altro modo» ([86]). Ai sensi dell'articolo 5 della legge sulle intercettazioni, il mandato è emesso per un periodo di tempo limitato e il giudice può imporre condizioni aggiuntive. La legge sulle intercettazioni prevede inoltre una serie di ulteriori garanzie, quali la presenza necessaria di testimoni (articoli 12 e 20), il divieto di intercettare le comunicazioni di determinati gruppi tutelati dal segreto professionale (ad esempio medici e avvocati) (articolo 15), l'obbligo di porre fine alle intercettazioni non più giustificate, anche durante il periodo di validità del mandato (articolo 18), o l'obbligo generale di informare la persona interessata e consentirle l'accesso alle registrazioni entro trenta giorni dalla fine delle intercettazioni (articoli 23 e 24).

(124) Per tutte le misure obbligatorie basate su un mandato, si può ricorrere soltanto a detto mezzo di ricerca delle prove «per quanto necessario al conseguimento dell'obiettivo» (articolo 197, comma 1, del codice di procedure penale) (vale a dire nel caso in cui gli obiettivi perseguiti con l'indagine non possano essere conseguiti in altro modo). Sebbene i criteri per determinare la necessità non siano ulteriormente specificati dalla legge, la Corte suprema del Giappone ha stabilito che il giudice che emette il mandato debba effettuare una valutazione complessiva tenendo conto, in particolare, i) della gravità del reato e delle circostanze nelle quali è stato commesso; ii) del valore e dell'importanza dei materiali da sequestrare quali elementi di prova; iii) della probabilità (rischio) che gli elementi di prova siano occultati o distrutti; e iv) della misura in cui il sequestro può causare pregiudizio alla persona interessata ([87]).

3.2.1.2. Richiesta di comunicazione volontaria basata su un «modulo di richiesta»

(125) Nei limiti delle loro competenze le autorità pubbliche possono raccogliere informazioni in formato elettronico sulla base delle richieste di comunicazione volontaria. Si tratta di una forma di cooperazione non obbligatoria in cui l'adempimento della richiesta non può essere imposto ([88]); le autorità pubbliche sono pertanto sollevate dall'obbligo di ottenere il mandato dell'autorità giudiziaria.

(126) Se tale richiesta è rivolta a un operatore economico e riguarda informazioni personali, l'operatore economico deve ottemperare agli obblighi dell'APPI. Ai sensi dell'articolo 23, comma 1, dell'APPI, gli operatori economici possono comunicare le informazioni personali a terzi senza il consenso della persona interessata solo in determinati casi, ad esempio quando la comunicazione è «basata su disposizioni legislative e regolamentari» ([89]). Nel settore del contrasto penale la base giuridica di dette richieste è costituita dall'articolo 197, comma 2, del codice di procedura penale, a norma del quale «alle organizzazioni private può essere richiesto di riferire su questioni necessarie all'indagine». Poiché è ammissibile soltanto nell'ambito di un'indagine penale, tale «modulo di richiesta» presuppone sempre l'esistenza di un sospetto concreto riguardo a un reato già commesso ([90]). Inoltre, siccome tali indagini sono generalmente svolte dalla polizia prefetturale, si applicano le limitazioni di cui all'articolo 2, comma 2, della legge sulla polizia ([91]), in base al quale le attività di polizia sono «rigorosamente limitate» all'adempimento delle responsabilità e delle funzioni della polizia stessa (vale a dire la prevenzione, la repressione e l'investigazione di reati). Nell'esecuzione dei propri compiti la polizia agisce inoltre in modo imparziale, equo e scevro da pregiudizi e non deve abusare mai dei propri poteri «interferendo così con i diritti e le libertà della persona garantiti dalla costituzione del Giappone» (che comprendono, come già indicato, il diritto al rispetto della vita privata e alla protezione dei dati) ([92]).

(127) Con particolare riferimento all'articolo 197, comma 2, del codice di procedura penale, l'Agenzia nazionale di polizia (NPA) – in qualità di autorità federale incaricata, tra l'altro, di tutte le questioni concernenti la polizia

([85]) L'allegato fa riferimento a 9 tipi di reati, ad esempio i reati concernenti droga e armi da fuoco, la tratta di esseri umani e l'omicidio organizzato. Si noti che il reato di recente introduzione di «preparazione di atti di terrorismo e di altri crimini organizzati» (cfr. nota a piè di pagina 76) non è incluso in questo elenco restrittivo.

([86]) Inoltre, in conformità all'articolo 23 della legge sulle intercettazioni, l'autorità inquirente è tenuta a informare per iscritto la persona le cui comunicazioni sono intercettate (e pertanto incluse nel verbale d'intercettazione).

([87]) Cfr. allegato II, sez. II.A.1), lettera b), punto 1.

([88]) In base alle informazioni ricevute gli operatori economici che non cooperano non subiscono conseguenze negative (neppure sanzioni) ai sensi di legge. Cfr. allegato II, sez. II.A.2), lettera a).

([89]) Secondo gli orientamenti della PPC (edizione norme generali), l'articolo 23, comma 1, punto i), fornisce la base per la comunicazione di informazioni personali in risposta sia a un mandato (articolo 218 del codice di procedura penale) che a un «modulo di richiesta» (articolo 197, comma 2, del codice di procedura penale).

([90]) Ciò significa che il «modulo di richiesta» può essere usato solamente per raccogliere informazioni in singoli casi e non per raccogliere dati personali su larga scala. Cfr. anche allegato II, sez. I.A.2), lettera b), punto 1.

([91]) Oltre ai regolamenti della Commissione prefetturale di pubblica sicurezza, cfr. articolo 189, comma 1, del codice di procedura penale.

([92]) Cfr. anche l'articolo 3 della legge sulla polizia, in base al quale risulta che il giuramento prestato da tutti gli operatori di polizia è di «essere fedele all'obbligo di difendere e rispettare la costituzione e le leggi del Giappone, e svolgere le proprie funzioni in modo imparziale, giusto, equo e scevro da pregiudizi».

giudiziaria – ha impartito direttive alla polizia prefetturale ([93]) sul «buon uso delle richieste di informazioni scritte nelle indagini». In base a tale comunicazione le richieste devono essere presentate utilizzando un modulo prestabilito («modulo n. 49» o il cosiddetto «modulo di richiesta») ([94]) e devono riguardare i documenti «relativi a un'indagine specifica», e le informazioni richieste devono essere «necessarie per l'indagine [in questione]». Per ogni caso l'investigatore capo «svolge un esame completo, tra l'altro, della necessità e del contenuto della singola richiesta» e deve ricevere l'approvazione interna da un funzionario di alto grado.

(128) In due sentenze del 1969 e del 2008 ([95]) la Corte suprema del Giappone ha stabilito limitazioni relative alle misure non obbligatorie che interferiscono con il diritto alla vita privata ([96]). In particolare la Corte ha affermato che tali misure devono essere «ragionevoli» e mantenersi entro «limiti generalmente ammissibili», ossia esse devono essere necessarie alle indagini su un indagato (raccolta degli elementi di prova) e devono essere svolte «con metodi adeguati al conseguimento della finalità dell'indagine» ([97]). Le sentenze dimostrano che ciò comporta un controllo di proporzionalità che tiene conto di tutte le circostanze del caso (ad esempio, il livello di interferenza con il diritto al rispetto della vita privata, comprese, tra l'altro, le aspettative in tal senso, la gravità del reato, la probabilità di ottenere elementi di prova utili, l'importanza di tali elementi probatori, eventuali modalità alternative di indagine) ([98]).

(129) Oltre alle limitazioni all'esercizio dell'autorità pubblica, gli operatori economici stessi sono tenuti a verificare («confermare») la necessità e la «razionalità» della fornitura di dati a un terzo ([99]). A tal proposito essi devono stabilire se la legge vieti loro di collaborare. Tali obblighi giuridici contrastanti possono essere dovuti, in particolare, a obblighi di riservatezza, come l'articolo 134 del codice penale (concernente il rapporto, ad esempio, tra un medico, un avvocato o un prete e il rispettivo paziente, cliente o parrocchiano). Inoltre «chiunque sia attivo nel settore delle telecomunicazioni è tenuto, durante la propria attività, a mantenere i segreti altrui di cui sia venuto a conoscenza nell'ambito delle comunicazioni gestite dall'operatore di telecomunicazioni» (articolo 4, comma 2, della legge sulle imprese di telecomunicazione). Tale obbligo è sostenuto dalla sanzione prevista dall'articolo 179 della legge sulle imprese di telecomunicazione, secondo cui chiunque abbia violato la segretezza delle comunicazioni gestite da un operatore di telecomunicazioni è colpevole di un reato ed è punito con una pena detentiva con obbligo di lavoro fino a due anni o con una pena pecuniaria non superiore a un milione di yen ([100]). Sebbene tale obbligo non sia assoluto e consenta, in particolare, misure che violano la segretezza delle comunicazioni che costituiscono «atti giustificabili» ai sensi dell'articolo 35 del codice penale, tale eccezione non copre la risposta alle richieste non obbligatorie delle autorità pubbliche relative alla comunicazione di informazioni in formato elettronico a norma dell'articolo 197, comma 2, del codice di procedura penale ([101]).

3.2.1.3. Ulteriore utilizzo delle informazioni raccolte

(130) Al momento della raccolta da parte delle autorità pubbliche giapponesi le informazioni personali rientrano nell'ambito di applicazione dell'APPIHAO. Tale legge disciplina la gestione (trattamento) delle «informazioni personali

([93]) A norma dell'articolo 30, comma 1, e dell'articolo 31, comma 2, della legge sulla polizia, il direttore generale degli uffici regionali di polizia (sedi locali dell'NPA) «dirige e controlla» la polizia prefetturale.

([94]) Il modulo di richiesta deve specificare anche le informazioni di contatto dell'«addetto alla gestione» (quali «denominazione della sezione [posizione], nome dell'addetto alla gestione, numero di telefono dell'ufficio, numero interno»).

([95]) Corte suprema, sentenza del 24 dicembre 1969, (1965(A) 1187); sentenza del 15 aprile 2008, (2007(A) 839).

([96]) Sebbene dette sentenze non riguardassero la raccolta di informazioni in formato elettronico, il governo giapponese ha chiarito che l'applicazione dei criteri elaborati dalla Corte suprema include qualsiasi ingerenza da parte delle autorità pubbliche nel diritto al rispetto della vita privata, compresi tutti i «mezzi di indagine volontari» e, di conseguenza, i criteri vincolano le autorità giapponesi anche al momento della formulazione delle richieste di comunicazione volontaria di informazioni. Cfr. allegato II, sez. II.A.2), lettera b), punto 1.

([97]) In base alle informazioni ricevute detti fattori devono considerarsi «ragionevoli secondo le convenzioni socialmente accettate». Cfr. allegato II, sez. II.A.2), lettera b), punto 1.

([98]) Per considerazioni analoghe nel contesto delle indagini obbligatorie (intercettazioni) cfr. anche Corte suprema, sentenza del 16 dicembre 1999, 1997 (A) 636.

([99]) A tale riguardo, le autorità giapponesi hanno segnalato gli orientamenti della PPC (edizione norme generali) e il punto 5/14 della «Domande e risposte» elaborate dalla PPC per l'applicazione dell'APPI. Secondo le autorità giapponesi, «data la crescente consapevolezza delle persone per quanto riguarda i loro diritti relativi alla vita privata, nonché il carico di lavoro generato da tali richieste, gli operatori economici sono sempre più prudenti nel rispondere a tali richieste». Cfr. allegato II, sez. II.A.2), anche in riferimento alla comunicazione 1999 dell'NPA. In base alle informazioni ricevute, in alcuni casi gli operatori hanno rifiutato in effetti di collaborare. Ad esempio, nella relazione sulla trasparenza del 2017, LINE (l'applicazione di messaggistica più diffusa in Giappone) afferma quanto segue: «Quando riceviamo richieste delle agenzie incaricate delle indagini, ecc., […] ne verifichiamo l'adeguatezza sotto il profilo della legalità, della protezione degli utenti, ecc. A seguito di tale verifica rifiutiamo la richiesta se presenta lacune giuridiche. Se il campo coperto della richiesta è troppo ampio ai fini dell'indagine, chiediamo spiegazioni all'agenzia incaricata delle indagini. Se la spiegazione non è motivata, non rispondiamo». Consultabile sul sito internet: https://linecorp.com/en/security/transparency/top

([100]) Le sanzioni sono una pena detentiva di 3 anni con obbligo di lavoro o una pena pecuniaria di importo non superiore a 2 milioni di yen per chiunque «operi nel settore delle telecomunicazioni».

([101]) Ai sensi del codice penale per «atti giustificabili» si intendono, in particolare, gli atti di un operatore di telecomunicazioni mediante i quali egli si conforma alle misure dello Stato che hanno forza giuridica (misure obbligatorie), ad esempio quando le autorità investigative adottano misure sulla base del mandato di un giudice. Cfr. allegato II, sez. II.A.2), lettera b), punto 2, per quanto riguarda gli orientamenti sulla protezione delle informazioni personali nel settore delle telecomunicazioni.

conservate» e impone in proposito una serie di limitazioni e garanzie (cfr. considerando 118) ([102]). Inoltre anche il fatto che un organo amministrativo possa conservare informazioni personali «solo quando la conservazione sia necessaria a svolgere attività di sua competenza previste da disposizioni legislative e regolamentari» (articolo 3, comma 1, dell'APPIHAO) impone restrizioni – almeno indirettamente – alla raccolta iniziale.

3.2.2. *Vigilanza indipendente*

(131) In Giappone la raccolta di informazioni in formato elettronico nel settore del contrasto penale rientra principalmente ([103]) tra le responsabilità della polizia prefetturale ([104]), che a tal proposito è soggetta a diversi livelli di vigilanza.

(132) In primo luogo, in tutti i casi in cui le informazioni in formato elettronico sono raccolte con mezzi coattivi di ricerca della prova (perquisizioni e sequestri), la polizia deve ottenere preventivamente un mandato del giudice (cfr. considerando 121). In tali casi, pertanto, la raccolta sarà controllata ex ante da un giudice che si atterrà rigidamente al criterio del «motivo adeguato».

(133) Sebbene non vi sia una verifica *ex ante* del giudice in caso di richieste di comunicazione volontaria, gli operatori economici cui sono rivolte tali richieste possono opporvisi senza incorrere in conseguenze negative (e devono tenere conto dell'impatto dell'eventuale comunicazione sulla privacy). Inoltre, a norma dell'articolo 192, comma 1, del codice di procedura penale, agli operatori di polizia devono sempre cooperare e coordinare le proprie azioni con il pubblico ministero (e la Commissione prefetturale per la sicurezza pubblica) ([105]). Il pubblico ministero, a sua volta, può impartire le istruzioni generali necessarie per proseguire l'indagine in modo equo e/o emettere ordinanze specifiche con riferimento a una singola indagine (articolo 193 del codice di procedure penale). Qualora tali istruzioni e/o ordinanze non siano rispettate, la procura può chiedere l'avvio di un'azione disciplinare (articolo 194 del codice di procedura penale). Di conseguenza, la polizia prefetturale opera sotto la supervisione del pubblico ministero.

(134) In secondo luogo, a norma dell'articolo 62 della costituzione, ciascuna camera del parlamento giapponese (la Dieta) può svolgere indagini nei confronti del governo, anche per quanto riguarda la legittimità della raccolta di informazioni da parte della polizia. A tal fine, può chiedere la presenza e la deposizione di testimoni e/o la presentazione di documenti. Tali poteri di indagine sono precisati ulteriormente nella legge sulla Dieta, in particolare al capo XII. In particolare, l'articolo 104 di detta legge stabilisce che il Gabinetto, le agenzie pubbliche e gli altri organi del governo «devono ottemperare alla richiesta di una delle camere o di una delle sue commissioni di presentare le relazioni e i dati necessari ai fini dell'esame dell'indagine». Il rifiuto di ottemperare alla richiesta è consentito soltanto se il governo fornisce un motivo plausibile ritenuto accettabile dalla Dieta o a seguito di una dichiarazione formale secondo la quale la presentazione delle relazioni o dei dati arrecherebbe «un grave pregiudizio all'interesse nazionale» ([106]). Inoltre i membri della Dieta possono presentare interrogazioni scritte al Gabinetto (articoli 74 e 75 della legge sulla Dieta) e in passato tali «richieste scritte» hanno riguardato anche la gestione di informazioni personali da parte dell'amministrazione ([107]). Il ruolo di supervisione dell'esecutivo di cui è investita la Dieta è rafforzato da obblighi di rendicontazione, ad esempio, ai sensi dell'articolo 29 della legge sulle intercettazioni.

(135) In terzo luogo, la polizia prefetturale è soggetta a vigilanza indipendente anche all'interno dell'esecutivo, in particolare, attraverso le Commissioni prefetturali di pubblica sicurezza, istituite a livello prefetturale per garantire l'amministrazione democratica e la neutralità politica della polizia ([108]). Tali commissioni sono composte di membri nominati dal governatore prefetturale con il consenso dell'assemblea prefetturale (tra i cittadini che non siano stati dipendenti pubblici del servizio di polizia nei cinque anni precedenti) e hanno un mandato garantito (che prevede, in particolare, soltanto la destituzione per giusta causa) ([109]). In base alle informazioni fornite, le commissioni non ricevono istruzioni e possono quindi essere considerate pienamente indipendenti ([110]). Per quanto

([102]) Per quanto riguarda i diritti delle persone interessate, cfr. sezione 3.1.

([103]) In linea di principio un pubblico ministero – o un suo assistente ai suoi ordini – può, se lo ritiene necessario, condurre indagini su un reato (articolo 191, comma 1, del codice di procedura penale).

([104]) In base alle informazioni ricevute, l'Agenzia nazionale di polizia non effettua singole indagini penali. Cfr. allegato II, sez. II.A.1), lettera a).

([105]) Cfr. anche l'articolo 246 del codice di procedura penale, secondo il quale la polizia giudiziaria è tenuta a trasmettere il fascicolo al pubblico ministero una volta che abbia condotto un'indagine su un reato («Principio di invio per tutti i casi»).

([106]) In alternativa la Dieta può chiedere che il Consiglio di vigilanza e revisione dei segreti specialmente designati conduca un'indagine in merito al rifiuto di rispondere. Cfr. articolo 104-II della legge sulla Dieta.

([107]) Cfr. allegato II, sez. II.B.4).

([108]) Inoltre, secondo le disposizioni dell'articolo 100 della legge sulle autonomie locali, l'assemblea locale ha il potere di svolgere indagini sulle attività delle autorità di contrasto istituite a livello prefetturale, compresa la polizia prefetturale.

([109]) Cfr. articoli da 39 a 41 della legge sulla polizia. Per quanto riguarda la neutralità politica, cfr. anche l'articolo 42 della legge sulla polizia.

([110]) Cfr. allegato II, sez. II.B.3) («sistema di consiglio indipendente»)

riguarda i compiti e i poteri delle Commissioni prefetturali di sicurezza pubblica, a norma dell'articolo 38, comma 3, in combinato disposto con l'articolo 2 e l'articolo 36, comma 2, della legge sulla polizia, queste sono responsabili della «protezione [dei] diritti e della libertà delle persone». A tal fine esse sono autorizzate a «controllare» ([111]) tutte le attività di indagine della polizia prefetturale, compresa la raccolta di dati personali. In particolare le commissioni «possono, se necessario, dirigere la polizia prefetturale in dettaglio o in singoli casi specifici di indagine sulla condotta irregolare del personale di polizia» ([112]). Quando riceve tali istruzioni o si rende conto in prima persona di un eventuale caso di condotta irregolare (compresa la violazione di leggi o altre negligenze dei propri doveri), il direttore della polizia prefetturale ([113]) è tenuto a indagare senza indugio sul caso e a riferire i risultati dell'indagine alla Commissione prefetturale di pubblica sicurezza (articolo 56, comma 3, della legge sulla polizia). Nei casi in cui quest'ultima lo ritenga necessario può anche nominare uno dei suoi membri affinché esamini l'avanzamento dell'esecuzione. Il procedimento continua fino a quando la Commissione prefetturale di pubblica sicurezza constati che l'incidente è stato risolto in modo appropriato.

(136) Inoltre, per quanto riguarda la corretta applicazione dell'APPIHAO, ha poteri di esecuzione della legge il ministro competente o il direttore dell'agenzia (ossia il commissario generale dell'NPA), sotto la supervisione del ministero dell'Interno e delle comunicazioni (MIC). Ai sensi dell'articolo 49 dell'APPIHAO il MIC «può raccogliere relazioni sullo stato di esecuzione della presente legge» dai direttori degli organi amministrativi (ministro). Per la funzione di vigilanza il MIC è aiutato dalle informazioni comunicate dai 51 «centri di informazione globale» (di cui uno in ciascuna prefettura in tutto il Giappone) che trattano ogni anno migliaia di richieste provenienti da persone ([114]) (che, a loro volta, possono rivelare possibili violazioni della legge). Qualora lo ritenga necessario per garantire il rispetto della legge, il MIC può chiedere di presentare spiegazioni e materiali e può formulare pareri riguardanti la gestione di informazioni personali da parte dell'organo amministrativo interessato (articoli 50 e 51 dell'APPIHAO).

3.2.3. *Ricorso individuale*

(137) Oltre alla vigilanza d'ufficio, le persone hanno diverse possibilità di ricorso, sia presso le autorità indipendenti (come le Commissioni prefetturali di pubblica sicurezza o la PPC) che presso gli organi giurisdizionali giapponesi.

