Parere 28/2018

relativo al progetto di decisione di esecuzione della Commissione europea

sull'adeguata protezione dei dati personali in Giappone

Adottato il 5 dicembre 2018

Sommario

Commented [ITDPA1]: To be amended in line with amended titles and sub-titles

Il comitato europeo per la protezione dei dati

visto l'articolo 70, paragrafo 1, lettera s), del regolamento 2016/679/UE 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 (in appresso: il "RGPD"),

visto l'accordo SEE e in particolare l'allegato XI e il protocollo n. 37 dello stesso, come modificato dalla decisione del Comitato misto SEE n. 154/2018 del 6 luglio 2018,

visti l'articolo 12 e l'articolo 22 del proprio regolamento interno del 25 maggio 2018,

HA ADOTTATO IL SEGUENTE PARERE:

1 SINTESI

1. La Commissione europea ha approvato il progetto di decisione di esecuzione sull'adeguata protezione dei dati personali da parte del Giappone ai sensi del regolamento generale sulla protezione dei dati (in appresso: RGPD)[1] il 5 settembre 2018[2]. A seguito di ciò, la Commissione europea ha avviato la procedura per la sua adozione formale.

2. Il 25 settembre 2018, la Commissione europea ha chiesto il parere del comitato europeo per la protezione dei dati ("CEPD")[3]. La Commissione è stata invitata a fornire al CEPD tutta la documentazione necessaria con riguardo a tale paese, inclusa qualsiasi pertinente corrispondenza con il governo del Giappone.

3. Alla luce delle discussioni che si sono tenute con il CEPD, la Commissione europea ha modificato due volte il suo progetto di decisione di adeguatezza e ha inviato la sua ultima versione il 13 novembre 2018[4][.] Il CEPD ha basato il presente parere su questa ultima versione del progetto di decisione di esecuzione (in appresso: "il progetto di decisione di adeguatezza").

4. La valutazione del CEPD sul livello di protezione garantito dalla decisione di adeguatezza della Commissione è stata effettuata sulla base dell'esame della decisione stessa nonché dell'analisi della documentazione messa a disposizione[5]- dalla Commissione[6].

5. Il CEPD si è concentrato sulla valutazione sia degli aspetti commerciali del progetto di decisione di adeguatezza sia dell'accesso da parte del governo ai dati personali trasferiti dall'UE ai fini

[1] Regolamento (UE) n. 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.
[2] Vedi il comunicato stampa http://europa.eu/rapid/press-release_IP-18-5433_en.htm.
[3] Ai sensi dell'articolo 70, paragrafo 1, lettera s), del RGPD.
[4] Per la versione aggiornata del progetto di decisione di esecuzione della Commissione europea, vedere l'allegato I del parere del CEPD.
[5] Il CEPD ha basato la sua analisi sulle traduzioni fornite dalle autorità giapponesi, verificate dalla Commissione europea[.]
[6] Per l'elenco dei documenti non forniti dalla Commissione europea al CEPD, vedere l'allegato II del parere del CEPD.

dell'applicazione della legge e della sicurezza nazionale, compresi i rimedi giuridici a disposizione dei singoli dell'UE. Il CEPD ha anche valutato se le garanzie previste dal quadro giuridico giapponese siano in atto ed efficaci.

6. Il CEPD ha utilizzato come riferimento principale per questo lavoro i criteri di riferimento per l'adeguatezza[7] da esso adottati nel febbraio 2018.

1.1 Aree di convergenza

7. L'obiettivo principale del CEPD è stato quello di fornire un parere alla Commissione europea sul livello di protezione garantito agli interessati nel contesto giapponese. È importante riconoscere che il CEPD non si aspetta che il quadro giuridico giapponese duplichi la normativa europea sulla protezione dei dati.