(138) In primo luogo, per quanto riguarda le informazioni personali raccolte da organi amministrativi, questi sono tenuti ad «adoperarsi a trattare in modo corretto e rapido tutti i reclami» concernenti il successivo trattamento (articolo 48 dell'APPIHAO). Sebbene il capo IV dell'APPIHAO sui diritti individuali non sia applicabile alle informazioni personali registrate in «documenti relativi ai processi e ai beni sequestrati» (articolo 53-2, comma 2, della codice di procedura penale), che comprendono anche le informazioni personali raccolte nell'ambito di indagini penali, le persone possono presentare un reclamo sulla base dei principi generali della protezione dei dati, quali, ad esempio, l'obbligo di conservare le informazioni personali soltanto «quando la conservazione è necessaria per lo svolgimento [delle funzioni di esecuzione della legge]» (articolo 3, paragrafo 1, dell'APPIHAO).

(139) Inoltre l'articolo 79 della legge sulla polizia garantisce alle persone che nutrono perplessità riguardanti l'"esercizio delle funzioni" da parte del personale di polizia il diritto di presentare un reclamo presso la Commissione prefetturale indipendente di sicurezza pubblica (competente). La Commissione tratta «lealmente» i reclami in conformità alla legislazione e alle ordinanze locali e informa per iscritto il denunciante dei risultati. In virtù dei suoi poteri di vigilare e «dirigere» la polizia prefetturale nei casi di «condotta irregolare del personale» (articolo 38, comma 3, e articolo 43-2, comma 1, della legge sulla polizia), la Commissione può chiedere alla polizia prefetturale di indagare sui fatti, può adottare misure appropriate in base ai risultati di tali indagini e può riferire sui risultati. Se ritiene che l'indagine svolta dalla polizia non sia stata adeguata, la Commissione può anche impartire istruzioni sul trattamento del reclamo.

(140) Al fine di facilitare la gestione dei reclami, l'NPA ha emanato una «comunicazione», rivolta alla polizia e alle Commissioni prefetturali di sicurezza pubblica, per il corretto trattamento dei reclami relativi all'esercizio delle funzioni da parte degli operatori di polizia. In tale documento l'NPA stabilisce norme per l'interpretazione e

([111]) Cfr. articolo 5, comma 3, e articolo 38, comma 3, della legge sulla polizia.

([112]) Cfr. articolo 38, comma 3, e articolo 43-2, comma 1, della legge sulla polizia. Nel caso in cui «impartisca un'istruzione» ai sensi dell'articolo 43-2, comma 1, la Commissione prefetturale di pubblica sicurezza può ordinare a una commissione da lei nominata di monitorarne l'esecuzione (comma 2). La Commissione può inoltre raccomandare misure disciplinari o la destituzione del direttore della polizia prefetturale (articolo 50, comma 2) e di altri operatori di polizia (articolo 55, comma 4, della legge sulla polizia).

([113]) Lo stesso vale per il sovrintendente generale nel caso della polizia metropolitana di Tokyo (cfr. articolo 48, comma 1, della legge sulla polizia).

([114]) In base alle informazioni ricevute, nell'esercizio finanziario 2017 (da aprile 2017 a marzo 2018), i «centri di informazione globale» hanno gestito in totale 5 186 richieste presentate da persone.

l'attuazione dell'articolo 79 della legge sulla polizia. Tra l'altro, impone alla polizia prefetturale di istituire un «sistema di trattamento dei reclami», di trattare tutti i reclami e comunicarli «prontamente» alla Commissione prefetturale di sicurezza pubblica competente. Nella comunicazione i reclami sono definiti come richieste volte a correggere «qualsiasi svantaggio specifico inflitto a seguito di un comportamento illecito o inappropriato» ([115]) o «l'omessa azione necessaria da parte di un operatore di polizia nell'esecuzione delle sue funzioni» ([116]) o ancora qualsiasi «lamentela/malcontento per inappropriatezza nell'esecuzione delle funzioni da parte di un operatore di polizia». L'ambito di applicazione materiale di un reclamo è quindi definito in linea di massima e comprende qualsiasi presunta raccolta illecita di dati, e il denunciante non è tenuto a dimostrare di aver subito un danno a seguito delle azioni dell'operatore di polizia. Soprattutto, la comunicazione stabilisce che gli stranieri (tra gli altri) debbano ricevere assistenza nella formulazione di un reclamo. A seguito di un reclamo, le Commissioni prefetturali di sicurezza pubblica sono tenute a garantire che la polizia prefetturale esamini i fatti, metta in atto misure «in conformità al risultato dell'esame» e presenti una relazione su tali risultati. Quando ritiene che l'esame sia insufficiente, la Commissione impartisce istruzioni sul trattamento del reclamo, che la polizia prefetturale è tenuta a seguire. In base alle relazioni ricevute e alle misure adottate, la Commissione comunica alla persona, tra l'altro, le misure adottate per rispondere al reclamo. La comunicazione dell'NPA sottolinea che i reclami dovrebbero essere trattati «con lealtà» e che il risultato dovrebbe essere comunicato «entro il tempo […] ritenuto opportuno alla luce delle norme sociali e del buon senso».

(141) In secondo luogo, poiché il ricorso dovrà essere esperito ovviamente all'estero, in un sistema estero e in una lingua straniera, al fine di facilitare il ricorso per le persone dell'UE i cui dati personali sono trasferiti a operatori economici in Giappone e successivamente consultati da autorità pubbliche, il governo giapponese si è valso dei propri poteri per creare un meccanismo specifico, amministrato e controllato dalla PPC, per la gestione e la risoluzione dei reclami in questo settore. Tale meccanismo si basa sull'obbligo di collaborazione imposto alle autorità pubbliche giapponesi dall'APPI e sul ruolo particolare della PPC nell'ambito dei trasferimenti internazionali di dati da paesi terzi ai sensi dell'articolo 6 dell'APPI e della politica di base (come stabilito dal governo giapponese mediante ordinanza del Gabinetto). I dettagli di tale meccanismo sono definiti nelle dichiarazioni, nelle garanzie e negli impegni ufficiali ricevuti dal governo giapponese e acclusi alla presente decisione come allegato II. Il meccanismo non è soggetto ad alcun obbligo di legittimazione ad agire ed è a accessibile a tutte le persone fisiche, indipendentemente dal fatto che siano sospettate o accusate di un reato.

(142) Nell'ambito del meccanismo la persona che sospetta che i suoi dati trasferiti dall'Unione europea siano stati raccolti o utilizzati dalle autorità pubbliche in Giappone (comprese quelle responsabili del contrasto penale) in violazione delle norme applicabili può presentare un reclamo alla PPC (personalmente o attraverso la propria autorità di protezione dei dati ai sensi dell'articolo 51 del regolamento generale sulla protezione dei dati). La PPC ha l'obbligo di trattare il reclamo e, in una prima fase, di darne comunicazione alle autorità pubbliche competenti, compresi i pertinenti organismi di vigilanza. Tali autorità sono tenute a cooperare con la PPC «anche fornendo le necessarie informazioni e il materiale pertinente, in modo che la PPC possa valutare se la raccolta o il successivo utilizzo di informazioni personali sia avvenuto in conformità alle norme applicabili» ([117]). Tale obbligo, derivante dall'articolo 80 dell'APPI (che impone alle autorità pubbliche giapponesi di cooperare con la PPC), si applica in generale e si estende quindi al riesame di qualsiasi misura di indagine adottata da tali autorità, che si sono inoltre impegnate a cooperare mediante garanzie scritte dei ministeri competenti e dei direttori delle agenzie, come si evince dall'allegato II.

(143) Qualora la valutazione indichi che è avvenuta una violazione delle norme applicabili, «la cooperazione delle autorità pubbliche con la PPC prevede l'obbligo di porre rimedio alla violazione», il che, in caso di raccolta illecita di informazioni personali, comprende la cancellazione di tali dati. È importante precisare che tale obbligo è ottemperato sotto la supervisione della PPC che «confermerà, prima di concludere la valutazione, che la violazione è stata completamente sanata».

(144) Una volta conclusa la valutazione, la PPC dà comunicazione alla persona dei risultati entro un lasso di tempo ragionevole, comprese, se del caso, le misure correttive adottate. Al tempo stesso la PPC deve informare la persona anche della possibilità di chiedere conferma dei risultati all'autorità pubblica competente e deve indicarle l'identità dell'autorità cui occorre presentare tale richiesta di conferma. La possibilità di ricevere tale conferma, compresi i

([115]) La condizione di uno «svantaggio specifico» indica semplicemente che il denunciante deve essere interessato personalmente dalla condotta (o dall'inazione) della polizia e non che il denunciante debba dimostrare il danno subito.

([116]) L'osservanza della legge, compresi gli obblighi giuridici per la raccolta e l'uso dei dati personali, rientra tra dette funzioni. Cfr. articolo 2, comma 2, e articolo 3 della legge sulla polizia.

([117]) Nell'effettuare la valutazione la PPC coopera con il MIC che, come spiegato al considerando 136, può chiedere di presentare motivazioni e materiali e può formulare pareri riguardanti la gestione di informazioni personali da parte dell'organo amministrativo interessato (articoli 50 e 51 dell'APPIHAO).

motivi su cui si fonda la decisione dell'autorità competente, può essere di aiuto alla persona per adottare ulteriori misure, anche in caso di ricorso giudiziario. È possibile limitare la comunicazione di informazioni dettagliate sui risultati della valutazione purché sussistano motivi fondati per ritenere che possa presentare un rischio per l'indagine in corso.

(145) In terzo luogo, la persona, qualora sia in disaccordo con una decisione giudiziaria (provvedimento) di sequestro ([118]) relativa ai propri dati personali o con le misure della polizia o del pubblico ministero prese in esecuzione di tale decisione, può presentare istanza affinché tale decisione o tali misure siano revocate o modificate (articolo 429, comma 1, articolo 430, commi 1 e 2, del codice di procedura penale, articolo 26 della legge sulle intercettazioni) ([119]). Nel caso in cui ritenga che il provvedimento o la sua esecuzione («procedura di sequestro») sia illegale, il giudice del riesame accoglie l'istanza e ordina la restituzione degli elementi sequestrati ([120]).

(146) In quarto luogo, come forma più indiretta di controllo giudiziario, qualora una persona ritenga che la raccolta delle sue informazioni personali nell'ambito di un'indagine penale sia illecita può invocare tale illegalità nel corso del processo. Se il giudice accoglie l'istanza, le prove saranno escluse in quanto inammissibili.

(147) Infine, ai sensi dell'articolo 1, comma 1, della legge sul ricorso avverso lo Stato, un giudice può concedere un indennizzo nel caso in cui un dipendente pubblico, nell'esercizio delle sue funzioni di pubblico ufficiale dello Stato, abbia cagionato un danno alla persona interessata illegalmente e per dolo o colpa. Ai sensi dell'articolo 4 della legge sul ricorso avverso lo Stato, la responsabilità dello Stato per i danni è basata sulle disposizioni del codice civile. Al riguardo, l'articolo 710 di detto codice stabilisce che la responsabilità copre anche i danni diversi da quelli materiali e, di conseguenza, il danno morale (ad esempio sotto forma di «disagio psichico»). Ciò include i casi in cui la privacy di una persona è stata violata con un'attività illegale di sorveglianza e/o con la raccolta dei suoi dati personali (ad esempio esecuzione illegale di un mandato) ([121]).

(148) Oltre a un risarcimento pecuniario, le persone, a certe condizioni, possono ottenere anche ingiunzioni (ad esempio la cancellazione dei dati personali raccolti dalle pubbliche autorità) sulla base dei propri diritti relativi al rispetto della vita privata di cui all'articolo 13 della costituzione ([122]).

(149) Per quanto riguarda tutte le possibilità di ricorso menzionate, il meccanismo di risoluzione delle controversie istituito dal governo giapponese prevede che una persona, se ancora non è soddisfatta del risultato del procedimento, possa rivolgersi alla PPC «che informa la persona delle varie possibilità e dei dettagli delle procedure per ottenere rimedio ai sensi delle disposizioni legislative e regolamentari giapponesi». Inoltre la PPC «fornirà alla persona sostegno, comprese la consulenza e l'assistenza per avviare ulteriori azioni dinanzi all'organo amministrativo o giurisdizionale competente».

(150) È compresa l'attivazione dei diritti procedurali previsti dal codice di procedura penale. Ad esempio, «[q]ualora la valutazione indichi che una persona è indagata nell'ambito di un procedimento penale, la CPP informa l'interessato del fatto» ([123]), nonché della possibilità, a norma dell'articolo 259 del codice di procedura penale, di chiedere al pubblico ministero che gli comunichi la decisione di non luogo a procedere. Inoltre, qualora la valutazione indichi che è stato avviato una procedimento riguardante le informazioni personali della persona e che questo si è concluso, la PPC informa la persona che il fascicolo può essere visionato a norma dell'articolo 53 del codice di procedura penale (e dell'articolo 4 della legge sui fascicoli definitivi dei casi penali). L'accesso al fascicolo è

([118]) Ciò include il mandato d'intercettazione per cui la legge sulle intercettazioni stabilisce un obbligo specifico di comunicazione (articolo 23). In conformità a tale disposizione l'autorità inquirente è tenuta a comunicare tale circostanza per iscritto alle persone le cui comunicazioni sono intercettate (e pertanto incluse nel verbale dell'intercettazione). Un altro esempio è l'articolo 100, comma 3, del codice di procedura penale, secondo il quale il giudice, quando dispone il sequestro di invii postali o telegrammi spediti dall'imputato o da questi ricevuti, ne dà comunicazione al mittente o al destinatario, a meno che vi sia il rischio che tale comunicazione ostacoli il procedimento giudiziario. L'articolo 222, comma 1, del codice di procedura penale, fa riferimento a tale disposizione per le perquisizioni e i sequestri effettuati da un autorità inquirente.

([119]) Sebbene tale istanza non abbia l'effetto di sospendere automaticamente l'esecuzione della decisione di sequestro, il giudice del riesame può ordinarne la sospensione fino a quando non abbia emesso una decisione nel merito. Cfr. articolo 429, comma 2, e articolo 432 in combinato disposto con l'articolo 424 del codice di procedura penale.

([120]) Cfr. allegato II, sez. II.C(1).

([121]) Cfr. allegato II, sez. II.C.2).

([122]) Cfr., ad esempio, tribunale distrettuale di Tokyo, sentenza del 24 marzo 1988 (n. 2925); tribunale distrettuale di Osaka, sentenza del 26 aprile 2007 (n. 2925). Secondo il Tribunale distrettuale di Osaka è necessario ponderare una serie di fattori come ad esempio: i) la natura e il contenuto delle informazioni personali in questione; ii) la modalità con cui sono state raccolte; iii) gli svantaggi per la persona nel caso in cui le informazioni non siano cancellate; iv) l'interesse pubblico, tra cui gli svantaggi per l'autorità pubblica nel caso in cui le informazioni siano cancellate.

([123]) In ogni caso, dopo l'avvio del procedimento penale, il pubblico ministero dovrà dare all'imputato la possibilità di visionare le prove (cfr. articoli da 298 a 299 del codice di procedura penale). Per quanto riguarda le vittime di reati, cfr. articoli da 316 a 333 del codice di procedura penale.

importante in quanto aiuta la persona a comprendere meglio le indagini svolte nei suoi confronti e quindi a preparare un'eventuale azione giudiziaria (ad esempio, una richiesta di risarcimento dei danni) nel caso in cui ritenga che i suoi dati siano stati raccolti o utilizzati illegalmente.

3.3. **Accesso e uso da parte delle autorità pubbliche giapponesi per motivi di sicurezza nazionale**

(151) Secondo le autorità giapponesi, non esiste alcuna legge in Giappone che consenta richieste coattive di informazioni o «intercettazioni amministrative» al di fuori di indagini penali. Di conseguenza, per ragioni di sicurezza nazionale le informazioni possono essere ottenute solo da una fonte liberamente accessibile a tutti o mediante comunicazione volontaria. Gli operatori economici che ricevono una richiesta di cooperazione volontaria (sotto forma di comunicazione delle informazioni in formato elettronico) non sono tenuti giuridicamente a fornire tali informazioni ([124]).

(152) Inoltre, in base alle informazioni ricevute, soltanto quattro enti pubblici sono autorizzati a raccogliere, per ragioni di sicurezza nazionale, informazioni in formato elettronico detenute da operatori economici giapponesi, vale a dire: i) l'Ufficio del Gabinetto per l'intelligence e la ricerca (CIRO), ii) il ministero della Difesa (MOD); iii) la polizia (sia l'Agenzia nazionale di polizia (NPA) ([125]) che la polizia prefetturale); iv) l'Agenzia di intelligence per la pubblica sicurezza (PSIA). Tuttavia il CIRO non raccoglie mai informazioni direttamente dagli operatori economici, neanche mediante intercettazione delle comunicazioni. Quando riceve informazioni da altre autorità governative al fine di fornire analisi al Gabinetto, tali altre autorità sono tenute a loro volta a rispettare la legislazione, comprese le limitazioni e le garanzie esaminate nella presente decisione. Le sue attività non sono quindi pertinenti nel contesto di un trasferimento.

3.3.1. *Base giuridica e limitazioni/garanzie applicabili*

(153) In base alle informazioni ricevute, il MOD raccoglie informazioni (in formato elettronico) in base alla legge sull'istituzione del MOD. Secondo l'articolo 3 di tale legge, la missione del MOD è di gestire e dirigere le forze militari e di «condurre le azioni connesse al fine di garantire la pace, l'indipendenza e la sicurezza della nazione». L'articolo 4, comma 4, stabilisce che il MOD ha competenza in materia di «difesa e protezione», di interventi intrapresi dalle forze di autodifesa nonché di dispiegamento delle forze militari, compresa la raccolta delle informazioni necessarie a condurre tali azioni. Il MOD ha soltanto il potere di raccogliere informazioni (in formato elettronico) da operatori economici mediante cooperazione volontaria.

(154) Per quanto riguarda la polizia prefetturale, le sue responsabilità e i suoi compiti includono il «mantenimento della pubblica sicurezza e dell'ordine pubblico» (articolo 35, comma 2, in combinato disposto con l'articolo 2, comma 1, della legge sulla polizia). In tale ambito di competenza la polizia può raccogliere informazioni, ma solo su base volontaria, senza forza di legge. Le attività della polizia sono inoltre «strettamente limitate» a quanto necessario allo svolgimento delle sue funzioni. Essa agisce in modo «imparziale, super partes, equo e scevro da pregiudizi» e non abusa mai dei propri poteri «in alcuno modo che interferisca nei diritti e nelle libertà di una persona garantiti dalla costituzione del Giappone» (articolo 2 della legge sulla polizia).

(155) La PSIA può svolgere infine indagini nell'ambito della legge sulla prevenzione delle attività sovversive (SAPA) e della legge sul controllo delle organizzazioni che hanno commesso omicidi di massa indiscriminati (ACO), nel caso in cui tali indagini siano necessarie a preparare l'adozione di misure di controllo nei confronti di determinate organizzazioni ([126]). Nell'ambito di entrambe le leggi, su richiesta del direttore generale della PSIA, la Commissione per il controllo della pubblica sicurezza può emettere determinate «disposizioni» (di sorveglianza/di divieto nel caso dell'ACO ([127]), di scioglimento/di divieto nel caso della SAPA ([128])) e in questo contesto la PSIA può svolgere indagini ([129]). In base alle informazioni ricevute, tali indagini sono sempre svolte su base volontaria, il che significa

([124]) Pertanto, gli operatori possono liberamente decidere di non cooperare, senza alcun rischio di sanzioni o di altre conseguenze negative. Cfr. allegato II, sez. III.A.1).

([125]) Secondo le informazioni ricevute, il ruolo principale dell'NPA è però di coordinare le indagini dei vari servizi di polizia prefetturale e di scambiare informazioni con autorità straniere. Persino in tale ruolo l'NPA è soggetta alla vigilanza della Commissione nazionale per la sicurezza pubblica, responsabile, tra l'altro, della protezione dei diritti e delle libertà delle persone fisiche (articolo 5, comma 1, della legge sulla polizia).

([126]) Cfr. allegato II, sez. III.A.1), punto 3. Il rispettivo ambito di applicazione di queste due leggi è limitato: la SAPA si riferisce ad «attività terroristiche sovversive» e l'ACO a «omicidi di massa indiscriminati» (ossia un'"attività terroristica sovversiva" ai sensi della SAPA «mediante la quale sono sia ucciso indiscriminatamente un elevato numero di persone»).

([127]) Cfr. articoli 5 e 8 dell'ACO. Una disposizione di sorveglianza prevede anche l'obbligo di rendicontazione per l'organizzazione interessata dalla misura. Per le garanzie procedurali, in particolare gli obblighi di trasparenza e l'autorizzazione preventiva da parte della Commissione per il controllo della pubblica sicurezza, cfr. gli articoli 12, 13 e da 15 a 27 dell'ACO.

([128]) Cfr. articoli 5 e 7 della SAPA. Per le garanzie procedurali, in particolare gli obblighi di trasparenza e l'autorizzazione preventiva da parte della Commissione per il controllo della pubblica sicurezza, cfr. gli articoli da 11 a 25 della SAPA.

([129]) Cfr. articolo 27 della SAPA e articoli 29 e 30 dell'ACO.

che la PSIA non può imporre al proprietario delle informazioni personali di fornirle ([130]). I controlli e le indagini sono sempre condotti solo nella misura minima necessaria a conseguire la finalità di controllo e non devono in alcun caso essere effettuati al fine di limitare «irragionevolmente» i diritti e le libertà garantiti dalla costituzione del Giappone (articolo 3, comma 1, della SAPA/dell'ACO). Inoltre, a norma dell'articolo 3, comma 2, della SAPA/dell'ACO, la PSIA non deve in alcun caso abusare di tali controlli o delle indagini preparatorie per tali controlli. L'operatore della PSIA che abbia compiuto un abuso di potere ai sensi della legge applicabile, obbligando una persona a fare qualcosa che non era tenuta a fare o interferendo con l'esercizio dei diritti di una persona, può essere soggetto a sanzioni penali a norma dell'articolo 45 della SAPA o dell'articolo 42 dell'ACO. Infine le due leggi prevedono esplicitamente che le rispettive disposizioni, compresi i poteri conferiti dalle medesime, «non devono in alcun caso essere oggetto di un'interpretazione estensiva» (articolo 2 della SAPA/dell'ACO).

(156) In tutti i casi di accesso da parte delle autorità pubbliche per motivi di sicurezza nazionale descritti nella presente sezione, si applicano le limitazioni previste dalla Corte suprema giapponese per i mezzi di indagine volontari, il che significa che la raccolta di informazioni (in formato elettronico) deve rispettare i principi di necessità e di proporzionalità («metodo adeguato») ([131]). Come confermato esplicitamente dalle autorità giapponesi, «la raccolta e il trattamento delle informazioni avviene soltanto per quanto necessario allo svolgimento delle funzioni specifiche dell'autorità pubblica competente nonché sulla base di minacce specifiche». Pertanto «ciò esclude la raccolta o l'accesso in modo massiccio e indiscriminato a informazioni personali per ragioni di sicurezza nazionale» ([132]).

(157) Inoltre, una volta raccolta, qualsiasi informazione personale conservata dalle autorità pubbliche per motivi di sicurezza nazionale rientra nelle tutele dell'APPIHAO che, di conseguenza, si applicano per quanto riguarda la conservazione, l'uso e la divulgazione successivi (cfr. il considerando 118).

3.3.2. *Vigilanza indipendente*

(158) La raccolta di informazioni personali per finalità di sicurezza nazionale è soggetta a diversi livelli di vigilanza da parte dei tre poteri dello Stato.

(159) In primo luogo, la Dieta del Giappone, attraverso le sue commissioni specializzate, può esaminare la legittimità delle indagini sulla base dei propri poteri di controllo parlamentare (articolo 62 della costituzione, e articolo 104 della legge sulla Dieta; cfr. considerando 134). Tale funzione di vigilanza è supportata da obblighi specifici di rendicontazione sulle attività svolte nell'ambito delle basi giuridiche summenzionate ([133]).

(160) In secondo luogo, esistono vari meccanismi di vigilanza all'interno dell'esecutivo.

(161) Per quanto riguarda il MOD, la vigilanza è esercitata dall'Ispettorato generale per il rispetto degli obblighi normativi (IGO) ([134]) che è stato istituito, sulla base dell'articolo 29 della legge sull'istituzione del MOD, come ufficio del MOD sotto la supervisione del ministro della Difesa (cui rende conto), pur essendo indipendente dai dipartimenti operativi del MOD. L'IGO ha la funzione di assicurare il rispetto delle disposizioni legislative e regolamentari nonché la corretta esecuzione dei compiti del personale del MOD. I suoi poteri includono la competenza a effettuare «ispezioni per la difesa», sia a intervalli regolari («ispezioni per la difesa periodiche») sia in singoli casi («ispezioni per la difesa speciali»), che in passato hanno riguardato anche la corretta gestione delle informazioni personali ([135]). Nell'ambito di tali ispezioni, l'IGO può accedere a siti (uffici) e chiedere la presentazione di

([130]) Cfr. allegato II, sez. III.A.1), punto 3.

([131]) Cfr. allegato II, sez. III.A.2), lettera b): «Dalla giurisprudenza della Corte suprema emerge che, per presentare una richiesta di cooperazione volontaria a un operatore economico, la richiesta deve essere necessaria per le indagini su un sospetto di reato e deve essere ragionevole ai fini del raggiungimento dell'obiettivo dell'indagine. Sebbene le indagini condotte dalle autorità inquirenti nel settore della sicurezza nazionale differiscano dalle indagini condotte dalle autorità omologhe nel settore dell'esecuzione della legge, per quanto riguarda sia la base giuridica che la finalità, i principi centrali di "necessità delle indagini" e di "adeguatezza del metodo" si applicano in modo analogo al settore della sicurezza nazionale e devono essere rispettati tenendo adeguatamente conto delle circostanze specifiche di ciascun caso».

([132]) Cfr. allegato II, sez. III.A.2), lettera b).

([133]) Cfr., ad esempio, articolo 36 della SAPA/articolo 31 dell'ACO (per la PSIA).

([134]) Il direttore dell'IGO è un ex pubblico ministero. Cfr. allegato II, sez. III.B.3).

([135]) Cfr. allegato II, sez. III.B.3). Secondo l'esempio fornito, l'ispezione periodica per la difesa del 2016 sulla «consapevolezza/preparazione relativamente al rispetto degli obblighi normativi» ha riguardato, tra l'altro, lo «stato della protezione delle informazioni personali» (gestione, conservazione, ecc.). La pertinente relazione ha evidenziato casi di gestione inadeguata dei dati e ha chiesto miglioramenti in proposito. Il MOD ha pubblicato la relazione sul proprio sito internet.

documenti o informazioni, incluse spiegazioni da parte del viceministro aggiunto del MOD. L'ispezione si conclude con una relazione, da presentare al ministro della Difesa, che illustra i risultati e le misure di miglioramento (la cui attuazione può essere nuovamente verificata attraverso ulteriori ispezioni). La relazione costituisce a sua volta la base delle istruzioni del ministro della Difesa per l'attuazione delle misure necessarie a risolvere la situazione; il viceministro aggiunto è incaricato di attuare tali misure e deve riferire sul seguito dato loro.

(162) Per quanto riguarda la polizia prefetturale, la vigilanza è garantita dalla Commissione prefetturale indipendente di sicurezza pubblica, come spiegato al considerando 135 per quanto riguarda il rispetto del contrasto penale.

(163) Infine, come indicato, la PSIA può svolgere indagini soltanto nella misura in cui esse siano necessarie all'adozione di una disposizione di divieto, di scioglimento o di sorveglianza ai sensi della SAPA/dell'ACO e tali disposizioni sono soggette alla vigilanza ex ante della Commissione per il controllo della pubblica sicurezza indipendente ([136]). Inoltre ispezioni regolari/periodiche (volte a controllare in modo globale le operazioni della PSIA) ([137]) e ispezioni interne speciali ([138]) sulle attività dei singoli dipartimenti/uffici, ecc. sono svolte da ispettori appositamente designati e possono risultare in istruzioni ai direttori dei dipartimenti pertinenti ecc. affinché adottino misure correttive o di miglioramento.

(164) Detti meccanismi di vigilanza, che sono ulteriormente rafforzati dalla possibilità per le persone di richiedere l'intervento della PPC in qualità di autorità di vigilanza indipendente (cfr. successiva sezione 168), forniscono adeguate garanzie contro il rischio che le autorità giapponesi abusino dei loro poteri nel settore della sicurezza nazionale e contro qualsiasi raccolta illecita di informazioni in formato elettronico.

3.3.3. *Ricorso individuale*

(165) Relativamente al ricorso individuale, per quanto riguarda le informazioni personali raccolte e perciò «conservate» da organi amministrativi, questi sono tenuti ad «adoperarsi a trattare in modo corretto e rapido tutti i reclami» concernenti tale trattamento (articolo 48 dell'APPIHAO).

(166) Inoltre, a differenza delle indagini penali, le persone (compresi i cittadini stranieri che vivono all'estero) hanno, in linea di principio, il diritto alla comunicazione ([139]), alla rettifica (compresa la cancellazione) e alla sospensione dell'utilizzo/della fornitura delle informazioni personali ai sensi dell'APPIHAO. Detto questo, il direttore dell'organo di amministrazione può rifiutare la comunicazione di informazioni «per le quali vi siano fondati motivi […] di ritenere che la comunicazione possa causare danni alla sicurezza nazionale» (articolo 14, punto iv), dell'APPIHAO), anche senza rivelare l'esistenza di tali informazioni (articolo 17 dell'APPIHAO). Analogamente, sebbene una persona possa chiedere la sospensione dell'utilizzo o la cancellazione delle informazioni personali a norma dell'articolo 36, comma 1, punto i), dell'APPIHAO, nel caso in cui l'organo amministrativo le abbia ottenuto illegalmente o le conservi/utilizzi al di là di quanto necessario per conseguire la finalità specifica, l'autorità può rifiutare la richiesta se ritiene che la sospensione dell'utilizzo «possa impedire la corretta esecuzione delle misure relative alla finalità di utilizzo delle informazioni personali conservate a causa della natura di tali misure» (articolo 38 dell'APPIHAO). Tuttavia, laddove sia possibile separare o escludere con facilità le parti soggette a un'eccezione, gli organi amministrativi sono tenuti a concedere almeno una comunicazione parziale (cfr., ad esempio, articolo 15, comma 1, dell'APPIHAO) ([140]).

([136]) Secondo la legge sull'istituzione della Commissione per il controllo della pubblica sicurezza, il presidente e i membri della Commissione «esercitano indipendentemente la loro autorità» (articolo 3). Essi sono nominati dal primo ministro con l'approvazione di entrambe le camere della Dieta e possono essere revocati solo per «valido motivo» (ad esempio, pena detentiva, condotta irregolare, disturbo mentale o fisico, apertura di una procedura fallimentare).

([137]) Regolamento per le ispezioni periodiche dell'Agenzia di intelligence per la pubblica sicurezza (direttore generale della PSIA, istruzione n. 4, 1986).

([138]) Regolamento per le ispezioni speciali dell'Agenzia di intelligence per la pubblica sicurezza (direttore generale della PSIA, istruzione n. 11, 2008). Le ispezioni speciali sono effettuate quando il direttore generale della PSIA lo ritiene necessario.

([139]) Ciò si riferisce al diritto di ricevere una copia delle «informazioni personali conservate».

([140]) Cfr. anche la possibilità di «comunicazione discrezionale» persino nel caso in cui «informazioni di cui è vietata la comunicazione» siano inserite tra le «informazioni personali conservate» di cui è chiesta la comunicazione (articolo 16 dell'APPIHAO).

(167) In ogni caso l'organo amministrativo deve adottare una decisione scritta entro un temine determinato (30 giorni, che a certe condizioni possono essere prorogati di altri 30). Se la richiesta è respinta o accolta solo parzialmente o se la persona ritiene, per altre ragioni, che la condotta dell'organo amministrativo sia «illecita o ingiusta», la persona può richiedere il riesame amministrativo in base alla legge per il riesame dei ricorsi amministrativi ([141]). In tal caso, il direttore dell'organo amministrativo che decide sul ricorso consulta la Commissione per il riesame della comunicazione di informazioni e della protezione delle informazioni personali (articoli 42 e 43 dell'APPIHAO), commissione specializzata indipendente i cui membri sono nominati dal primo ministro con l'approvazione di entrambe le camere della Dieta. In base alle informazioni ricevute, la Commissione può svolgere un controllo ([142]) e, a tal fine, chiedere all'organo amministrativo di fornire le informazioni personali conservate, compresi gli eventuali contenuti classificati, nonché ulteriori informazioni e documenti. Sebbene la relazione finale inviata al ricorrente e all'organo amministrativo e resa pubblica non sia giuridicamente vincolante, le raccomandazioni sono rispettate in quasi tutti i casi ([143]). Inoltre il richiedente ha la possibilità di impugnare la decisione in sede giudiziaria sulla base della legge in materia di contenzioso amministrativo. Ciò consente un controllo giudiziale sull'utilizzo delle eccezioni per motivi di sicurezza nazionale, anche sul fatto che esse costituiscano un abuso o siano ancora giustificate.

(168) Al fine di agevolare l'esercizio dei diritti summenzionati previsti dall'APPIHAO, il MIC ha istituito 51 «centri di informazione globale» che forniscono informazioni consolidate su tali diritti, le procedure applicabili per presentare una richiesta e i possibili mezzi di ricorso ([144]). Per quanto riguarda gli organi amministrativi, questi sono tenuti a fornire «informazioni che contribuiscono a specificare le informazioni personali conservate in loro possesso» ([145]) e ad adottare «altre misure adeguate in considerazione delle esigenze della persona che intende presentare la richiesta» (articolo 47, comma 1, dell'APPIHAO).

(169) Come nel caso di indagini nell'ambito del contrasto penale, anche nell'ambito della sicurezza nazionale le persone possono ottenere un risarcimento a titolo individuale contattando direttamente la PPC. Ciò consentirà di avviare la specifica procedura di risoluzione delle controversie che il governo giapponese ha creato per i cittadini dell'UE i cui dati personali sono trasferiti ai sensi della presente decisione (cfr. le spiegazioni dettagliate nei considerando da 141 a 144 e 149).

(170) Le persone possono inoltre presentare un ricorso giudiziale sotto forma di azione per il risarcimento dei danni ai sensi della legge sul ricorso avverso lo Stato, che copre anche i danni morali e, a determinate condizioni, la cancellazione dei dati raccolti (cfr. considerando 147).

4. CONCLUSIONI: LIVELLO ADEGUATO DI PROTEZIONE DEI DATI PERSONALI TRASFERITI DALL'UNIONE EUROPEA AGLI OPERATORI ECONOMICI IN GIAPPONE

(171) La Commissione ritiene che l'APPI, completata dalle norme integrative figuranti nell'allegato I, nonché dalle dichiarazioni, dalle garanzie e dagli impegni ufficiali figuranti nell'allegato II, assicuri un livello di protezione dei dati personali trasferiti dall'Unione europea sostanzialmente equivalente a quello garantito dal regolamento (UE) 2016/679.

(172) Inoltre la Commissione ritiene che, nel complesso, i meccanismi di vigilanza e i mezzi di ricorso previsti dalla normativa giapponese permettano di individuare e punire nella pratica le violazioni commesse dai PIHBO destinatari 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.

([141]) Legge per il riesame dei ricorsi amministrativi (legge n. 160 del 2014), in particolare articolo 1, comma 1.

([142]) Cfr. articolo 9 della legge sull'istituzione della Commissione per il riesame della comunicazione di informazioni e della protezione delle informazioni personali (legge n. 60 del 2003).

([143]) In base alle informazioni ricevute, nei 13 anni intercorsi dal 2005 (quando l'APPIHAO è entrata in vigore) ad ora, l'organo amministrativo non si è attenuto alla relazione soltanto in due casi su oltre 2000, nonostante il fatto che le decisioni amministrative siano state contraddette in numerose occasioni dalla Commissione per il riesame. Inoltre, quando adotta una decisione che si discosta dalle conclusioni della relazione, l'organo amministrativo deve indicarne chiaramente i motivi. Cfr. allegato II, sez. III.C, in riferimento all'articolo 50, comma 1, punto iv),della legge per il riesame dei ricorsi amministrativi.

([144]) I centri di informazione globale – uno in ciascuna prefettura – forniscono ai cittadini spiegazioni sulle informazioni personali raccolte dalle autorità pubbliche (ad esempio banche dati esistenti) e sulle norme in materia di protezione dei dati applicabili (APPIHAO), comprese le modalità per esercitare il diritto di comunicazione, di rettifica o di sospensione dell'utilizzo. I centri funzionano nel contempo come punto di contatto per richieste/reclami da parte dei cittadini. Cfr. allegato II, sez. II.C.4), lettera a).

([145]) Cfr. anche gli articoli 10 e 11 dell'APPIHAO relativi al «registro dei fascicoli delle informazioni personali» che prevede tuttavia ampie eccezioni quando si tratta di fascicoli «di informazioni a carattere personale» preparati o ottenuti per le indagini penali o che implicano questioni concernenti la sicurezza e altri importanti interessi dello Stato (cfr. articolo 10, comma 2, punti i) e ii), dell'APPIHAO).

(173) Infine, sulla base delle informazioni disponibili sull'ordinamento giuridico giapponese, comprese le dichiarazioni, le garanzie e gli impegni del governo giapponese figuranti nell'allegato II, la Commissione ritiene che qualsiasi ingerenza da parte di autorità pubbliche giapponesi nei diritti fondamentali delle persone i cui dati personali sono trasferiti dall'Unione europea al Giappone, per finalità di interesse pubblico, in particolare a fini di contrasto penale e di sicurezza nazionale, sarà limitata a quanto strettamente necessario a conseguire l'obiettivo legittimo in questione, e che contro tali ingerenze esista un'efficace tutela giuridica.

(174) Pertanto, alla luce delle conclusioni della presente decisione, la Commissione ritiene che il Giappone garantisca un livello adeguato di protezione per i dati personali trasferiti dall'Unione europea ai PIHBO presenti in Giappone che sono soggetti all'APPI, tranne nei casi in cui il destinatario rientri in una delle categorie elencate all'articolo 76, comma 1, dell'APPI, e le finalità del trattamento corrispondano, in tutto o in parte, a una delle finalità previste da tale disposizione.

(175) La Commissione conclude pertanto che sia raggiunto il livello di adeguatezza di cui all'articolo 45 del regolamento (UE) 2016/679, interpretato alla luce della Carta dei diritti fondamentali dell'Unione europea, in particolare nella sentenza *Schrems* ([146]).

5. AZIONE DELLE AUTORITÀ DI PROTEZIONE DEI DATI E INFORMAZIONE DELLA COMMISSIONE

(176) Secondo la giurisprudenza della Corte di giustizia ([147]), 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 Giappone 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.

(177) La Commissione dovrebbe pertanto controllare su base continuativa la situazione per quanto riguarda il quadro giuridico e la prassi effettiva del trattamento dei dati personali valutati dalla presente decisione, compreso il rispetto da parte delle autorità giapponesi delle dichiarazioni, delle garanzie e degli impegni figuranti nell'allegato II. Per agevolare questo processo, le autorità giapponesi dovrebbero informare la Commissione degli sviluppi sostanziali rilevanti ai fini della presente decisione, per quanto riguarda il trattamento dei dati personali da parte degli operatori economici e le limitazioni e le garanzie applicabili all'accesso ai dati personali da parte delle autorità pubbliche. Ciò dovrebbe includere qualsiasi decisione adottata dalla PPC ai sensi dell'articolo 24 dell'APPI che riconosce che un paese terzo fornisce un livello di protezione equivalente a quello garantito dal Giappone.

(178) Inoltre, al fine di consentire alla Commissione di svolgere in modo efficace la propria funzione di controllo, 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 gli operatori economici in Giappone. La Commissione dovrebbe inoltre essere informata delle eventuali indicazioni del fatto che le azioni delle autorità pubbliche giapponesi responsabili della prevenzione, dell'investigazione, dell'accertamento o del perseguimento dei reati ovvero della sicurezza nazionale, compresi gli organismi di vigilanza, non garantiscono il necessario livello di protezione.

(179) 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. 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. Allo stesso tempo, come spiegato dalla Corte di giustizia nella sentenza Schrems ([148]) e come riconosciuto nell'articolo 58, paragrafo 5, del regolamento, quando un'autorità di protezione dei dati contesta, anche a seguito di un reclamo, la compatibilità di una decisione di adeguatezza della Commissione con i diritti fondamentali della persona al rispetto della vita privata e alla protezione dei dati, la normativa nazionale deve prevedere mezzi di ricorso che le consentano di far valere tali censure dinanzi a un giudice nazionale, il quale, in caso di dubbio, deve sospendere il procedimento e disporre un rinvio pregiudiziale alla Corte di giustizia ([149]).

([146]) Cfr. nota a piè di pagina 3.
([147]) *Schrems*, punto 76.
([148]) *Schrems*, punto 65.
([149]) *Schrems*, punto 65: «A tal riguardo, 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».

6. **RIESAME PERIODICO DELLA CONSTATAZIONE DI ADEGUATEZZA**

(180) In applicazione dell'articolo 45, paragrafo 3, del regolamento (UE) 2016/679 ([150]) e alla luce del fatto che il livello di protezione assicurato dall'ordinamento giuridico giapponese può evolversi, la Commissione, successivamente all'adozione della presente decisione, dovrebbe verificare periodicamente se le constatazioni relative al livello di protezione assicurato dal Giappone continuino ad essere giustificate in fatto e in diritto.

(181) A tal fine, la presente decisione dovrebbe essere oggetto di un primo riesame entro due anni dall'entrata in vigore. A seguito del primo riesame, e tenuto conto del suo esito, la Commissione deciderà, in stretta consultazione con il comitato istituito a norma dell'articolo 93, paragrafo 1, del GDPR, se mantenere il ciclo di due anni. In ogni caso i successivi riesami dovrebbero avvenire almeno ogni quattro anni ([151]). Detto riesame dovrebbe riguardare tutti gli aspetti del funzionamento della presente decisione, in particolare l'applicazione delle norme integrative (con particolare riguardo alle tutele in caso di trasferimenti successivi), l'applicazione delle norme in materia di consenso, anche in caso di ritiro dello stesso, l'efficacia dell'esercizio dei diritti individuali, nonché le limitazioni e le garanzie per l'accesso da parte delle pubbliche amministrazioni, compreso il meccanismo di ricorso di cui all'allegato II della presente decisione. Dovrebbe inoltre includere l'efficacia della vigilanza e dei compiti esecutivi, per quanto riguarda le norme applicabili ai PIHBO e nel settore del contrasto penale e della sicurezza nazionale.

(182) Per effettuare il riesame, la Commissione dovrebbe incontrare la CPP, accompagnata, se del caso, da altre autorità giapponesi 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 (EDPB). Nel quadro del riesame congiunto la Commissione dovrebbe chiedere alla PPC 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 ([152]). 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 giapponesi o di altri portatori di interessi in Giappone, dell'EDPB, 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.