8. Tuttavia il CEPD ricorda che, affinché si possa ritenere che la legislazione del paese terzo fornisca un livello di protezione adeguato, la giurisprudenza della CGUE nonché l'articolo 45 del RGPD richiedono che detta legislazione debba essere conforme all'essenza dei principi fondamentali sanciti nel medesimo regolamento. Negli ambiti della protezione dei dati, il CEPD rileva inoltre che vi sono conformità in settori importanti tra il RGPD e il quadro giuridico giapponese con riguardo a talune disposizioni fondamentali, come l'esattezza e la minimizzazione dei dati, le limitazioni alla conservazione, la sicurezza dei dati, le limitazioni della finalità, e il requisito dell'esistenza di un'autorità di controllo indipendente, la Commissione per la protezione delle informazioni personali (PPC).

9. In aggiunta a quanto sopra, il CEPD accoglie con favore gli sforzi compiuti dalla Commissione europea e dalle autorità giapponesi intesi a garantire che il Giappone fornisca un livello di protezione adeguato a quello del RGPD, in particolare colmando le distanze tra il RGPD e il quadro di protezione dei dati del Giappone tramite l'adozione da parte della PPC di Norme integrative, applicabili solo ai dati personali trasferiti dall'UE in Giappone – le 'Supplementary Rules', appunto "Norme integrative". Per esempio, il CEPD osserva che la PPC ha acconsentito a trattare ulteriori categorie di dati come dati sensibili (ai sensi della legislazione giapponese, i dati sensibili non includono l'orientamento sessuale né l'appartenenza sindacale). Inoltre, le Norme integrative garantiscono che i diritti degli interessati si applicheranno a tutti i dati personali trasferiti dall'UE, indipendentemente dal periodo di conservazione (mentre l'ordinamento giuridico giapponese prevede che i diritti degli interessati non possono essere fatti valere per i dati personali dei quali è prevista la cancellazione entro un periodo di sei mesi).

10. Il CEPD rileva inoltre l'impegno della Commissione europea nel rafforzamento della decisione di adeguatezza in risposta alle preoccupazioni sollevate dal Comitato stesso.

1.2 Le problematiche di carattere generale

11. Rimangono però da affrontare alcune problematiche e il CEPD suggerisce le seguenti come le principali aree del sistema giapponese che dovrebbero essere rafforzate e monitorate attentamente.

12. La prima riguarda il monitoraggio di questa nuova architettura di adeguatezza, che associa un quadro giuridico esistente a specifiche Norme integrative, al fine di garantire che si tratti di un sistema sostenibile e affidabile che non darà luogo a **questioni pratiche relative alla concreta ed efficiente ottemperanza** da parte degli organismi giapponesi e all'applicazione della normativa da parte della PPC.

[7] WP254, criteri di riferimento per l'adeguatezza, 6 febbraio 2018.

13. In secondo luogo, il CEPD prende atto dei ripetuti impegni e rassicurazioni della Commissione europea e delle autorità giapponesi per quanto riguarda la natura vincolante ed esecutiva delle Norme integrative, e invita contestualmente la Commissione europea a **monitorare in modo continuo la loro natura vincolante e la loro effettiva applicazione in Giappone**, in quanto il loro valore giuridico è un elemento assolutamente essenziale dell'adeguatezza UE - Giappone. Per quanto riguarda le linee-guida della PPC, il CEPD accoglierebbe con favore un chiarimento nel progetto di decisione di adeguatezza in relazione alla **loro natura vincolante e chiede alla Commissione di vigilare attentamente su questo aspetto** [8].

1.3 Aspetti commerciali specifici

14. In riferimento agli aspetti commerciali del progetto di decisione di adeguatezza UE - Giappone, il CEPD nutre specifiche preoccupazioni e vorrebbe chiedere chiarimenti su alcuni elementi importanti.

1.3.1 Preoccupazioni del CEPD relative a principi fondamentali della protezione dei dati

15. Il CEPD accoglie con favore il fatto che le Norme integrative escludano che i dati personali trasferiti dall'UE possano essere ulteriormente trasferiti in un paese terzo sulla base del sistema APEC CBPR. In aggiunta, il CEPD riconosce che nel suo nuovo progetto di decisione di adeguatezza, la Commissione europea si è impegnata a sospendere la decisione di adeguatezza qualora trasferimenti ulteriori non garantiscano più la continuità della protezione.