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

7. **SOSPENSIONE DELLA DECISIONE DI ADEGUATEZZA**

(184) Se, in base alle verifiche periodiche e ad hoc o ad altre informazioni disponibili, la Commissione conclude che il livello di protezione offerto dall'ordinamento giuridico giapponese non può più essere considerato sostanzialmente equivalente a quello dell'Unione europea, ne dovrebbe informare le autorità giapponesi competenti e chiedere che siano adottate misure appropriate entro un termine stabilito ragionevole. Ciò comprende le norme applicabili sia agli operatori economici che alle autorità pubbliche giapponesi responsabili del contrasto penale o della sicurezza nazionale. Ad esempio, tale procedimento sarebbe avviato in casi in cui, nell'ambito delle garanzie che assicurano la continuità della protezione ai sensi dell'articolo 44 del GDPR, non siano più effettuati trasferimenti successivi, compresi quelli sulla base di decisioni adottate dalla PPC a norma dell'articolo 24 dell'APPI che riconoscono che un paese terzo fornisce un livello di protezione equivalente a quello garantito dal Giappone.

(185) Se, dopo il termine stabilito, le autorità giapponesi competenti non riescono a dimostrare in modo soddisfacente che la presente decisione continua a essere basata su un adeguato livello di protezione, la Commissione dovrebbe avviare, in applicazione dell'articolo 45, paragrafo 5, del regolamento (UE) 2016/679, la procedura di sospensione o abrogazione, totale o parziale, della presente decisione. In alternativa, la Commissione dovrebbe avviare la procedura di modifica della 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 è garantita la continuità della protezione a norma dell'articolo 44 del GDPR.

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

([151]) 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.

([152]) Cfr. anche allegato II, sez. IV: «Nel quadro del riesame periodico della decisione di adeguatezza, la PPC e la Commissione europea si scambiano informazioni sul trattamento dei dati alle condizioni previste dalla constatazione di adeguatezza, comprese quelle stabilite nella presente dichiarazione».

(186) In particolare, la Commissione dovrebbe avviare la procedura di sospensione o abrogazione in presenza di indicazioni del fatto che le norme integrative di cui all'allegato I non sono rispettate dagli operatori economici che ricevono dati personali a norma della presente decisione e/o non sono fatte rispettare effettivamente oppure del fatto che le autorità giapponesi non rispettano le dichiarazioni, le garanzie e gli impegni che figurano nell'allegato II della presente decisione.

(187) La Commissione dovrebbe inoltre valutare l'opportunità di avviare la procedura di modifica, sospensione o abrogazione della presente decisione se, nel contesto del riesame congiunto o in altro contesto, le autorità giapponesi competenti non forniscano le informazioni o i chiarimenti necessari alla valutazione del livello di protezione offerto ai dati personali trasferiti dall'Unione europea al Giappone o della 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.

(188) Per motivi di urgenza debitamente giustificati, come un rischio di grave violazione dei diritti degli interessati, la Commissione dovrebbe considerare la possibilità di adottare una decisione di sospensione o abrogazione della presente decisione immediatamente applicabile, a norma dell'articolo 93, paragrafo 3, del regolamento (UE) 2016/679 in combinato disposto con l'articolo 8 del regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio ([153]).

8. **CONSIDERAZIONI FINALI**

(189) Il comitato europeo per la protezione dei dati ha pubblicato il proprio parere ([154]), del quale si è tenuto conto nell'elaborazione della presente decisione.

(190) Il Parlamento europeo ha adottato una risoluzione su una strategia per il commercio digitale che invita la Commissione ad attribuire la priorità all'adozione delle decisioni di adeguatezza con importanti partner commerciali e ad accelerarne i tempi, alle condizioni stabilite dal regolamento (UE) 2016/679, in quanto importante meccanismo per proteggere il trasferimento dei dati personali dall'Unione europea ([155]). Il Parlamento europeo ha adottato inoltre una risoluzione sull'adeguatezza della protezione dei dati personali offerta dal Giappone ([156]).

(191) Le misure di cui alla presente decisione sono conformi al parere del comitato istituito dall'articolo 93, paragrafo 1, del GDPR,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

1. Ai fini dell'articolo 45 del regolamento (UE) 2016/679, il Giappone garantisce un livello adeguato di protezione dei dati personali trasferiti dall'Unione europea a operatori economici che gestiscono informazioni personali in Giappone soggetti alla legge sulla protezione delle informazioni personali, quale integrata dalle norme integrative di cui all'allegato I, nonché dalle dichiarazioni, dalle garanzie e dagli impegni ufficiali che figurano nell'allegato II.

([153]) Regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione (GU L 55 del 28.2.2011, pag. 13).

([154]) Parere 28/2018 relativo al progetto di decisione di esecuzione della Commissione europea per quanto riguarda la protezione adeguata dei dati personali da parte del Giappone, adottato il 5 dicembre 2018.

([155]) Risoluzione del Parlamento europeo del 12 dicembre 2017 «Verso una strategia per il commercio digitale» (2017/2065(INI)). Cfr. in particolare il punto 8 («[…] ricorda che i dati personali possono essere trasferiti a paesi terzi senza ricorrere alle disposizioni generali negli accordi commerciali allorché sono soddisfatti i requisiti – sia attuali che futuri – di cui […] al capo V del regolamento (UE) 2016/679; riconosce che le decisioni di adeguatezza, anche quelle parziali e quelle riguardanti settori specifici, costituiscono un meccanismo fondamentale per proteggere il trasferimento di dati personali dall'UE verso un paese terzo; osserva che l'UE ha soltanto adottato decisioni di adeguatezza con 4 dei suoi 20 maggiori partner commerciali […]») e il punto 9 («invita la Commissione ad attribuire la priorità all'adozione delle decisioni di adeguatezza e ad accelerarne i tempi, a condizione che i paesi terzi garantiscano, in considerazione della loro legislazione nazionale o dei loro impegni internazionali, un livello di protezione "sostanzialmente equivalente" a quello assicurato all'interno dell'Unione […]»).

([156]) Risoluzione del Parlamento europeo del 13 dicembre 2018 «Adeguatezza della protezione dei dati personali offerta dal Giappone» (2018/2979(RSP))

2. La presente decisione non riguarda i dati personali trasferiti a destinatari che rientrano in una delle categorie seguenti, purché una delle finalità del trattamento dei dati personali corrisponda, in tutto o in parte, a uno delle rispettive finalità elencate:

a) emittenti radiotelevisive, case editrici di giornali, agenzie di comunicazione e altre organizzazioni della stampa (comprese le persone che svolgono attività di stampa per professione) purché trattino dati personali a fini di stampa;

b) persone che svolgono un'attività di scrittura professionale, purché questa preveda l'utilizzo di informazioni personali;

c) università e qualsiasi altra organizzazione o gruppo che svolge studi accademici o qualsiasi persona appartenente a tale organizzazione o gruppo, purché trattino dati personali ai fini di studi accademici;

d) istituzioni religiosi purché trattino dati personali ai fini di attività religiose (comprese tutte le attività connesse); e

e) organizzazioni politiche purché trattino dati personali ai fini dell'attività politica (comprese tutte le attività connesse).

Articolo 2

Lo Stato membro interessato informa senza indugio la Commissione quando, al fine di proteggere le persone con riguardo al trattamento dei dati personali che le riguardano, le autorità competenti negli Stati membri esercitano i poteri di cui dispongono a norma dell'articolo 58 del regolamento (UE) 2016/679 e ciò comporta la sospensione o il divieto definitivo dei flussi di dati verso uno specifico operatore economico in Giappone nell'ambito di cui all'articolo 1.

Articolo 3

1. La Commissione monitora costantemente l'applicazione del quadro giuridico su cui si basa la presente decisione, comprese le condizioni in cui sono effettuati i trasferimenti successivi, al fine di valutare se il Giappone continua a garantire un livello adeguato di protezione ai sensi dell'articolo 1.

2. Gli Stati membri e la Commissione si informano dei casi in cui la Commissione per la protezione delle informazioni personali o qualsiasi altra autorità giapponese competente non garantisce il rispetto del quadro giuridico su cui si basa la presente decisione.

3. Gli Stati membri e la Commissione si informano di qualsiasi indicazione del fatto che le ingerenze delle autorità pubbliche giapponesi nel diritto delle persone alla protezione dei dati personali che le riguardano vadano oltre quanto strettamente necessario o che contro le ingerenze di tale natura non esista una tutela giuridica efficace.

4. Entro due 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, paragrafo 1, in base a tutte le informazioni disponibili, comprese quelle ricevute nell'ambito del riesame congiunto effettuato con le autorità giapponesi pertinenti.

5. In presenza di indicazioni del fatto che non è più assicurato un adeguato livello di protezione la Commissione informa le autorità giapponesi competenti. Se necessario, essa può decidere di sospendere, modificare o abrogare la presente decisione o di limitarne l'ambito d'applicazione, in particolare in presenza di indicazioni del fatto che:

a) gli operatori economici in Giappone che hanno ricevuto dati personali dall'Unione europea nell'ambito della presente decisione non rispettano le garanzie aggiuntive previste dalle norme integrative che figurano nell'allegato I, ovvero del fatto che la vigilanza e il controllo del rispetto in questo senso sono insufficienti;

b) le autorità pubbliche giapponesi non rispettano le dichiarazioni, le garanzie e gli impegni che figurano nell'allegato II, in particolare per quanto riguarda le condizioni e le limitazioni alla raccolta dei dati personali trasferiti nell'ambito della presente decisione e all'accesso da parte delle autorità pubbliche a tali dati per motivi di contrasto penale o di sicurezza nazionale.

La Commissione può inoltre presentare detti progetti di misure se la mancanza di collaborazione del governo giapponese le impedisce di stabilire se la constatazione di cui all'articolo 1, paragrafo 1, ne risulti compromessa.

Articolo 4

Gli Stati membri sono destinatari della presente decisione.

Fatto a Bruxelles, il 23 gennaio 2019

Per la Commissione
Věra JOUROVÁ
Membro della Commissione

ALLEGATO 1

NORME INTEGRATIVE AI SENSI DELLA LEGGE SULLA PROTEZIONE DELLE INFORMAZIONI PERSONALI PER LA GESTIONE DEI DATI PERSONALI CHE SONO TRASFERITI DALL'UE IN BASE ALLA DECISIONE DI ADEGUATEZZA

Indice

[Termini]

Legge	legge sulla protezione delle informazioni personali (legge n. 57 del 2003)
ordinanza del Gabinetto	ordinanza del Gabinetto per l'attuazione della legge sulla protezione delle informazioni personali (ordinanza del Gabinetto n. 507 del 2003)
norme	norme esecutive della legge sulla protezione delle informazioni personali (norme della Commissione per la protezione delle informazioni personali n. 3 del 2016)
orientamenti sulle norme generali	orientamenti sulla legge sulla protezione delle informazioni personali (volume norme generali) (comunicazione della Commissione per la protezione delle informazioni personali n. 65 del 2015)
UE	Unione europea, compresi i suoi Stati membri e, visto l'accordo SEE, l'Islanda, il Liechtenstein e la Norvegia
GDPR	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)
decisione di adeguatezza	decisione con cui la Commissione europea constata che un dato paese terzo o un dato territorio all'interno del paese terzo ecc. garantisce un livello di protezione adeguato dei dati personali a norma dell'articolo 45 del GDPR

Ai fini della fluidità del trasferimento reciproco dei dati personali fra il Giappone e l'UE, la Commissione per la protezione delle informazioni personali ha stabilito che l'UE costituisce un "paese straniero" il cui sistema di protezione delle informazioni personali è riconosciuto, in termini di tutela dei diritti e interessi della persona, equivalente a quello giapponese a norma dell'articolo 24 della legge; contemporaneamente la Commissione europea ha stabilito che il Giappone garantisce un livello di protezione adeguato dei dati personali a norma dell'articolo 45 del GDPR.

Sarà assicurata la fluidità del trasferimento reciproco dei dati personali fra il Giappone e l'UE garantendo un elevato livello di protezione dei diritti e interessi della persona. Per assicurare tale elevato livello di protezione delle informazioni personali provenienti dall'UE ricevute in base alla decisione di adeguatezza e dato che, nonostante la considerevole convergenza, i due sistemi presentano alcune differenze di rilievo, la Commissione per la protezione delle informazioni personali ha adottato le presenti norme integrative, fondate sulla legge di attuazione ecc. della cooperazione coi governi di altri paesi, nell'intento di provvedere a che gli operatori economici responsabili gestiscano tali informazioni personali provenienti dall'UE in modo appropriato e a che gli obblighi imposti dalle norme in materia siano assolti in modo corretto ed efficace ([1]).

([1]) Articoli 4, 6, 8, 24, 60 e 78 della legge e articolo 11 delle norme.

L'articolo 6 della legge conferisce in particolare il potere di prendere i necessari provvedimenti legislativi e di altro tipo per potenziare la protezione delle informazioni personali e allineare il sistema agli standard internazionali, tramite l'adozione di norme più rigorose a integrazione e supplemento di quelle della legge e dell'ordinanza del Gabinetto. In quanto autorità competente dell'amministrazione generale della legge, la Commissione per la protezione delle informazioni personali gode quindi del potere, conferito dall'articolo 6 della legge, di adottare disposizioni più rigorose mediante le presenti norme integrative, con le quali è innalzato il livello di protezione dei diritti e interessi della persona con riguardo alla gestione dei dati personali provenienti dall'UE ricevuti in base alla decisione di adeguatezza, anche relativamente alle "informazioni personali particolarmente sensibili", ai sensi dell'articolo 2, comma 3, della legge, e ai "dati personali conservati", ai sensi dell'articolo 2, comma 7, della legge (anche in termini di periodo di conservazione applicabile).

Questo rende le norme integrative vincolanti per l'operatore economico responsabile della gestione di informazioni personali che ha ricevuto dati personali trasferiti dall'UE in base alla decisione di adeguatezza; tale operatore è quindi tenuto a conformarvisi. Dato tale carattere vincolante delle norme integrative, la Commissione per la protezione delle informazioni personali può dare esecuzione a tutti i relativi diritti e obblighi analogamente a quanto avviene per le disposizioni della legge che esse integrano con maggior rigore e/o livello di dettaglio. In caso di violazione dei diritti e obblighi sanciti dalle norme integrative, la persona può presentare ricorso al giudice esattamente come per le disposizioni della legge che esse integrano con maggior rigore e/o livello di dettaglio.

Per quanto riguarda l'esecuzione, se l'operatore economico responsabile della gestione di informazioni personali viene meno a uno o più obblighi imposti dalle norme integrative, la Commissione per la protezione delle informazioni personali ha il potere di adottare misure a norma dell'articolo 42 della legge. Quanto alle informazioni personali provenienti dall'UE ricevute in base alla decisione di adeguatezza in generale, l'inerzia, non giustificata da motivo legittimo ([2]), dell'operatore economico responsabile della gestione di informazioni personali a seguito di una raccomandazione ad agire ricevuta a norma dell'articolo 42, comma 1, della legge è considerata una violazione grave di natura imminente dei diritti e degli interessi della persona ai sensi dell'articolo 42, comma 2, della legge.

1. Informazioni personali particolarmente sensibili (articolo 2, comma 3, della legge)

Articolo 2, comma 3, della legge

3. Ai fini della presente legge per "informazioni personali particolarmente sensibili" s'intendono le informazioni personali concernenti razza, credo, status sociale, storia clinica e precedenti penali del titolare e i danni da questi subiti a causa di un reato o altre descrizioni ecc. per cui l'ordinanza del Gabinetto impone una gestione particolarmente attenta al fine di non causare ingiustamente discriminazioni, pregiudizi o altri svantaggi al titolare.

Articolo 2 dell'ordinanza del Gabinetto

Le descrizioni ecc. previste per ordinanza del Gabinetto a norma dell'articolo 2, comma 3, della legge sono le descrizioni ecc. contenenti una o più delle informazioni indicate qui di seguito (escluse quelle relative alla storia clinica o ai precedenti penali del titolare):

i) presenza di disabilità fisiche, disabilità intellettive, disabilità mentali (comprese le disabilità dello sviluppo) o altre disabilità delle funzioni fisiche o psichiche previste dalle norme della Commissione per la protezione delle informazioni personali;

ii) risultati di una visita medica o altro esame (di seguito "visita medica ecc.") effettuato sul titolare a fini di prevenzione e diagnosi precoce di una malattia da un medico o altro operatore del settore medico (di seguito "medico ecc.");

iii) fatto che, in base ai risultati della visita medica ecc. o a causa di una malattia, ferita o altra evoluzione fisica o psichica, un medico ecc. abbia dato al titolare indicazioni sul modo di migliorare lo stato fisico o psichico ovvero una terapia medica o una prescrizione medica;

iv) pronuncia nei confronti del titolare, in quanto indagato o imputato, di un provvedimento di arresto, perquisizione, sequestro o incarcerazione, di un procedimento penale o di altre procedure penali;

([2]) Per "motivo legittimo" s'intende un "evento di carattere straordinario al di fuori del controllo dell'operatore economico responsabile della gestione di informazioni personali che non può essere ragionevolmente previsto (ad esempio, catastrofi naturali) o il caso in cui la necessità di agire a seguito di una raccomandazione emanata dalla Commissione per la protezione delle informazioni personali a norma dell'articolo 42, comma 1, della legge è venuta meno poiché tale operatore ha adottato misure alternative che costituiscono un rimedio integrale della violazione.

v) adozione nei confronti del titolare, in quanto autore o autore presunto di reati contro minori a norma dell'articolo 3, comma 1, della legge sui minori, di un procedimento d'indagine, osservazione e protezione, audizione e decisione, misura cautelare o altra procedura in un caso di tutela di minore.

Articolo 5 delle norme

Costituiscono disabilità delle funzioni fisiche o psichiche previste dalle norme della Commissione per la protezione delle informazioni personali ai sensi dell'articolo 2, punto i), dell'ordinanza:

i) le disabilità fisiche indicate nella tabella allegata alla legge sul benessere delle persone con disabilità fisica (legge n. 283 del 1949);

ii) le disabilità intellettive previste dalla legge sul benessere delle persone con disabilità intellettiva (legge n. 37 del 1960);

iii) le disabilità psichiche previste dalla legge sulla salute mentale e il benessere delle persone con disabilità psichiche (legge n. 123 del 1950), comprese le disabilità dello sviluppo previste all'articolo 2, comma 1, della legge sul sostegno alle persone con disabilità dello sviluppo ed escluse le disabilità intellettive ai sensi della legge sul benessere delle persone con disabilità intellettiva;

iv) le malattie per cui non è stabilito un protocollo terapeutico o altre malattie peculiari la cui gravità stabilita per ordinanza del Gabinetto a norma dell'articolo 4, comma 1, della legge sul sostegno globale alla quotidianità e alla socialità delle persone con disabilità (legge n. 123 del 2005) è equivalente a quanto previsto dal ministro della Salute, del lavoro e del benessere nel medesimo comma.

Se i dati personali provenienti dall'UE ricevuti in base alla decisione di adeguatezza contengono dati sulla vita sessuale o l'orientamento sessuale della persona ovvero sulla sua appartenenza sindacale, che ai sensi del GDPR costituiscono categorie particolari di dati personali, è fatto obbligo all'operatore economico responsabile della gestione di informazioni personali di trattare tali dati alla stregua di informazioni personali particolarmente sensibili ai sensi dell'articolo 2, comma 3, della legge.

2. Dati personali conservati (articolo 2, comma 7, della legge)

Articolo 2, comma 7, della legge

7. Ai fini della presente legge per "dati personali conservati" s'intendono i dati personali per i quali l'operatore economico responsabile della gestione delle informazioni personali ha facoltà di divulgazione, correzione, aggiunta o cancellazione quanto al contenuto, così come di cessazione dell'utilizzo, cancellazione e cessazione della fornitura a terzi quanto ai dati stessi, ad eccezione di quelli per i quali, per ordinanza del Gabinetto, la divulgazione della presenza o assenza è considerata pregiudizievole dell'interesse pubblico o di altra natura e di quelli destinati ad essere cancellati nell'arco del periodo, di un anno al massimo, fissato con ordinanza del Gabinetto.

Articolo 4 dell'ordinanza del Gabinetto

Per ordinanza del Gabinetto costituiscono dati personali conservati ai sensi dell'articolo 2, comma 7, i dati:

i) in grado, qualora ne fosse resa nota la presenza o l'assenza, di pregiudicare la vita, l'integrità fisica o il patrimonio del titolare o di un terzo";

ii) in grado, qualora ne fosse resa nota la presenza o l'assenza, di incoraggiare o causare un atto illegale o ingiusto;

iii) in grado, qualora ne fosse resa nota la presenza o l'assenza, di compromettere la sicurezza nazionale, distruggere un rapporto di fiducia con un paese straniero o un'organizzazione internazionale, o arrecare svantaggio nei negoziati con un paese straniero o un'organizzazione internazionale;

iv) in grado, qualora ne fosse resa nota la presenza o l'assenza, di ostacolare il mantenimento della sicurezza e dell'ordine pubblici, ad esempio la prevenzione, la lotta o le indagini relative a un reato.

Articolo 5 dell'ordinanza del Gabinetto

Il periodo fissato con ordinanza del Gabinetto ai sensi dell'articolo 2, comma 7, della legge è di sei mesi.

I dati personali provenienti dall'UE ricevuti in base alla decisione di adeguatezza devono essere gestiti come dati personali conservati ai sensi dell'articolo 2, comma 7, della legge, indipendentemente dal periodo entro il quale sono destinati a essere cancellati.

I dati personali provenienti dall'UE ricevuti in base alla decisione di adeguatezza non devono essere gestiti come dati personali conservati se, per ordinanza del Gabinetto, rientrano fra i dati personali per i quali "la divulgazione della presenza o assenza è considerata pregiudizievole dell'interesse pubblico o di altra natura" (v. l'articolo 4 dell'ordinanza del Gabinetto; orientamenti sulle norme generali, "2-7. Dati personali conservati").

3. Indicazione della finalità dell'utilizzo, limitazione dovuta alla finalità dell'utilizzo (articolo 15, comma 1, articolo 16, comma 1, e articolo 26, commi 1 e 3, della legge)

Articolo 15, comma 1, della legge

1. Nel corso della propria attività l'operatore economico che gestisce informazioni personali indica nel modo più esplicito possibile la finalità con cui usa le informazioni personali (di seguito "finalità dell'utilizzo").

Articolo 16, comma 1, della legge

1. Nel corso della propria attività l'operatore economico che gestisce informazioni personali non si spinge oltre l'ambito necessario per conseguire la finalità dell'utilizzo indicata a norma dell'articolo 15 senza aver previamente ottenuto il consenso del titolare.

Articolo 26, commi 1 e 3, della legge

1. L'operatore economico responsabile della gestione di informazioni personali cui un terzo ha fornito dati personali conferma gli elementi seguenti in conformità delle norme della Commissione per la protezione delle informazioni personali: (omissis)

   i) (omissis)

   ii) circostanze in cui i dati personali sono stati acquisiti dal terzo.

3. Confermati gli elementi a norma del comma 1, l'operatore economico responsabile della gestione di informazioni personali registra, in conformità delle norme della Commissione per la protezione delle informazioni personali, la data in cui ha ricevuto i dati personali, l'avvenuta conferma e gli altri elementi previsti dalle norme della Commissione per la protezione delle informazioni personali.

Prima di potersi spingere oltre l'ambito necessario per conseguire la finalità dell'utilizzo indicata all'articolo 15, comma 1, della legge, l'operatore economico responsabile della gestione di informazioni personali deve ottenere il consenso del titolare (articolo 16, comma 1, della legge). Le norme impongono a tale operatore economico che riceve dati personali da un terzo di confermare elementi quali le circostanze in cui i dati personali sono stati acquisiti dal terzo e di tenerne una registrazione (articolo 26, commi 1 e 3, della legge).

Se l'operatore economico responsabile della gestione di informazioni personali riceve i dati personali dall'UE in base alla decisione di adeguatezza, le circostanze in cui i dati personali sono stati acquisiti, che l'articolo 26, commi 1 e 3, impone di confermare e registrare, devono indicare con quale finalità di utilizzo i dati sono stati trasferiti dall'UE.

Analogamente, se l'operatore economico responsabile della gestione di informazioni personali riceve da un suo omologo dati personali precedentemente trasferiti dall'UE in base alla decisione di adeguatezza, le circostanze in cui i dati personali sono stati acquisiti, che l'articolo 26, commi 1 e 3, impone di confermare e registrare, devono indicare con quale finalità di utilizzo i dati sono stati trasferiti.

Nei casi citati l'operatore economico responsabile della gestione di informazioni personali è tenuto a indicare la finalità d'utilizzo di detti dati personali, che deve rientrare nell'ambito della finalità di utilizzo per la quale sono stati originariamente o successivamente ricevuti, quale confermata e registrata a norma dell'articolo 26, commi 1 e 3, e a utilizzare i dati nei limiti di tale ambito (come prescritto dall'articolo 15, comma 1, e dall'articolo 16, comma 1, della legge).

4. Limitazioni della fornitura a un terzo in un paese straniero (articolo 24 della legge); articolo 11-2 delle norme)

Articolo 24 della legge

Tranne nei casi indicati in ciascuna voce dell'articolo precedente, comma 1, l'operatore economico responsabile della gestione di informazioni personali deve ottenere il consenso del titolare prima di poter fornire dati personali a un terzo (esclusa la persona che ha instaurato un sistema conforme ai criteri che, in base alle norme della Commissione per la protezione delle informazioni personali, sono necessari per poter assicurare continuativamente interventi equivalenti a quelli messi in atto da detto operatore per la gestione dei dati personali ai sensi della presente sezione - di seguito *idem*) in un paese straniero (ossia un paese o una regione esterna al territorio del Giappone - di seguito *idem*) (esclusi i paesi che, in base alle norme della Commissione per la protezione delle informazioni personali, sono paesi stranieri che hanno instaurato un sistema di protezione delle informazioni personali riconosciuto conforme a criteri equivalenti a quelli vigenti in Giappone per quanto riguarda la protezione dei diritti e degli interessi della persona - di seguito *idem*). In tal caso non si applica l'articolo precedente.

Articolo 11-2 delle norme

I criteri fissati dalle norme della Commissione per la protezione delle informazioni personali in conformità dell'articolo 24 della legge sono soddisfatti se:

i) l'operatore economico responsabile della gestione di informazioni personali e la persona cui sono forniti i dati personali provvedono a che, riguardo alla gestione di detti dati da parte di detta persona che li riceve, siano attuate, con un metodo adeguato e ragionevole, misure conformi al capo IV, sezione 1, della legge;

ii) la persona cui sono forniti i dati personali ha ottenuto il riconoscimento in base a un quadro internazionale relativo alla gestione delle informazioni personali.

Prima di poter fornire a un terzo in un paese straniero dati personali che ha ricevuto dall'Unione europea in base alla decisione di adeguatezza, l'operatore economico responsabile della gestione di informazioni personali deve ottenere il consenso del titolare, secondo quanto previsto all'articolo 24 della legge, dopo che questi ha ricevuto, in merito alle circostanze del trasferimento, le informazioni necessarie a decidere se acconsentire, escluse le ipotesi indicate nei punti da i) a iii) seguenti:

i) il terzo è ubicato in un paese che, in base alle norme, è un paese straniero che ha instaurato un sistema di protezione delle informazioni personali riconosciuto conforme a criteri equivalenti a quelli vigenti in Giappone per quanto riguarda la protezione dei diritti e degli interessi della persona;

ii) l'operatore economico responsabile della gestione di informazioni personali e la persona cui sono forniti i dati personali hanno, riguardo alla gestione di detti dati da parte del terzo destinatario, attuato, con un metodo adeguato e ragionevole (mediante un contratto, altre forme di accordi vincolanti o modalità vincolanti stabilite all'interno di un gruppo societario), misure concordate che garantiscono un livello di protezione equivalente a quello previsto dalla legge, in combinato disposto con le presenti norme;

iii) casi indicati nelle diverse voci dell'articolo 23, comma 1, della legge.

5. Informazioni trattate in forma anonima (articolo 2, comma 9, e articolo 36, commi 1 e 2, della legge)

Articolo 2, comma 9, della legge

9. Ai fini della presente legge per "informazioni trattate in forma anonima" s'intendono le informazioni sulla persona prodotte mediante un metodo che ne rende impossibile il ripristino o l'identificazione la persona, a seguito di uno degli interventi previsti ai punti seguenti per la rispettiva categoria di informazioni:

i) informazioni personali di cui al comma 1, punto i):

cancellazione parziale delle descrizioni ecc. contenute nelle informazioni personali (anche sostituendole con altre descrizioni ecc. mediante un metodo non contraddistinto da regolarità che permette di ripristinare le parti cancellate);

ii) informazioni personali di cui al comma 1, punto ii):

cancellazione totale dei codici identificativi individuali contenuti nelle informazioni personali (anche sostituendoli con altre descrizioni ecc. mediante un metodo non contraddistinto da regolarità che permette di ripristinare i codici identificativi individuali cancellati).

Articolo 36, comma 1, della legge

1. L'operatore economico responsabile della gestione di informazioni personali che produce informazioni trattate in forma anonima (limitatamente a quelle che confluiscono in banche dati di informazioni trattate in forma anonima ecc. - di seguito *idem*) tratta dette informazioni secondo i criteri che, in base alle norme della Commissione per la protezione delle informazioni personali, sono necessari per rendere impossibile l'identificazione della persona o il ripristino delle informazioni personali originarie.

Articolo 19 delle norme

I criteri stabiliti dalle norme della Commissione per la protezione delle informazioni personali a norma dell'articolo 36, comma 1, della legge sono i seguenti:

i) cancellazione totale o parziale delle descrizioni ecc. contenute nelle informazioni personali che permettono di identificare la persona (anche sostituendole con altre descrizioni ecc. mediante un metodo non contraddistinto da regolarità che permette di ripristinare le parti cancellate);

ii) cancellazione totale dei codici identificativi individuali contenuti nelle informazioni personali (anche sostituendoli con altre descrizioni ecc. mediante un metodo non contraddistinto da regolarità che permette di ripristinare i codici identificativi individuali cancellati);

iii) cancellazione dei codici (limitatamente a quelli che instaurano collegamenti fra più informazioni su cui l'operatore economico responsabile della gestione di informazioni personali lavora concretamente) che collegano le informazioni personali a quelle risultanti dagli interventi operati su di esse (anche sostituendo i codici con altri che non instaurano questo tipo di collegamento, mediante un metodo non contraddistinto da regolarità che permette di ripristinare i codici);

iv) cancellazione delle descrizioni ecc. caratteristiche (anche sostituendole con altre mediante un metodo non contraddistinto da regolarità che permette di ripristinare le descrizioni ecc. caratteristiche);

v) oltre a quanto indicato ai punti precedenti, intervento consono all'esito dell'esame delle caratteristiche ecc. delle banche dati di informazioni personali ecc., quale la differenza fra le descrizioni ecc. contenute nelle informazioni personali e quelle contenute nelle altre informazioni personali presenti nella banca dati di informazioni personali ecc. in cui sono confluite le informazioni personali.

Articolo 36, comma 2, della legge

1. L'operatore economico responsabile della gestione di informazioni personali che ha prodotto informazioni trattate in forma anonima provvede al controllo di sicurezza sulle informazioni applicando i criteri che, in base alle norme della Commissione per la protezione delle informazioni personali, sono necessari per impedire la fuga di informazioni relative a tali descrizioni ecc., di codici identificativi individuali cancellati dalle informazioni personali usate per produrre le informazioni trattate in forma anonima e di informazioni relative al metodo di trattamento applicato a norma del comma 1.

Articolo 20 delle norme

I criteri stabiliti dalle norme della Commissione per la protezione delle informazioni personali a norma dell'articolo 36, comma 2, della legge sono i seguenti:

i) definizione precisa dei poteri e delle competenze della persona che gestisce le informazioni relative alle descrizioni ecc., i codici identificativi individuali cancellati dalle informazioni personali usate per produrre le informazioni trattate in forma anonima e le informazioni relative al metodo di trattamento applicato a norma dell'articolo 36, comma 1 (limitatamente ai casi in cui le informazioni in questione permettono di ripristinare le informazioni personali originarie) (di seguito "informazioni relative al metodo di trattamento ecc.");

ii) fissazione delle norme e procedure applicabili alla gestione delle informazioni relative al metodo di trattamento ecc., adeguata gestione delle informazioni relative al metodo di trattamento ecc. in conformità delle norme e procedure, valutazione della gestione e, in esito alla valutazione, adozione delle necessarie misure di miglioramento;

iii) intervento necessario e appropriato per impedire la gestione delle informazioni relative al metodo di trattamento ecc. alla persona priva di legittimazione in tal senso.

Le informazioni personali provenienti dall'UE ricevute in base alla decisione di adeguatezza sono considerate informazioni trattate in forma anonima ai sensi dell'articolo 2, comma 9, della legge soltanto se l'operatore economico responsabile della gestione di informazioni personali interviene per rendere irreversibile l'impossibilità per chiunque di identificare la persona, anche cancellando le informazioni relative al metodo di trattamento ecc. (ossia le informazioni relative alle descrizioni ecc., i codici identificativi individuali cancellati dalle informazioni personali usate per produrre le informazioni trattate in forma anonima e le informazioni relative al metodo di trattamento applicato a norma del dell'articolo 36, comma 1, della legge (limitatamente ai casi in cui le informazioni in questione permettono di ripristinare le informazioni personali originarie)).

ALLEGATO 2

S.E. Věra Jourová, Commissaria per la Giustizia, i consumatori e la parità di genere della Commissione europea

Signora Commissario,

con grande compiacimento accolgo le discussioni costruttive tenutesi tra il Giappone e la Commissione europea ai fini dell'instaurazione di un quadro per il trasferimento dei dati personali tra il Giappone e l'UE e viceversa.

A seguito della richiesta trasmessa dalla Commissione europea al governo del Giappone, allego un documento che traccia una panoramica del quadro giuridico in materia di accesso alle informazioni da parte del governo giapponese.

Il documento riguarda le attività di vari ministeri e agenzie del governo giapponese (segretariato del gabinetto, Agenzia nazionale di polizia, Commissione per la protezione delle informazioni personali, Ministero dell'Interno e delle comunicazioni, Ministero della Giustizia, Agenzia di intelligence per la pubblica sicurezza, Ministero della Difesa), ciascuno o ciascuna dei quali è, per quanto riguarda il contenuto, responsabile dei passi di rispettiva competenza. I pertinenti ministeri e agenzie sono indicati qui di seguito con le rispettive firme.

Qualsiasi quesito sul presente documento è da porsi alla Commissione per la protezione delle informazioni personali, che coordinerà la risposta con il competente ministero o agenzia.

È mio auspicio che il presente documento possa essere d'ausilio alla Commissione europea nel processo decisionale.

Nel ringraziarLa del grande contributo apportato ai lavori, La prego di accogliere, signora Commissario, i sensi della mia più alta stima

Yoko Kamikawa

Ministro della Giustizia

Il presente documento è stato redatto dal Ministero della Giustizia e dai ministeri e agenzie competenti, elencati qui di seguito.

Koichi Hamano

Consigliere, segretariato del Gabinetto

Schunichi Kuryu

Commissario generale dell'Agenzia nazionale di polizia

Mari Sonoda

Segretario generale, Commissione per la protezione delle informazioni personali

Mitsuru Yasuda

Viceministro, Ministero dell'Interno e della comunicazione

Seimei Nakagawa

Agenzia di intelligence per la pubblica sicurezza

Kenichi Takahashi

Viceministro amministrativo della Difesa

14 Settembre 2018

Raccolta e uso delle informazioni personali da parte delle autorità pubbliche giapponesi per motivi di contrasto penale e di sicurezza nazionale

Il presente documento fornisce una panoramica del quadro giuridico per la raccolta e l'uso delle informazioni personali (in formato elettronico) da parte delle autorità pubbliche giapponesi per motivi di contrasto penale e di sicurezza nazionale (di seguito denominato «accesso da parte delle pubbliche amministrazioni»), in particolare per quanto riguarda le basi giuridiche disponibili e le condizioni (limitazioni) e le garanzie applicabili, inclusi la vigilanza indipendente e le possibilità di ricorso individuale. La presente dichiarazione, rivolta alla Commissione europea, intende esprimere l'impegno e fornire la garanzia che l'accesso da parte delle pubbliche amministrazioni alle informazioni personali trasferite dall'UE al Giappone sarà limitato a quanto necessario e proporzionato e sarà soggetto a vigilanza indipendente, e che le persone interessate potranno ottenere un risarcimento in caso di eventuali violazioni del loro diritto fondamentale al rispetto della vita privata e alla protezione dei dati. La presente dichiarazione prevede inoltre la creazione di un nuovo meccanismo di ricorso, gestito dalla Commissione per la protezione delle informazioni personali (PPC), per gestire i reclami da parte di cittadini dell'UE in materia di accesso da parte delle pubbliche amministrazioni ai loro dati personali trasferiti dall'UE al Giappone.

I. **Principi giuridici generali in materia di accesso da parte delle pubbliche amministrazioni**

In quanto esercizio di pubblici poteri, l'accesso da parte delle pubbliche amministrazioni deve essere effettuato nel pieno rispetto della legge (principio di legittimità). In Giappone le informazioni personali sono protette sia nel settore privato che nel settore pubblico da un meccanismo a più livelli.

A. Quadro costituzionale e principio della riserva di legge

L'articolo 13 della costituzione e la giurisprudenza riconoscono il diritto al rispetto della vita privata come diritto costituzionale. A tale riguardo, la Corte suprema ha statuito che è normale che le persone fisiche non vogliano che altri vengano a conoscenza delle loro informazioni personali senza un valido motivo, e che questa aspettativa dovrebbe essere protetta ([1]). Ulteriori tutele sono sancite all'articolo 21, comma 2, della costituzione, che garantisce il rispetto della segretezza delle comunicazioni, e all'articolo 35 della costituzione, che garantisce il diritto a non essere sottoposto a perquisizione e sequestro senza mandato, il che significa che la raccolta di informazioni personali, compreso l'accesso a tali informazioni, mediante mezzi forzosi deve sempre basarsi su un mandato del giudice. Tale mandato può essere emesso soltanto per l'indagine su un reato già commesso. Pertanto, nel quadro giuridico del Giappone la raccolta di informazioni mediante mezzi forzosi ai fini (non di un'indagine penale ma) della sicurezza nazionale ma non è consentita.

Inoltre, in conformità del principio della riserva di legge, la raccolta forzosa di informazioni deve essere espressamente autorizzata dalla legge. In caso di raccolta non forzosa/volontaria, le informazioni sono ottenute da fonti che possono essere consultate o ricevute liberamente in base a una richiesta di comunicazione volontaria, vale a dire una richiesta il cui adempimento non può essere imposto alle persone fisiche o giuridiche che detengono le informazioni. Tuttavia, ciò è consentito solo nella misura in cui l'autorità pubblica è competente a svolgere l'indagine, dato che ogni autorità pubblica può intervenire soltanto nell'ambito delle sue competenze amministrative previste dalla legge (indipendentemente dal fatto che le sue attività interferiscano con i diritti e le libertà delle persone fisiche). Questo principio si applica alla capacità dell'autorità di raccogliere informazioni personali.

B. Norme specifiche sulla protezione delle informazioni personali

La legge sulla protezione delle informazioni personali (APPI) e la legge sulla protezione delle informazioni personali detenute da organi amministrativi (APPIHAO), che si basano sulle disposizioni costituzionali e le precisano ulteriormente, garantiscono il diritto a informazioni personali sia nel settore privato che in quello pubblico.

L'articolo 7 dell'APPI stabilisce che la PPC formula la «politica di base in materia di protezione delle informazioni personali» (politica di base). La politica di base, adottata mediante decisione del Gabinetto del Giappone, in qualità di organo centrale del governo giapponese (primo ministro e ministri di Stato), fissa la direzione per la protezione delle informazioni personali in Giappone. In questo modo la PPC, in qualità di autorità di controllo indipendente, costituisce il «centro di comando» del sistema di protezione delle informazioni personali del Giappone.

Ogniqualvolta organi amministrativi raccolgono informazioni personali, a prescindere dal fatto che lo facciano mediante mezzi forzosi o non forzosi, essi in linea di principio ([2]) devono rispettare i requisiti previsti dall'APPIHAO. L'APPIHAO è una legge generale applicabile al trattamento delle «informazioni personali conservate» ([3]) da «organi amministrativi»(di cui

([1]) Corte suprema, sentenza del 12 settembre 2003, causa n. 1656 (2002 (Ju)).
([2]) Per quanto concerne le eccezioni relative al capo 4 dell'APPIHAO, cfr. infra, p. 16.
([3]) All'articolo 2, comma 5, dell'APPIHAO, "informazioni personali conservate" significa informazioni personali preparate o ottenute da un dipendente di un organo amministrativo nell'espletamento delle sue funzioni e detenute da tale organo amministrativo a uso organizzativo da parte dei suoi dipendenti.

all'articolo 2, comma 1, dell'APPIHAO). Essa concerne quindi anche il trattamento dei dati nel settore del contrasto penale e della sicurezza nazionale. Tra le autorità pubbliche autorizzate ad attuare l'accesso da parte delle pubbliche amministrazioni, tutte le autorità, ad eccezione della polizia prefetturale, sono pubbliche amministrazioni nazionali che rientrano nella definizione di «organi amministrativi». La gestione delle informazioni personali da parte della polizia prefetturale è disciplinato da ordinanze prefetturali ([4]) che stabiliscono principi relativi alla protezione delle informazioni personali, ai diritti e agli obblighi equivalenti a quanto previsto dall'APPIHAO.

II. **Accesso da parte delle pubbliche amministrazioni per motivi di contrasto penale**

A) Basi giuridiche e limitazioni

1) Raccolta di informazioni personali mediante mezzi forzosi

a) Basi giuridiche

A norma dell'articolo 35 della costituzione, il diritto di ogni persona all'inviolabilità del domicilio, dei propri documenti e degli effetti personali contro ingressi, perquisizioni e sequestri non deve essere compromesso, se non in base a un mandato emesso per «un motivo adeguato» e che descriva in particolare il luogo da perquisire e le cose da sequestrare. Di conseguenza, la raccolta forzosa di informazioni in formato elettronico da parte di autorità pubbliche nell'ambito di un'indagine penale può avvenire solo sulla base di un mandato. Ciò vale sia per la raccolta dei registri elettronici contenenti informazioni (personali) che per l'intercettazione delle comunicazioni in tempo reale (le cosiddette «intercettazioni»). L'unica eccezione a questa regola (che tuttavia non è pertinente nel contesto di un trasferimento elettronico di informazioni personali provenienti dall'estero) è l'articolo 220, comma 1, del codice di procedura penale ([5]), secondo il quale un magistrato, un assistente di un magistrato o un ufficiale di polizia giudiziaria possono, quando arrestano un indagato o un «trasgressore in flagranza di reato», se del caso, effettuare perquisizioni e sequestri «in loco al momento dell'arresto».