16. Ai sensi della legislazione giapponese, una delle basi giuridiche dei trasferimenti ulteriori è il riconoscimento che un paese terzo fornisce un livello di protezione adeguato a quello del Giappone. Tuttavia, la valutazione dell'adeguatezza di un paese terzo da parte del Giappone non sembra includere le specifiche "Norme integrative" negoziate tra la Commissione europea e la PPC, che sono applicabili solo ai dati personali dell'UE al fine di fornire un livello di protezione sostanzialmente equivalente agli standard del RGPD. Ne consegue che i dati personali dell'UE trasferiti dal Giappone verso un altro paese terzo che, sulla base della valutazione di adeguatezza giapponese, non dispone di un quadro di protezione dei dati riconosciuto come sostanzialmente equivalente al RGPD, non necessariamente godranno della protezione specifica prevista per i dati personali dell'UE.

17. **Va tuttavia tenuto presente che possono verificarsi trasferimenti ulteriori di dati personali verso paesi terzi che potranno essere oggetto di un'eventuale successiva decisione di adeguatezza da parte del Giappone. Questi paesi terzi potrebbero non essere stati oggetto di una previa valutazione o di una previa decisione di adeguatezza da parte dell'UE. In un caso del genere, la Commissione dovrebbe intervenire in qualità di autorità di vigilanza e garantire che sia mantenuto il livello di protezione dei dati UE, oppure prendere in considerazione la sospensione della decisione di adeguatezza in esame.**

18. Inoltre, il CEPD nutre preoccupazioni in relazione agli obblighi in materia di **consenso e trasparenza** dei titolari del trattamento (PIHBO). Il CEPD ha controllato accuratamente questi elementi poiché, diversamente dal diritto europeo sulla protezione dei dati, il consenso ha un ruolo centrale nell'ordinamento giuridico giapponese come base per il trattamento e per i trasferimenti di dati. Per esempio, il CEPD nutre preoccupazioni per quanto riguarda la nozione di consenso, la cui definizione non include il diritto di revoca, un elemento essenziale nel diritto dell'UE per assicurare che l'interessato abbia un controllo reale sui propri dati personali. Per quanto riguarda gli obblighi di trasparenza di un PIHBO, vi sono dubbi sul fatto che agli interessati sia fornita informazione proattivamente.

[8] Per ulteriori informazioni vedere la sezione 1.3.4 del presente parere.

19. Il CEPD è preoccupato del fatto che il **sistema di giapponese di tutela giuridica** possa essere di non facile accesso per gli interessati nell'UE che hanno bisogno di assistenza o che desiderano presentare un reclamo, considerando che l'assistenza della PPC è disponibile tramite assistenza telefonica e solo in giapponese. Lo stesso problema sussiste con il servizio di mediazione fornito dalla PPC, in quanto il sistema non è reso pubblico nella versione inglese del sito web della PPC, mentre anche importanti documenti informativi, come ad esempio le domande frequenti sulla APPI, sono disponibili solo in giapponese. A questo proposito, il CEPD gradirebbe che la Commissione discutesse con la PPC la possibilità di istituire un servizio online, almeno in inglese, inteso a fornire assistenza e a gestire i reclami degli interessati nell'Unione europea - analogo a quello previsto nell'allegato II della presente decisione di adeguatezza. Sarà anche necessario che la Commissione europea vigili attentamente sull'effettività delle sanzioni e dei relativi rimedi.

1.3.2 Chiarimenti necessari

20. Il CEPD accoglierebbe con favore rassicurazioni su alcuni aspetti del progetto di decisione di adeguatezza, su cui sono tuttora necessari ulteriori chiarimenti.