L'articolo 197, comma 1, del codice di procedura penale dispone che misure di indagine obbligatorie «non si applicano a meno che il presente codice non preveda disposizioni speciali». Per quanto riguarda la raccolta forzosa di informazioni elettroniche, le pertinenti basi giuridiche al riguardo sono l'articolo 218, comma 1, del codice di procedura penale (in base al quale un magistrato, un assistente di un magistrato o un ufficiale di polizia giudiziaria possono, se necessario ai fini dell'indagine sul reato, effettuare una perquisizione, un sequestro o un'ispezione in base a un mandato emesso da un giudice) e l'articolo 222, comma 2, del codice di procedura penale (in base al quale le misure obbligatorie per l'intercettazione delle comunicazioni elettroniche senza il consenso di una delle parti sono eseguite sulla base di altre leggi). Quest'ultima disposizione si riferisce alla legge sulle intercettazioni delle comunicazioni ai fini delle indagini giudiziarie («legge sulle intercettazioni»), che all'articolo 3, comma 1, stabilisce le condizioni alle quali le comunicazioni relative a taluni reati gravi possono essere intercettate sulla base di un mandato d'intercettazione emesso da un giudice ([6]).

Per quanto riguarda la polizia, il potere di indagine spetta in ogni caso alla polizia prefetturale, mentre l'Agenzia nazionale di polizia (NPA) non svolge indagini penali sulla base del codice di procedura penale.

b) Limitazioni

La raccolta forzosa di informazioni elettroniche è limitata dalla costituzione e dalle disposizioni autorizzative, così come interpretate dalla giurisprudenza, che prevede in particolare i criteri che i giudici devono applicare quando emettono un mandato. Inoltre, l'APPIHAO impone una serie di limitazioni applicabili sia alla raccolta che alla gestione delle informazioni (mentre le ordinanze locali riproducono in sostanza gli stessi criteri per la polizia prefetturale).

(1) Limitazioni derivanti dalla costituzione e dalle disposizioni autorizzative

A norma dell'articolo 197, comma 1, del codice di procedura penale, le disposizioni coercitive non si applicano a meno che il medesimo codice non preveda disposizioni speciali. L'articolo 218, comma 1, del codice di procedura penale

([4]) Ogni prefettura ha la propria «ordinanza prefetturale» applicabile alla protezione delle informazioni personali da parte della polizia prefetturale. Non esistono traduzioni in inglese di queste ordinanze prefetturali.

([5]) L'articolo 220, comma 1, del codice di procedura penale stabilisce che quando un magistrato, un assistente di un magistrato o un ufficiale di polizia arrestano un indagato, essi possono, se del caso, adottare le seguenti misure: a) ingresso nel domicilio di un'altra persona, ecc. per cercare l'indagato; b) perquisizione, sequestro o ispezione in loco al momento dell'arresto.

([6]) Nello specifico, la disposizione stabilisce che «il magistrato o la polizia giudiziaria possono, nei casi che rientrano in uno dei seguenti punti, quando si verifica una situazione sufficiente per sospettare che si svolgeranno comunicazioni relative alla commissione, alla preparazione, a intese su ulteriori azioni, tra cui la distruzione delle prove, istruzioni e altri scambi in merito al reato previsti da ciascuno dei suddetti punti (in prosieguo, "una serie di reati" ai punti due e tre), nonché comunicazioni che contemplano argomenti relativi a detto reato (in prosieguo, "le comunicazioni relative al reato" nel presente paragrafo) e nei casi in cui è estremamente difficile individuare l'autore del reato o chiarire le situazioni/i dettagli della perpetrazione in altro modo, intercettare le comunicazioni relative al reato, sulla base del mandato d'intercettazione emesso dal giudice, se un mezzo di comunicazione indicato da un numero di telefono e da altri numeri/codici per individuare la fonte o il destinatario della telefonata ed è utilizzato dal sospetto sulla base di un contratto con un operatore di telecomunicazioni, ecc. (fatta eccezione per quelle che possono essere ritenute non sospettate di poter essere utilizzate come "comunicazioni relative a reati"), o quando vi sono motivi per sospettare che siano utilizzate come " comunicazioni relative a reati", è possibile intercettare le comunicazioni relative al reato mediante tale mezzo di comunicazione».

stabilisce che il sequestro, ecc. possa essere effettuato sulla base di un mandato emesso da un giudice solo «se necessario ai fini dell'indagine sul reato». Sebbene i criteri per valutare la necessità non siano ulteriormente specificati dalla legge, la Corte suprema ([7]) ha stabilito che, nel valutare la necessità di disposizioni, il giudice dovrebbe effettuare una valutazione complessiva, tenendo conto, in particolare, dei seguenti elementi:

a) la gravità del reato e le circostanze nelle quali è stato commesso;

b) il valore e l'importanza dei materiali sequestrati quali elementi di prova;

c) la probabilità di occultamento o distruzione dei materiali sequestrati;

d) l'entità degli svantaggi causati dal sequestro;

e) altre condizioni connesse.

Limitazioni discendono anche dall'obbligo di cui all'articolo 35 della costituzione di presentare «un motivo adeguato». In virtù del criterio del «motivo adeguato», è possibile emettere un mandato se: 1) vi è la necessità di indagini penali (cfr. la sentenza della Corte suprema del 18 marzo 1969, causa n. 100 (1968 (Shi)) di cui sopra); 2) vi è una situazione in cui si ritiene che l'indagato (l'imputato) abbia commesso un reato (articolo 156, comma 1, delle norme di procedura penale) ([8]); 3) il mandato d'indagine relativo al corpo, agli effetti, al domicilio o a qualsiasi altro luogo di una persona diversa dall'imputato dovrebbe essere emesso solo quando è ragionevole supporre che esistano gli effetti da sequestrare (articolo 102, comma 2, del codice di procedura penale). Quando il giudice ritiene che le prove documentali fornite dalle autorità inquirenti presentino motivi insufficienti per sospettare un reato, respingere la richiesta di mandato. Va osservato, a tal riguardo, che ai sensi della legge sulla repressione della criminalità organizzata e il controllo dei proventi della criminalità, le «attività preparatorie per commettere» un reato pianificato (ad esempio, la preparazione del denaro per commettere un reato di terrorismo) costituiscono di per sé reati e possono pertanto essere oggetto di indagini obbligatorie sulla base di un mandato.

Infine, qualora il mandato di indagine riguardi il corpo, gli effetti, il domicilio o qualsiasi altro luogo di una persona diversa dall'indagato o dall'imputato, esso è emesso solo quando è ragionevole supporre che esistano gli effetti da sequestrare (articolo 102, comma 2, e articolo 222, comma 1, del codice di procedura penale).

Per quanto riguarda specificamente l'intercettazione di comunicazioni ai fini dell'indagine penale sulla base della legge sulle intercettazioni, quest'ultima può essere effettuata soltanto qualora siano soddisfatte le condizioni rigorose di cui all'articolo 3, comma 1. Ai sensi di tale disposizione, l'intercettazione richiede sempre un mandato preventivo del giudice, che può essere emesso solo in un numero limitato di situazioni ([9]).

2) Limitazioni derivanti dall'APPIHAO

Per quanto riguarda la raccolta ([10]) e la gestione ulteriore (compresi, in particolare, la conservazione, la gestione e l'uso) di informazioni personali da parte di organi amministrativi, l'APPIHAO prevede, in particolare, le limitazioni elencate di seguito.

a) Ai sensi dell'articolo 3, comma 1, dell'APPIHAO, gli organi amministrativi possono conservare informazioni personali solo qualora tale conservazione sia necessaria per l'esercizio delle funzioni di loro competenza secondo quanto previsto dalle disposizioni legislative e regolamentari. In caso di conservazione sono inoltre tenuti a specificare (per quanto possibile) la finalità dell'uso delle informazioni personali. A norma dell'articolo 3, commi 2 e 3, dell'APPIHAO, gli organi amministrativi non conservano informazioni personali oltre quanto necessario per il raggiungimento della finalità d'uso così specificata, e non modificano la finalità d'uso al di là di quanto può essere considerato ragionevolmente pertinente per la finalità originaria.

b) L'articolo 5 dell'APPIHAO dispone che il direttore di un organo amministrativo si adoperi per mantenere esatte e aggiornate le informazioni personali conservate, nei limiti necessari per il raggiungimento della finalità d'uso.

c) L'articolo 6, comma 1, dell'APPIHAO dispone che il direttore di un organo amministrativo adotti le misure necessarie per la prevenzione di fughe, perdite o danni e per l'adeguata gestione delle informazioni personali conservate.

d) A norma dell'articolo 7 dell'APPIHAO, nessun dipendente (ed ex dipendente) comunica le informazioni personali acquisite a un'altra persona senza un giustificato motivo, né utilizza tali informazioni per una finalità ingiusta.

([7]) Sentenza del 18 marzo 1969, causa n. 100 (1968 (Shi))

([8]) L'articolo 156, comma 1, delle norme di procedura penale dispone quanto segue: «Nel presentare la richiesta di cui al punto 1) del precedente articolo, il richiedente fornisce gli elementi sulla base dei quali l'indagato o l'imputato dovrebbe essere considerato l'autore del reato.»

([9]) Cfr. nota a piè di pagina 6.

([10]) L'articolo 3, commi 1 e 2, dell'APPIHAO limita la portata della conservazione e, in tal modo, anche la raccolta di informazioni personali.

e) Inoltre, l'articolo 8, comma 1, dell'APPIHAO dispone che il direttore di un organo amministrativo, salvo se altrimenti previsto da disposizioni legislative e regolamentari, non utilizza né fornisce ad un'altra persona per scopi diversi dalla finalità d'uso specificata le informazioni personali conservate. L'articolo 8, comma 2, prevede eccezioni a questa regola in situazioni specifiche, che tuttavia si applicano soltanto se tale comunicazione eccezionale non è suscettibile di arrecare un «ingiusto» pregiudizio ai diritti e agli interessi dell'interessato o di un terzo.

f) A norma dell'articolo 9 dell'APPIHAO, quando le informazioni personali conservate sono fornite ad un'altra persona, il direttore di un organo amministrativo, se del caso, impone restrizioni sulle finalità o sulle modalità d'uso, o qualsiasi altra restrizione necessaria; esso può altresì chiedere alla persona destinataria di prendere le misure necessarie alla prevenzione delle fughe e all'adeguata gestione delle informazioni.

g) L'articolo 48 dell'APPIHAO dispone che il direttore di un organo amministrativo si adoperi per trattare in modo corretto e rapido tutti i reclami concernenti il trattamento delle informazioni personali.

2) Raccolta di informazioni personali mediante richieste di cooperazione volontaria (mezzi di indagine volontari)

a) Base giuridica

A prescindere dall'uso di mezzi forzosi, le informazioni personali sono ottenute o da una fonte liberamente accessibile o mediante comunicazione volontaria, anche da parte degli operatori economici che detengono tali informazioni.

Per quanto riguarda quest'ultima modalità, l'articolo 197, comma 2, del codice di procedura penale conferisce alla magistratura e alla polizia giudiziaria il potere di presentare «richieste di informazioni scritte nelle indagini» (i cosiddetti «moduli di richiesta»). Ai sensi del codice di procedura penale le persone indagate sono tenute a riferire alle autorità inquirenti, ma non vi è modo di obbligarle in tal senso, se gli uffici pubblici o le organizzazioni pubbliche e/o private che hanno ricevuto la richiesta si rifiutano di ottemperare. Se non rispondono alle richieste, non possono essere irrogate sanzioni penali o di altro tipo. Se le autorità inquirenti considerano le informazioni richieste indispensabili, dovranno ottenerle mediante perquisizioni e sequestri sulla base di un mandato del giudice.

Data la crescente consapevolezza delle persone per quanto riguarda i loro diritti relativi alla vita privata, nonché il carico di lavoro generato da tali richieste, gli operatori economici sono sempre più prudenti nel rispondere a tali richieste ([11]). Al momento di decidere se cooperare, gli operatori economici tengono conto, in particolare, della natura delle informazioni richieste, del rapporto che intrattengono con la persona interessata, dei rischi per la loro reputazione, dei rischi di contenzioso, ecc.

b) Limitazioni

Per quanto riguarda la raccolta forzosa di informazioni in formato elettronico, i mezzi di indagine volontari sono limitati dalla costituzione, così come interpretata dalla giurisprudenza, e dalle disposizioni autorizzative. Inoltre, gli operatori economici non sono autorizzati per legge a comunicare informazioni in determinate situazioni. Infine, l'APPIHAO prevede una serie di limitazioni applicabili sia alla raccolta che alla gestione delle informazioni (mentre le ordinanze locali riproducono in sostanza gli stessi criteri per la polizia prefetturale).

1) Limitazioni derivanti dalla costituzione e dalle disposizioni autorizzative

Tenendo conto delle finalità dell'articolo 13 della costituzione, in una decisione del 24 dicembre 1969 (1965 (A) n. 1187) e in una del 15 aprile 2008 (2007 (A) n. 839) la Corte suprema ha imposto limiti alle indagini volontarie condotte dalle autorità inquirenti. Sebbene tali decisioni riguardino casi in cui le informazioni personali (sotto forma di immagini) sono state raccolte mediante fotografie/riprese video, le risultanze sono pertinenti per le indagini volontarie (non obbligatorie) che interferiscono con la vita privata delle persone in generale. Pertanto, per quanto riguarda la raccolta di informazioni personali mediante mezzi di indagine volontari, tali decisioni devono essere applicate e rispettate, tenendo conto delle circostanze specifiche di ciascun caso.

In base alle suddette decisioni, la legittimità dell'indagine volontaria dipende dal rispetto di tre criteri:

— il «sospetto di reato» (occorre verificare se sia stato commesso un reato);

— la «necessità delle indagini» (occorre valutare se la richiesta rientri nell'ambito di quanto necessario ai fini dell'indagine);

([11]) Cfr. anche la comunicazione dell'Agenzia nazionale di polizia del 7 dicembre 1999 (pag. 9) che riporta la medesima indicazione.

— l'«adeguatezza del metodo» (occorre valutare se i mezzi di indagine volontaria siano «adeguati» o ragionevoli ai fini del raggiungimento dell'obiettivo dell'indagine) ([12]).

In generale, tenendo conto dei tre criteri summenzionati, la legittimità dell'indagine volontaria è giudicata alla luce del fatto che possa essere considerata ragionevole secondo convenzioni socialmente accettate.

L'obbligo di «necessità» dell'indagine discende direttamente anche dall'articolo 197 del codice di procedura penale ed è stato confermato nelle istruzioni impartite dall'Agenzia nazionale di polizia (NPA) alla polizia prefetturale per quanto riguarda l'uso del «modulo di richiesta». La comunicazione dell'NPA del 7 dicembre 1999 stabilisce una serie di limitazioni procedurali, tra cui l'obbligo di utilizzare «moduli di richiesta» solo se necessario ai fini dell'indagine. Inoltre, l'articolo 197, comma 1, del codice di procedura penale si limita alle indagini penali e può quindi essere applicato solo in presenza del sospetto concreto di un reato già commesso. Tale base giuridica non è invece applicabile ai fini della raccolta e dell'uso di informazioni personali, qualora non sia stata ancora commessa alcuna violazione della legge.

2) Limitazioni relative a taluni operatori economici

In determinati settori si applicano limitazioni supplementari sulla base delle tutele previste da altre disposizioni.

In primo luogo, le autorità inquirenti e gli operatori di telecomunicazioni che dispongono di informazioni personali hanno il dovere di rispettare la segretezza delle comunicazioni garantita dall'articolo 21, comma 2, della costituzione ([13]). Inoltre, gli operatori di telecomunicazioni hanno lo stesso dovere a norma dell'articolo 4 della legge sulle imprese di telecomunicazione ([14]). In conformità agli orientamenti sulla protezione delle informazioni personali nel settore delle telecomunicazioni, pubblicati dal ministero dell'Interno e delle comunicazioni (MIC) e basati sulla costituzione e sulla legge sulle imprese di telecomunicazione, nei casi in cui è in gioco la segretezza delle comunicazioni, gli operatori di telecomunicazioni non devono rivelare a terzi informazioni personali riguardanti la segretezza delle comunicazioni, salvo nei casi in cui abbiano ottenuto il consenso dell'interessato o possano fare affidamento su una delle «cause di giustificazione» dell'inosservanza del codice penale. Queste ultime si riferiscono agli «atti giustificabili» (articolo 35 del codice penale), alla «legittima difesa» (articolo 36 del codice penale) e alla «prevenzione di un pericolo esistente» (articolo 37 del codice penale). Ai sensi del codice penale per «atti giustificabili» si intendono solo gli atti di un operatore di telecomunicazioni mediante i quali esso si conforma alle misure obbligatorie dello Stato, il che esclude l'indagine volontaria. Pertanto, se le autorità inquirenti chiedono informazioni personali sulla base di un «modulo di richiesta» (articolo 197, comma 2, del codice di procedura penale), all'operatore di telecomunicazioni è fatto divieto di comunicare i dati.

In secondo luogo, gli operatori economici sono tenuti a respingere le richieste di cooperazione volontaria ove la legge vieti loro di comunicare informazioni personali. A titolo esemplificativo, ciò comprende i casi in cui l'operatore ha il dovere di rispettare la riservatezza delle informazioni, ad esempio ai sensi dell'articolo 134 del codice penale ([15]).

3) Limitazioni basate sull'APPIHAO

Per quanto riguarda la raccolta e l'ulteriore gestione delle informazioni personali da parte di organi amministrativi, l'APPIHAO prevede limitazioni come illustrato alla sezione II.A.1, lettera b), punto 2. Limitazioni equivalenti discendono dalle ordinanze prefetturali applicabili alla polizia prefetturale.

B) Vigilanza

1) Vigilanza giudiziaria

Per quanto riguarda la raccolta di informazioni personali con mezzi forzosi, essa deve essere basata su un mandato ([16]) ed è quindi soggetta all'esame preventivo da parte di un giudice. Nel caso in cui l'indagine sia illecita, un giudice può escludere tali prove nel successivo processo penale del caso. Una persona può chiedere tale esclusione nel corso del processo sostenendo che l'indagine era illecita.

([12]) La gravità del reato e l'urgenza sono fattori pertinenti ai fini della valutazione dell '«adeguatezza del metodo».

([13]) L'articolo 21, comma 2, della costituzione recita: «Non è ammessa la censura, né la violazione della segretezza dei mezzi di comunicazione».

([14]) L'articolo 4 della legge sulle imprese di telecomunicazione recita: «1) Non è ammessa la violazione della segretezza delle comunicazioni gestite dall'operatore di telecomunicazioni. 2) Chiunque sia attivo nel settore delle telecomunicazioni non divulga durante la propria attività i segreti di cui sia venuto a conoscenza nell'ambito delle comunicazioni gestite dall'operatore di telecomunicazioni. La stessa disposizione si applica anche dopo la cessazione dalle funzioni».

([15]) L'articolo 134 del codice penale recita: «1) Quando un medico, un farmacista, un distributore di prodotti farmaceutici, un'ostetrica, un procuratore legale, un avvocato, un notaio o qualsiasi altra persona che abbia esercitato in precedenza tale professione comunica, senza giustificati motivi, le informazioni riservate di un'altra persona delle quali è venuto a conoscenza durante l'esercizio di tale professione, è inflitta una pena detentiva con obbligo di lavoro fino a sei mesi o una pena pecuniaria di importo non superiore a 100 000 yen. 2) La stessa disposizione si applica nel caso in cui una persona che esercita o ha esercitato un ufficio religioso comunichi, senza giustificati motivi, informazioni riservate su un'altra persona delle quali è venuta a conoscenza nel corso di tali attività religiose».

([16]) Per quanto riguarda l'eccezione a questa norma, si veda la nota 5.

2) Vigilanza basata sull'APPIHAO

In Giappone il ministro o il direttore di un ministero o di un'agenzia ha poteri di vigilanza e di esecuzione in forza dell'APPIHAO, mentre il ministro dell'Interno e delle comunicazioni può svolgere indagini sull'esecuzione dell'APPIHAO da parte di tutti gli altri ministeri.

Se lo ritiene necessario per il conseguimento delle finalità dell'APPIHAO – ad esempio in base all'indagine sullo stato dell'esecuzione dell'APPIHAO ([17]), al trattamento dei reclami o alle indagini su uno dei suoi centri di informazione globale – il ministro dell'Interno e delle comunicazioni può chiedere al direttore di un organo amministrativo di presentare spiegazioni e materiali in merito alla gestione delle informazioni personali da parte dell'organo amministrativo in questione, sulla base dell'articolo 50 dell'APPIHAO. Il ministro può formulare pareri rivolti al direttore dell'organo amministrativo in merito al trattamento delle informazioni personali nell'organo amministrativo qualora lo ritenga necessario per conseguire le finalità dell'APPIHAO. Inoltre, il ministro può, ad esempio, chiedere una revisione delle misure mediante gli interventi che può attuare ai sensi degli articoli 50 e 51 della medesima legge, quando si sospetta che si sia verificata una violazione o un'inadeguata attuazione della legge. Ciò contribuisce a garantire l'applicazione uniforme dell'APPIHAO e l'osservanza della stessa.

3) Vigilanza sulla polizia da parte delle Commissioni di sicurezza pubblica

Per quanto riguarda l'amministrazione di polizia, l'NPA è soggetta alla vigilanza della Commissione nazionale per la sicurezza pubblica, mentre la polizia prefetturale è soggetta alla vigilanza di una delle Commissioni prefetturali di sicurezza pubblica istituite in ogni prefettura. Ciascuno di questi organi di vigilanza garantisce la gestione democratica e la neutralità politica dell'amministrazione di polizia.

La Commissione nazionale per la sicurezza pubblica è responsabile delle questioni di sua competenza ai sensi della legge sulla polizia e di altre norme. Ciò comprende la nomina del commissario generale dell'NPA e degli alti operatori di polizia locali, nonché l'istituzione di politiche globali che definiscano gli orientamenti o le misure di base per l'amministrazione dell'NPA.

In virtù della legge sulla polizia le Commissioni prefetturali di sicurezza pubblica sono composte da rappresentanti dei cittadini della prefettura interessata e gestiscono la polizia prefetturale in qualità di consiglio indipendente. I membri sono nominati dal governatore prefetturale con il consenso dell'assemblea prefetturale in virtù dell'articolo 39 della legge sulla polizia. Il loro mandato è di tre anni e può essere revocato contro la loro volontà solo per ragioni specifiche elencate dalla legge (ad esempio l'incapacità di svolgere le proprie funzioni, la violazione dei propri doveri, la condotta scorretta, ecc.), garantendo così l'indipendenza dei membri (cfr. articoli 40 e 41 della legge sulla polizia). Inoltre, al fine di garantire la loro neutralità politica, l'articolo 42 della legge sulla polizia vieta ai membri delle Commissioni, durante il loro mandato, di essere membri di un organo legislativo, di diventare membri esecutivi di un partito politico o di qualsiasi altro organo politico o di impegnarsi attivamente in movimenti politici. Anche se ciascuna Commissione rientra nella sfera di competenza del rispettivo governatore prefetturale, quest'ultimo non ha il potere di impartire istruzioni per l'esercizio delle sue funzioni.

A norma dell'articolo 38, comma 3, in combinato disposto con l'articolo 2 e l'articolo 36, comma 2, della legge sulla polizia, le Commissioni prefetturali di sicurezza pubblica sono responsabili della «protezione dei diritti e della libertà delle persone». A tal fine esse ricevono le relazioni trasmesse dai direttori della polizia prefetturale relative alle attività esercitate nell'ambito della loro sfera di competenza, anche durante riunioni regolari che si svolgono tre o quattro volte al mese. Le Commissioni forniscono orientamenti su tali questioni mediante l'elaborazione di politiche globali.

Inoltre, nell'ambito della loro funzione di controllo, le Commissioni prefetturali di sicurezza pubblica possono impartire istruzioni alla polizia prefetturale in singoli casi concreti, qualora lo ritengano necessario nel contesto di un'ispezione sulle attività della polizia prefetturale o in caso di condotta scorretta del personale della stessa. Inoltre le Commissioni, qualora lo ritengano necessario, possono designare un membro che esamini lo stato di attuazione dell'istruzione impartita (articolo 43-2 della legge sulla polizia).

([17]) Al fine di garantire la trasparenza e facilitare la vigilanza da parte del MIC, il direttore di un organo amministrativo è tenuto, ai sensi dell'articolo 11 dell'APPIHAO, a registrare ciascun elemento prescritto all'articolo 10, comma 1, dell'APPIHAO, ossia la denominazione dell'organo amministrativo che conserva il fascicolo, le finalità dell'utilizzo del fascicolo, il metodo di raccolta delle informazioni personali, ecc. (il cosiddetto «registro dei fascicoli delle informazioni personali»). Tuttavia, i fascicoli di informazioni a carattere personale contemplati dall'articolo 10, comma 2, dell'APPIHAO, quali quelli preparati o ottenuti nell'ambito di un'indagine penale o quelli riguardanti questioni attinenti alla sicurezza nazionale, sono esentati dall'obbligo di notifica al MIC e dall'obbligo di essere inseriti nel registro pubblico. In ogni caso, ai sensi dell'articolo 7 della legge sulla gestione dei documenti e degli archivi pubblici, il direttore di un organo amministrativo è sempre tenuto a registrare la classificazione, il titolo, il periodo di conservazione, il luogo di conservazione, ecc. dei documenti amministrativi («registro dei fascicoli dei documenti amministrativi»). Per entrambi i registri, le informazioni contenute nell'indice sono pubblicate su internet e consentono alle persone di verificare che tipo di informazioni personali contiene il fascicolo e quale organo amministrativo le conserva.

4) Vigilanza da parte della Dieta

La Dieta può svolgere indagini in relazione alle attività delle autorità pubbliche e, a tal fine, può chiedere di produrre documenti e convocare testimoni a deporre (articolo 62 della costituzione). In tale contesto, la competente commissione della Dieta può esaminare l'adeguatezza delle attività di raccolta di informazioni condotte dalla polizia.

Tali poteri sono ulteriormente specificati nella legge sulla Dieta. A norma dell'articolo 104 della suddetta legge, la Dieta può esigere che il Gabinetto e le agenzie pubbliche presentino le relazioni e i dati necessari ai fini dello svolgimento dell'indagine. Inoltre, i membri della Dieta possono presentare «richieste scritte» ai sensi dell'articolo 74 della legge sulla Dieta. Tali richieste devono essere approvate dal presidente della camera e, in linea di principio, il Gabinetto deve rispondere per iscritto entro sette giorni (qualora sia impossibile rispondere entro tale termine, la circostanza deve essere giustificata e deve essere fissato un nuovo termine, articolo 75 della legge sulla Dieta). In passato, le «richieste scritte» della Dieta hanno riguardato anche la gestione di informazioni personali da parte dell'amministrazione ([18]).

C) Ricorso individuale

Ai sensi dell'articolo 32 della costituzione del Giappone, nessuno può vedersi negare il diritto di accesso alla giustizia. Inoltre, l'articolo 17 della costituzione garantisce a ogni persona il diritto di citare in giudizio lo Stato o un ente pubblico per ottenere un risarcimento (come previsto dalla legge) nel caso in cui abbia subito danni a causa dell'atto illecito di un pubblico ufficiale.

1) Ricorso giurisdizionale contro la raccolta forzosa di informazioni sulla base di un mandato (articolo 430 del codice di procedura penale)

Ai sensi dell'articolo 430, comma 2, del codice di procedura penale, chiunque non sia soddisfatto delle misure adottate da un ufficiale di polizia concernenti il sequestro di elementi (in particolare se contengono informazioni personali) sulla base di un mandato, può presentare istanza (il cosiddetto «quasi reclamo») dinanzi al giudice competente affinché tali misure siano «revocate o modificate».

Tale istanza può essere proposta senza dover attendere la conclusione del caso. Se ritiene che il sequestro non fosse necessario o che vi siano altri motivi per ritenere il sequestro illecito, il giudice può ordinare la revoca o la modifica di tali misure.

2) Ricorso giurisdizionale ai sensi del codice di procedura civile e della legge sul ricorso avverso lo Stato

Se una persona ritiene che sia stato violato il suo diritto al rispetto della vita privata sancito dall'articolo 13 della Costituzione, può promuovere un'azione civile con la quale chiede la cancellazione delle informazioni personali raccolte nell'ambito di un'indagine penale.

Inoltre, una persona può promuovere un'azione di risarcimento danni fondata sulla legge sul ricorso avverso lo Stato in combinato disposto con i pertinenti articoli del codice civile qualora ritenga che il suo diritto al rispetto della vita privata sia stato violato e che la raccolta di informazioni personali che la riguardano o attività di sorveglianza nei suoi confronti le abbiano cagionato un danno ([19]). Poiché il «danno» oggetto del ricorso per risarcimento non si limita al danno materiale (articolo 710 del codice civile), può comprendere anche il «disagio psichico». L'importo dell'indennizzo di tale danno morale sarà valutato dal giudice sulla base di una libera valutazione che tiene conto di fattori diversi in ciascuna causa ([20]).

L'articolo 1, comma 1, della legge sul ricorso avverso lo Stato stabilisce il diritto all'indennizzo laddove i) il dipendente pubblico che esercita funzioni di pubblico ufficiale dello Stato o di un ente pubblico ii) nell'esercizio delle sue funzioni, iii) per dolo o colpa, iv) illegalmente, v) abbia cagionato un danno a un'altra persona.

La persona deve avviare l'azione conformemente al codice di procedura civile. Le norme vigenti prevedono che l'azione vada avviata dinanzi al giudice che ha competenza per il luogo in cui è stato commesso l'illecito.

([18]) Cfr. ad esempio la richiesta scritta della camera dei consiglieri n. 92 del 27 marzo 2009 relativa alla gestione delle informazioni raccolte nel contesto delle indagini penali, in particolare le violazioni degli obblighi di riservatezza da parte della polizia e delle autorità responsabili dell'azione penale.

([19]) Un esempio di questo tipo di azione è la causa nota come «Causa dell'elenco dell'Agenzia della difesa» (tribunale distrettuale di Niigata, decisione dell'11 maggio 2006, (2002(Wa) No.514)). La causa riguardava un funzionario dell'Agenzia della difesa che aveva preparato, conservato e distribuito un elenco con i nominativi di chi aveva presentato domanda di comunicazione di documenti amministrativi all'Agenzia della difesa. L'elenco riportava informazioni personali della parte attrice. Sostenendo che si configurava violazione della sua vita privata e del suo diritto all'informazione, la parte attrice ha chiesto al convenuto di versare un indennizzo ai sensi dell'articolo 1, comma 1, della legge sul ricorso avverso lo Stato. La richiesta è stata parzialmente accolta dal giudice che ha riconosciuto alla parte attrice un risarcimento parziale.

([20]) Corte suprema, decisione del 5 aprile 1910 (1910(O) N.71).

3) Ricorso individuale avverso indagini illecite/indebite della polizia: reclamo alla Commissione prefetturale di sicurezza pubblica (articolo 79 della legge sulla polizia)

A norma dell'articolo 79 della legge sulla polizia ([21]), come ulteriormente precisato in una istruzione dal direttore dell'NPA alla polizia prefetturale e alle Commissioni prefetturali di sicurezza pubblica ([22]), le persone possono presentare un reclamo scritto ([23]) alla competente Commissione prefetturale di sicurezza pubblica in merito a qualsivoglia comportamento illecito o scorretto di un operatore di polizia nell'esercizio delle sue funzioni, anche per quanto riguarda la raccolta e l'utilizzo di informazioni personali. La Commissione prefetturale tratta lealmente i reclami in conformità alla legislazione e alle ordinanze locali e comunica per iscritto al reclamante l'esito dell'istruttoria.

In virtù dei poteri di controllo che le sono conferiti dall'articolo 38, comma 3, della legge sulla polizia, la Commissione prefetturale di sicurezza pubblica emana un'istruzione per la polizia prefetturale affinché questa indaghi sui fatti, attui le misure necessarie secondo l'esito dell'istruttoria e riferisca i risultati alla Commissione. Laddove lo ritenga necessario, la Commissione prefetturale può inoltre emanare un'istruzione in merito alla gestione del reclamo, ad esempio se giudica insufficiente l'indagine svolta dalla polizia. Queste modalità attuative sono descritte nella comunicazione che l'NPA ha indirizzato ai capi della polizia prefetturale.

La comunicazione al reclamante dell'esito dell'istruttoria tiene altresì conto dei rapporti di polizia sull'indagine e delle misure adottate su richiesta della Commissione prefetturale.

4) Ricorso individuale ai sensi dell'APPIHAO e del codice di procedura penale

a) APPIHAO

Ai sensi dell'articolo 48 dell'APPIHAO, gli organi amministrativi devono adoperarsi per trattare in modo corretto e rapido tutti i reclami concernenti la gestione di informazioni personali. Per mettere a disposizione delle persone informazioni consolidate (ad esempio sui loro diritti in materia di comunicazione, rettifica e sospensione dell'utilizzo ai sensi dell'APPIHAO) e offrire un punto di contatto per le domande di informazioni, il MIC, sulla base dell'articolo 47, comma 2, dell'APPIHAO, ha istituito in ciascuna prefettura un centro di informazione globale sulla comunicazione delle informazioni/protezione delle informazioni personali, cui possono rivolgersi anche i non residenti. A titolo di esempio, nell'esercizio 2017 (da aprile 2017 a marzo 2018) i centri di informazione globale hanno risposto in totale a 5186 domande di informazioni.

Gli articoli 12 e 27 dell'APPIHAO riconoscono alle persone il diritto di chiedere la comunicazione e la rettifica delle informazioni personali conservate. Inoltre, ai sensi dell'articolo 36 dell'APPIHAO, le persone possono chiedere la sospensione dell'utilizzo o la cancellazione delle loro informazioni personali conservate laddove l'organo amministrativo non abbia ottenuto tali informazioni in modo lecito, oppure le conservi o utilizzi in violazione della legge.

Tuttavia, le informazioni personali raccolte (o sulla base di un mandato o tramite un «modulo di richiesta») e conservate a fini di indagine penale ([24]), rientrano generalmente nella categoria delle «informazioni personali registrate in documenti relativi ai processi e ai beni sequestrati». Tali informazioni personali sono pertanto escluse dall'ambito di applicazione dei diritti individuali del capo 4 dell'APPIHAO ai sensi dell'articolo 53-2 del codice di procedura penale ([25]). Il trattamento di tali informazioni personali e i diritti della persona riguardo all'accesso e alla rettifica sono invece disciplinati da norme

([21]) Articolo 79 della legge sulla polizia (estratto):
1. Chiunque abbia motivo di dolersi del personale della polizia prefetturale nell'esercizio delle sue funzioni può presentare un reclamo scritto alla Commissione prefetturale di sicurezza pubblica secondo la procedura prescritta nell'ordinanza della Commissione nazionale per la sicurezza pubblica.
2. La Commissione prefetturale di sicurezza pubblica che ha ricevuto un reclamo di cui al precedente comma lo tratta lealmente in conformità alla legislazione e alle ordinanze locali e comunica per iscritto al reclamante l'esito dell'istruttoria, tranne nei seguenti casi:
   1) se può essere stabilito che il reclamo è stato presentato al fine di ostacolare il legittimo esercizio delle funzioni della polizia prefetturale;
   2) se l'attuale luogo di residenza del reclamante è ignoto;
   3) se può essere stabilito che il reclamo è stato presentato congiuntamente ad altri reclamanti ai quali è già stato comunicato l'esito del reclamo congiunto.

([22]) NPA, comunicazione sulla corretta gestione dei reclami riguardanti l'esercizio delle funzioni degli operatori di polizia, 13 aprile 2001, e suo allegato 1 «Norme per l'interpretazione e l'attuazione dell'articolo 79 della legge sulla polizia».

([23]) Conformemente alla comunicazione dell'NPA (cfr. nota precedente), le persone che incontrano difficoltà nella stesura del reclamo scritto ricevono assistenza. Tra i casi per cui è prevista espressamente tale possibilità figurano i cittadini stranieri.

([24]) D'altro canto, certi documenti non sono classificati come «documenti relativi ai processi» in quanto non sono di per sé informazioni ottenute in base a un mandato o a richieste scritte di informazioni su questioni oggetto d'indagine, bensì sono creati sulla base di tali documenti. In questo caso, alle informazioni private non si applica l'articolo 45, comma 1, dell'APPIHAO e pertanto esse non sono escluse dall'ambito di applicazione del capo 4 dell'APPIHAO.

([25]) L'articolo 53-2, comma 2, del codice di procedura penale stabilisce che le disposizioni del capo IV dell'APPIHAO non si applicano alle informazioni personali registrate in documenti relativi ai processi e ai beni sequestrati.

particolari ai sensi del codice di procedura penale e della legge sui fascicoli definitivi dei casi penali (cfr. infra) ([26]). L'esclusione è giustificata da vari fattori quali la tutela della vita privata delle persone interessate, la segretezza delle indagini e il regolare svolgimento del processo penale. Fatto salvo quanto sopra, rimangono applicabili le disposizioni del capo 2 dell'APPIHAO che disciplinano i principi relativi alla gestione di tali informazioni.

b) Codice di procedura penale

Ai sensi del codice di procedura penale, le possibilità di accesso alle informazioni personali raccolte ai fini di un'indagine penale dipendono sia dalla fase del procedimento che dal ruolo della persona nell'indagine (indagato, imputato, vittima, ecc.).

In deroga alla norma dell'articolo 47 del codice di procedura penale secondo la quale i documenti relativi al processo non sono resi pubblici prima dell'inizio del processo stesso (poiché questo potrebbe violare l'onorabilità e/o la vita privata delle persone interessate e ostacolare le indagini/il processo), in linea di principio è consentito alla vittima di visionare tali informazioni nella misura in cui ciò è considerato ragionevole tenuto conto della finalità della disposizione dell'articolo 47 del codice di procedura penale ([27]).

Gli indagati, dal canto loro, di norma verranno a sapere di essere oggetto di indagine penale al momento dell'interrogatorio da parte della polizia giudiziaria o del magistrato. Se successivamente il magistrato decide di non avviare l'azione penale, ne dà tempestiva comunicazione all'indagato su richiesta di quest'ultimo (articolo 259 del codice di procedura penale).

Se invece decide di avviare l'azione penale, il magistrato dà all'imputato o al suo legale la possibilità di visionare gli elementi di prova prima di chiederne l'esame da parte del giudice (articolo 299 del codice di procedura penale). Questo consente all'imputato di verificare le informazioni personali che lo riguardano, raccolte nell'ambito dell'indagine penale.

Infine, la protezione delle informazioni personali raccolte nell'ambito di un'indagine penale, sia che si tratti di un indagato, dell'imputato o di qualsiasi altra persona (ad esempio una vittima di reato) è garantita dall'obbligo di riservatezza (articolo 100 della legge sulla pubblica amministrazione nazionale) e dalla minaccia di sanzione in caso di fuga di informazioni riservate gestite nell'esercizio di funzioni di pubblica amministrazione (articolo 109, punto xii), della legge sulla pubblica amministrazione nazionale).

5) Ricorso individuale avverso indagini illecite/indebite di autorità pubbliche: reclamo alla PPC

A norma dell'articolo 6 dell'APPI, il governo adotta i provvedimenti necessari, in collaborazione con i governi dei paesi terzi, per costruire un sistema di norme in materia di informazioni personali allineato agli standard internazionali per mezzo della promozione della cooperazione con le organizzazioni internazionali e altri consessi internazionali. Fondandosi su tale disposizione, la politica di base in materia di protezione delle informazioni personali (adottata con decisione del Gabinetto) delega alla PPC, in quanto autorità competente dell'amministrazione generale dell'APPI, il potere di adottare le misure necessarie a colmare le differenze tra i sistemi e le operazioni del Giappone e quelli del paese straniero interessato, al fine di assicurare la gestione appropriata delle informazioni personali pervenute da tale paese.

Inoltre, come stabilito dall'articolo 61, punti i) e ii) dell'APPI, alla PPC è affidato il compito di formulare e promuovere una politica di base, nonché di svolgere un ruolo di mediazione nell'ambito dei reclami presentati nei confronti di operatori economici. Infine, gli organi amministrativi hanno stretti contatti e cooperano tra di loro (articolo 80 dell'APPI).

Sulla base di tali disposizioni, la PPC gestirà i reclami presentati dalle persone come segue:

a) la persona che ha motivo di sospettare che i suoi dati trasferiti dall'UE siano stati raccolti o utilizzati dalle autorità pubbliche del Giappone, ivi comprese le autorità responsabili delle attività di cui al capo II e al capo III del presente dichiarazione, in violazione delle norme vigenti, comprese quelle cui si applica la presente dichiarazione, può presentare un reclamo alla PPC (personalmente o attraverso la propria autorità di protezione dei dati);

b) la PPC gestisce il reclamo, anche avvalendosi dei poteri conferitile dall'articolo 6, dall'articolo 61, punto ii), e dall'articolo 80, dell'APPI, e ne dà comunicazione alle autorità pubbliche competenti, compresi i pertinenti organismi di vigilanza.

([26]) Ai sensi del codice di procedura penale e della legge sui fascicoli definitivi dei casi penali, l'accesso ai beni sequestrati e la relativa rettifica nonché i documenti/le informazioni personali riguardanti i processi penali sono disciplinati da un sistema di norme unico e caratterizzante che mira a tutelare la vita privata delle persone interessate, la segretezza delle indagini, il regolare svolgimento del processo penale, ecc.

([27]) Più specificamente, ai fini di una maggiore tutela delle vittime di reati, in linea di principio è loro consentito visionare le informazioni relative agli elementi di prova oggettivi riguardanti l'archiviazione dei casi che prevedono la partecipazione della vittima ai sensi dell'articolo 316-33 ss. del codice di procedura penale.

Tali autorità sono tenute a cooperare con la PPC ai sensi dell'articolo 80 dell'APPI, anche fornendo le necessarie informazioni e il materiale pertinente, in modo che la PPC possa valutare se la raccolta o il successivo utilizzo di informazioni personali siano avvenuti in conformità alle norme applicabili. Nell'effettuare la valutazione, la PPC coopera con il MIC;

c) qualora la valutazione indichi che è avvenuta una violazione delle norme applicabili, la cooperazione delle autorità pubbliche con la PPC prevede l'obbligo di porre rimedio alla violazione.

In caso di raccolta illecita di informazioni personali ai sensi delle norme vigenti, il rimedio comprende la cancellazione delle informazioni personali raccolte.

In caso di violazione delle norme applicabili, la PPC confermerà inoltre, prima di concludere la valutazione, che la violazione è stata completamente sanata;

d) una volta conclusa la valutazione, la PPC dà comunicazione alla persona dei risultati entro un lasso di tempo ragionevole, comprese, se del caso, le misure correttive adottate. Tramite tale comunicazione, la PPC informa altresì la persona della possibilità di chiedere conferma dei risultati all'autorità pubblica competente e indica l'autorità cui occorre presentare tale richiesta di conferma.

È possibile limitare la comunicazione di informazioni dettagliate sui risultati della valutazione purché sussistano motivi fondati per ritenere che possa presentare un rischio per l'indagine in corso.

Laddove il reclamo abbia per oggetto la raccolta ovvero l'utilizzo di dati personali nel settore del contrasto penale, qualora la valutazione indichi che è stato avviato una procedimento riguardante le informazioni personali della persona e che questo si è concluso, la PPC informerà la persona che il fascicolo può essere visionato a norma dell'articolo 53 del codice di procedura penale e dell'articolo 4 della legge sui fascicoli definitivi dei casi penali.

Laddove la valutazione indichi che una persona è indagata nell'ambito di un procedimento penale, la PPC informerà l'interessato di questo fatto nonché della possibilità di presentare richiesta ai sensi dell'articolo 259 del codice di procedura penale;

e) se una persona continua a non essere soddisfatta del risultato del procedimento, può rivolgersi alla PPC, che informa la persona delle varie possibilità e dei dettagli delle procedure per ottenere rimedio ai sensi delle disposizioni legislative e regolamentari giapponesi. La PPC fornirà alla persona sostegno, comprese la consulenza e l'assistenza per avviare ulteriori azioni dinanzi all'organo amministrativo o giurisdizionale competente.

III. **Accesso da parte delle pubbliche amministrazioni per motivi di sicurezza nazionale**

A. Basi giuridiche e limitazioni alla raccolta di informazioni personali

1) Basi giuridiche della raccolta da parte del ministero/dell'agenzia interessato/a

Come indicato sopra, la raccolta di informazioni personali per motivi di sicurezza nazionale da parte di organi amministrativi deve rientrare nell'ambito di applicazione della loro competenza amministrativa.

In Giappone non vi sono norme che consentano la raccolta di informazioni con mezzi forzosi soltanto per motivi di sicurezza nazionale. A norma dell'articolo 35 della costituzione, è possibile raccogliere informazioni personali forzosamente esclusivamente sulla base di un mandato emesso da un'autorità giurisdizionale per le indagini di un reato. Tale mandato può pertanto essere emesso soltanto ai fini di un'indagine penale. Ciò significa che il sistema giuridico giapponese non consente la raccolta di informazioni/l'accesso alle informazioni per motivi di sicurezza nazionale con mezzi forzosi. Di contro, nel settore della sicurezza nazionale, i ministeri/le agenzie interessati/e possono ottenere informazioni soltanto da fonti liberamente accessibili o riceverle da operatori economici o persone fisiche mediante comunicazione volontaria. Gli operatori economici che ricevano una richiesta di cooperazione volontaria non hanno l'obbligo giuridico di fornire le informazioni e, pertanto, non rischiano conseguenze negative in caso di rifiuto.

Vi sono una serie di dipartimenti e agenzie ministeriali che hanno responsabilità nel settore della sicurezza nazionale.

1) Segretariato del Gabinetto

Il segretariato del Gabinetto raccoglie e ricerca informazioni concernenti importanti politiche del Gabinetto ([28]) di cui all'articolo 12-2 della legge sul Gabinetto ([29]). Il segretariato non ha tuttavia il potere di raccogliere informazioni personali direttamente dagli operatori economici. Esso raccoglie, incorpora, analizza e valuta informazioni provenienti, ad esempio, da fonti aperte e altre autorità pubbliche.

2) NPA/polizia prefetturale

La polizia prefetturale di ciascuna prefettura è autorizzata a raccogliere informazioni entro l'ambito di applicazione delle proprie competenze ai sensi dell'articolo 2 della legge sulla polizia. Può accadere che l'NPA raccolga direttamente informazioni entro l'ambito di applicazione della propria competenza conformemente alla legge sulla polizia. Ciò riguarda in particolare le attività dell'Ufficio di sicurezza e del Dipartimento di intelligence e affari esteri dell'NPA. A norma dell'articolo 24 della legge sulla polizia, l'Ufficio di sicurezza è responsabile delle questioni concernenti la polizia di sicurezza ([30]) e il Dipartimento di intelligence e affari esteri di quelle concernenti cittadini stranieri e cittadini giapponesi con attività che hanno sede in paesi stranieri.

3) Agenzia di intelligence per la pubblica sicurezza (PSIA)

L'applicazione della legge sulla prevenzione delle attività sovversive (SAPA) e della legge sul controllo delle organizzazioni che hanno commesso omicidi di massa indiscriminati (ACO) rientra principalmente nelle competenze dell'Agenzia di intelligence per la pubblica sicurezza (PSIA) che è un'agenzia del ministero della Giustizia.

La SAPA e l'ACO stabiliscono che, a condizioni rigorose, possono essere adottate disposizioni amministrative (ossia misure che stabiliscono, ad esempio, la limitazione delle attività delle organizzazioni interessate e il loro scioglimento) contro organizzazioni che commettono gravi atti («attività terroristica sovversiva» o «omicidi di massa indiscriminati») che violano la «sicurezza pubblica» o il «sistema fondamentale della società» ai sensi della costituzione. L'"attività terroristica sovversiva" rientra nell'ambito di applicazione della SAPA (cfr. articolo 4 relativo ad attività quali l'insurrezione, l'istigazione dell'aggressione straniera, l'omicidio con finalità politiche), mentre l'ACO riguarda gli «omicidi di massa indiscriminati» (cfr. articolo 4 dell'ACO). Possono essere soggette alle disposizioni della SAPA o dell'ACO soltanto organizzazioni individuate con precisione che rappresentano una minaccia interna o esterna specifica alla sicurezza pubblica.

A tal fine la SAPA e l'ACO prevedono poteri giuridici di indagine. I fondamentali poteri di indagine degli operatori della PSIA (PSIO) sono previsti dall'articolo 27 della SAPA e dall'articolo 29 dell'ACO. La PSIA conduce le indagini a norma di tali disposizioni, purché esse siano necessarie ai fini delle summenzionate disposizioni in materia di controllo delle organizzazioni (ad esempio, gruppi di sinistra radicale, la setta *Aum Shinrikyo* ed alcuni gruppi giapponesi molto vicini alla Corea del Nord sono stati portati come esempi di indagini passate). Tuttavia tali indagini non possono avvalersi di mezzi forzosi e le organizzazioni che detengono informazioni personali non possono essere obbligate a fornirle.

La raccolta e l'utilizzo delle informazioni comunicate alla PSIA su base volontaria sono soggetti alle garanzie e alle limitazioni pertinenti stabilite dalla legge, quali la segretezza delle comunicazioni garantita dalla costituzione e le norme sulla gestione delle informazioni personali a norma dell'APPIHAO.

4) Ministero della Difesa (MOD)

Per quanto riguarda la raccolta di informazioni da parte del ministero della Difesa (MOD), il MOD raccoglie informazioni sulla base degli articoli 3 e 4 della legge sull'istituzione del MOD per quanto necessario all'esercizio degli affari che rientrano nella sua competenza amministrativa, con particolare riguardo alla difesa e alla protezione, agli interventi intrapresi dalle forze di autodifesa nonché al dispiegamento delle forze di autodifesa terrestre, marina e aerea. Il MOD può raccogliere tali informazioni esclusivamente mediante cooperazione volontaria e da fonti liberamente accessibili, ma non raccoglie informazioni sul pubblico in generale.

2) Limitazioni e garanzie

a) Limitazioni di legge

1) Limitazioni generali basate sull'APPIHAO

L'APPIHAO è una legge generale che si applica alla raccolta e alla gestione di informazioni personali da parte di organi amministrativi in ogni settore di attività di detti organi. Le limitazioni e le garanzie descritte nella sezione II.A.1, lettera b), punto 2, si applicano anche, ad esempio, alla conservazione delle informazioni personali nel settore della sicurezza nazionale.

([28]) Sono condotte dall'Ufficio per l'intelligence e la ricerca del Gabinetto sulla base dell'articolo 4 dell'Ordinanza sull'organizzazione del segretariato del Gabinetto.

([29]) Ciò comprende «la raccolta e la ricerca di intelligence concernente importanti politiche del Gabinetto».

([30]) La polizia di sicurezza è responsabile delle attività di controllo della criminalità relative alla sicurezza pubblica e all'interesse nazionale. Ciò comprende il controllo della criminalità e la raccolta di informazioni sull'attività illegale di gruppi di estrema sinistra e destra e sulle attività dannose contro il Giappone.

2) Limitazioni specifiche applicabili alla polizia (NPA e polizia prefetturale)

Come specificato sopra nella sezione relativa alla raccolta di informazioni per motivi di contrasto penale, la polizia può raccogliere informazioni esclusivamente nell'ambito di applicazione delle proprie competenze e, quando lo fa, può agire, a norma dell'articolo 2, paragrafo 2, della legge sulla polizia, soltanto «limitandosi strettamente» all'espletamento dei propri doveri e in modo «imparziale, *super partes*, equo e scevro da pregiudizi». Non deve inoltre «mai abusare dei propri poteri in alcun modo che interferisca nei diritti e nelle libertà di una persona garantiti dalla costituzione del Giappone».

3) Limitazioni specifiche applicabili alla PSIA

L'articolo 3 della SAPA e l'articolo 3 dell'ACO stabiliscono che le indagini svolte ai sensi di tali norme sono condotte solo nella misura minima necessaria a conseguire le finalità perseguite e non devono in alcun caso essere effettuate in modo limitare da «irragionevolmente» i diritti umani fondamentali. Inoltre, ai sensi dell'articolo 45 della SAPA e dell'articolo 42 dell'ACO, l'abuso di potere da parte di un operatore della PSIA costituisce un reato punibile con sanzioni penali più severe rispetto agli abusi di potere «generali» in altri settori della pubblica amministrazione.

4) Limitazioni specifiche applicabili al MOD

Per quanto riguarda la raccolta di informazioni da parte del MOD, come indicato all'articolo 4 della legge sull'istituzione del MOD, essa è limitata a quanto «necessario» per svolgere i compiti riguardanti 1) la difesa e la protezione, 2) gli interventi che dovranno intraprendere le forze di autodifesa, 3) l'organizzazione, il numero dei membri del personale, le strutture, le attrezzature e il dispiegamento delle forze di autodifesa terrestre, marina e aerea.

b) Altre limitazioni

Come spiegato nella sezione II.A.2, lettera b), punto 1, riguardo alle indagini penali, dalla giurisprudenza della Corte suprema emerge che, affinché possa essere presentata a un operatore economico una richiesta di cooperazione volontaria, questa deve essere necessaria per le indagini su un sospetto di reato e deve essere ragionevole ai fini del raggiungimento dell'obiettivo dell'indagine.

Sebbene le indagini condotte dalle autorità inquirenti nel settore della sicurezza nazionale differiscano dalle indagini condotte dalle autorità omologhe nel settore dell'esecuzione della legge, per quanto riguarda sia la base giuridica che la finalità, i principi centrali di «necessità delle indagini» e di «adeguatezza del metodo» si applicano in modo analogo al settore della sicurezza nazionale e devono essere rispettati tenendo adeguatamente conto delle circostanze specifiche di ciascun caso.

La combinazione delle summenzionate limitazioni garantisce che la raccolta e il trattamento delle informazioni avvengano soltanto per quanto necessario allo svolgimento delle funzioni specifiche dell'autorità pubblica competente nonché sulla base di minacce specifiche. Ciò esclude la raccolta o l'accesso in modo massiccio e indiscriminato a informazioni personali per ragioni di sicurezza nazionale.

B. Vigilanza

1) Vigilanza basata sull'APPIHAO

Come spiegato nella sezione II.B.2, nella pubblica amministrazione giapponese, il ministro o il direttore del ministero o di un'agenzia è investito del potere di vigilare e di garantire il rispetto dell'APPIHAO nel proprio ministero o nella propria agenzia. Il ministro dell'Interno e delle comunicazioni può inoltre svolgere indagini sullo stato dell'esecuzione dell'APPIHAO, chiedere a ciascun ministro di presentare materiali e spiegazioni sulla base degli articoli 49 e 50 dell'APPIHAO, formulare pareri rivolti a ciascun ministro a norma dell'articolo 51 dell'APPIHAO. Ad esempio, il ministro dell'Interno e delle comunicazioni può chiedere una revisione delle misure mediante gli interventi di cui agli articoli 50 e 51 dell'APPIHAO.

2) Vigilanza sulla polizia da parte delle Commissioni prefetturali di sicurezza pubblica

Come spiegato nella sezione «II. Accesso da parte delle pubbliche amministrazioni per motivi di contrasto penale», le Commissioni prefetturali di sicurezza pubblica supervisionano le attività della polizia prefetturale.

Per quanto riguarda l'NPA, le funzioni di supervisione sono esercitate dalla Commissione nazionale di sicurezza pubblica. A norma dell'articolo 5 della legge sulla polizia, tale commissione è responsabile, in particolare, della «protezione dei diritti e delle libertà delle persone». A tal fine, elabora, in particolare politiche globali che fissino norme per l'amministrazione delle questioni previste in ciascuna voce dell'articolo 5, paragrafo 4, della legge della polizia e che stabiliscano altre istruzioni o misure di base che dovrebbero essere utilizzate nello svolgimento di tali attività. La Commissione nazionale di sicurezza pubblica ha lo stesso grado di indipendenza delle Commissioni prefetturali di sicurezza pubblica.

3) Vigilanza del MOD mediante l'Ispettorato generale per il rispetto degli obblighi normativi

L'Ispettorato generale per il rispetto degli obblighi normativi (IGO) è un ufficio indipendente all'interno del MOD ed è sotto la diretta supervisione del ministro della Difesa, ai sensi dell'articolo 29 della legge sull'istituzione del MOD. L'IGO può effettuare ispezioni per verificare il rispetto delle disposizioni legislative e regolamentari da parte del personale del MOD. Tali ispezione sono denominate «ispezioni di difesa».

L'IGO svolge ispezioni dal punto di vista di un ufficio indipendente, in modo da garantire il rispetto delle norme da parte dell'intero ministero, comprese le forze di autodifesa. Esso svolge le proprie funzioni indipendentemente dai dipartimenti operativi del MOD. Dopo un'ispezione, l'IGO ne riferisce senza indugio i risultati, e le misure migliorative necessarie, direttamente al ministro della Difesa. Sulla base della relazione dell'IGO, il ministro della Difesa può emettere ordinanze per attuare le misure necessarie a porre rimedio alla situazione. Il viceministro aggiunto è responsabile dell'attuazione di tali misure e deve riferire al ministro della Difesa sullo stato di avanzamento della stessa.

Come misura di trasparenza volontaria, le risultanze delle ispezioni di difesa sono ora pubblicate sul sito internet del MOD (sebbene non sia imposto dalla legge).

Vi sono tre categorie di ispezioni di difesa:

(i) ispezioni di difesa regolari, condotte periodicamente ([31]);

(ii) ispezioni di difesa di controllo, condotte per verificare se le misure migliorative sono state effettivamente adottate;

(iii) ispezioni di difesa speciali, condotte per questioni specifiche e ordinate dal ministro della Difesa.

Nel contesto di tali ispezioni l'ispettore generale può, ad esempio, chiedere relazioni da parte dell'ufficio interessato, domandare la presentazione di documenti, effettuare l'accesso in loco per condurre l'ispezione, chiedere spiegazioni al viceministro aggiunto. Tenuto conto della natura delle sue funzioni di ispezione, l'IGO è diretto da esperti del settore legale di altissimo grado (ex procuratore generale).

4) Vigilanza della PSIA

La PSIA svolge ispezioni regolari e speciali delle operazioni dei suoi singoli dipartimenti e uffici (ad esempio, Dipartimento di intelligence per la sicurezza pubblica, Uffici e Unità distaccate di intelligence per la sicurezza pubblica). Ai fini delle ispezioni regolari, un direttore generale aggiunto e/o un direttore sono designati come ispettore/i. Tali ispezioni riguardano anche la gestione delle informazioni personali.

5) Vigilanza da parte della Dieta

Per quanto riguarda la raccolta di informazioni per motivi di contrasto penale, la Dieta, attraverso il suo comitato competente, può esaminare la liceità delle attività di raccolta delle informazioni nel settore della sicurezza nazionale. I poteri di indagine della Dieta si fondano sull'articolo 62 della costituzione e sugli articoli 74 e 104 della legge sulla Dieta.

C) Ricorso individuale

Il ricorso individuale può essere esercitato con gli stessi mezzi disponibili nel settore del contrasto penale. Ciò comprende anche il nuovo meccanismo di ricorso, amministrato e sorvegliato dalla PPC, per la gestione e la risoluzione dei reclami presentati da persone fisiche dell'UE. A tal fine si rimanda ai passaggi pertinenti della sezione II.C.

Sono inoltre disponibili mezzi specifici di ricorso individuale per il settore della sicurezza nazionale.

Le informazioni personali raccolte da un organo amministrativo per motivi di sicurezza nazionale sono soggette alle disposizioni del capo 4 dell'APPIHAO, che comprende il diritto a chiedere la comunicazione (articolo 12), la correzione (comprese l'aggiunta o la cancellazione) delle informazioni personali conservate di una persona (articolo 27) nonché il diritto a chiedere la sospensione dell'utilizzo delle informazioni personali nel caso in cui l'organo amministrativo abbia

([31]) A titolo esemplificativo di un'ispezione pertinente ai fini delle questioni oggetto della presente dichiarazione, si può citare l'ispezione di difesa regolare del 2016 concernente la «Consapevolezza/preparazione relativa al rispetto della legge», in quanto la protezione delle informazioni personali costituiva uno dei punti focali dell'ispezione. Più in particolare, l'ispezione ha riguardato, tra l'altro, lo stato della gestione e della conservazione delle informazioni personali. Nella sua relazione l'IGO ha individuato diversi aspetti inadeguati relativi alla gestione delle informazioni personali che dovrebbero essere migliorati, come la mancata protezione dei dati mediante password. La relazione è disponibile sul sito del MOD.

ottenuto le informazioni in questione in modo illegale (articolo 36). Ciò premesso, nel settore della sicurezza nazionale, l'esercizio di tali diritti è soggetto a determinate limitazioni: le richieste di comunicazione, di correzione o di sospensione non saranno accolte se riguardano «informazioni per le quali il direttore di un organo amministrativo abbia fondati motivi di ritenere che la comunicazione possa arrecare un pregiudizio alla sicurezza nazionale, provocare un danno alla relazione di fiducia reciproca con un altro paese o a un'organizzazione internazionale o causare uno svantaggio nei negoziati con un altro Stato o un'organizzazione internazionale» (articolo 14, punto iv)). Non tutte le raccolte volontarie di informazioni relative alla sicurezza nazionale rientrano pertanto in tale eccezione, in quanto quest'ultima richiede sempre una valutazione concreta dei rischi legati alla loro comunicazione.

Inoltre, se la richiesta di una persona è rifiutata con la motivazione che le informazioni interessate sono considerate non comunicabili ai sensi dell'articolo 14, punto iv), la persona può presentare un ricorso amministrativo per il riesame di tale decisione, sostenendo, ad esempio, che le condizioni di cui all'articolo 14, punto iv), non sono soddisfatte nel caso in questione. In tal caso, prima di prendere una decisione, il direttore dell'organo amministrativo interessato consulta la Commissione per il riesame della comunicazione di informazioni e della protezione delle informazioni personali che esaminerà il ricorso da un punto di vista indipendente. La commissione è un organo altamente specializzato e indipendente i cui membri sono nominati dal primo ministro, tra le persone con un livello molto elevato di competenze, con l'approvazione di entrambe le camere della Dieta ([32]). La commissione detiene forti poteri di indagine, compresa la possibilità di chiedere documenti e la comunicazione delle informazioni personali in questione, emettere deliberazioni a porte chiuse e applicare la procedura mediante indice Vaughn ([33]). La commissione redige poi una relazione scritta che è trasmessa alla persona interessata ([34]). Le risultanze contenute nella relazione sono rese pubbliche. Sebbene la relazione, da un punto di vista formale, non sia giuridicamente vincolante, l'organo amministrativo interessato vi si conforma quasi sempre ([35]).

Infine, a norma dell'articolo 3, comma 3, della legge in materia di contenzioso amministrativo, la persona può avviare un'azione giudiziaria al fine di ottenere la revoca della decisione presa dall'organo amministrativo di non comunicare le informazioni personali.

IV. **Riesame periodico**

Nel quadro del riesame periodico della decisione di adeguatezza, la PPC e la Commissione europea si scambiano informazioni sul trattamento dei dati alle condizioni previste dalla constatazione di adeguatezza, comprese quelle stabilite nella presente dichiarazione.

([32]) Cfr. articolo 4 della legge sull'istituzione della Commissione per il riesame della comunicazione di informazioni e della protezione delle informazioni personali.

([33]) Cfr. articolo 9 della legge sull'istituzione della Commissione per il riesame della comunicazione di informazioni e della protezione delle informazioni personali.

([34]) Cfr. articolo 16 della legge sull'istituzione della Commissione per il riesame della comunicazione di informazioni e della protezione delle informazioni personali.

([35]) Negli ultimi tre anni non vi sono precedenti in cui l'organo amministrativo interessato abbia preso una decisione difforme rispetto alle conclusioni della Commissione. In precedenza i casi in cui ciò si è verificato sono stati estremamente rari: solo due casi su 2 000 dal 2005 (anno in cui è entrata in vigore l'APPIHAO). Quando l'organo amministrativo prende una decisione che differisce dalle conclusioni della commissione, a norma dell'articolo 50, paragrafo 1, voce 4, della legge per il riesame dei ricorsi amministrativi come applicato con la sostituzione dell'articolo 42, comma 2, dell'APPIHAO, ne indica chiaramente i motivi.