21. Questi si riferiscono, ad esempio**,** ad alcuni concetti chiave della legislazione giapponese. Più specificamente, vi è una mancanza di chiarezza circa lo **status del cosiddetto "fiduciario"**- un termine che ricorda il ruolo del responsabile del trattamento dei dati ai sensi del RGPD, ma sulle cui capacità di definire e modificare finalità e strumenti del trattamento restano elementi di ambiguità.

22. A causa della mancanza dei relativi documenti, il CEPD vorrebbe ottenere rassicurazioni anche in merito alla questione se le **limitazioni ai diritti degli interessati** (in particolare ai diritti di accesso, rettifica e opposizione) siano necessarie e proporzionate in una società democratica e rispettino il contenuto essenziale dei diritti fondamentali.

23. Il CEPD si attende inoltre che la Commissione europea controlli attentamente l'effettiva tutela dei **dati personali trasferiti dall'UE al Giappone, sulla base del progetto di decisione di adeguatezza, durante tutto il loro "ciclo di vita"** anche se la legislazione giapponese impone un obbligo di registrazione dell'origine dei dati per un massimo di tre anni.

1.4 Sull'accesso da parte delle autorità pubbliche a dati trasferiti in Giappone

24. Il CEPD ha analizzato il quadro giuridico applicabile agli enti governativi giapponesi quando accedono ai dati personali trasferiti dall'UE al Giappone per attività di contrasto o di sicurezza nazionale. Pur prendendo atto delle rassicurazioni fornite dal governo giapponese, di cui all'allegato II del progetto di decisione di adeguatezza, il CEPD ha identificato un certo numero di aspetti che necessitano di chiarimenti e per i quali nutre preoccupazione, fra cui si evidenziano i seguenti.

25. Con riguardo alle attività di contrasto, il CEPD rileva che i principi giuridici che si applicano all'accesso ai dati spesso sembrano simili alle regole dell'UE, nella misura in cui sono disponibili. La mancanza di traduzioni di numerosi testi giuridici e della giurisprudenza pertinente rendono difficile, tuttavia, concludere che tutte le procedure di accesso ai dati siano necessarie e proporzionate e che tali principi siano applicati secondo modalità "sostanzialmente equivalenti" al diritto dell'UE.

26. In materia di sicurezza nazionale, il CEPD prende atto del fatto che il governo del Giappone ha ribadito che le informazioni possono essere ottenute solo da fonti liberamente accessibili o tramite la comunicazione volontaria da parte delle imprese, e che non raccoglie informazioni sul pubblico in generale. Tuttavia, il Comitato è consapevole delle preoccupazioni espresse da esperti e nei mezzi di comunicazione e auspica ulteriori chiarimenti sulle misure di sorveglianza disposte dagli enti governativi giapponesi.

27. Per quanto riguarda il diritto di ricorso giurisdizionale degli interessati dell'UE, in materia sia di attività di contrasto sia di sicurezza nazionale, il CEPD accoglie con favore il fatto che la Commissione europea e il governo giapponese abbiano negoziato un meccanismo aggiuntivo inteso a fornire agli interessati dell'UE una via di ricorso ulteriore, ampliando in tal modo i poteri dell'autorità giapponese di protezione dei dati. Tuttavia, resta il problema che questo nuovo meccanismo non compensa del tutto le carenze in materia di vigilanza e di mezzi di ricorso da cui è affetto il diritto giapponese. Il CEPD chiede quindi ulteriori chiarimenti al fine di garantire che questo nuovo meccanismo compensi pienamente tali carenze.

1.5 Conclusione

28. Il CEPD ritiene che questa decisione di adeguatezza sia di fondamentale importanza. Poiché è la prima decisione di adeguatezza dalla data di entrata in vigore del RGPD, essa costituirà **un precedente per le future richieste di valutazioni di adeguatezza nonché per il riesame delle decisioni di adeguatezza adottate ai sensi della direttiva 95/46[9].** È anche importante sottolineare che le persone sono sempre più consapevoli dell'impatto della globalizzazione sulla loro vita privata e si rivolgono alle rispettive autorità di vigilanza per accertare la presenza di garanzie adeguate in caso di trasferimento dei loro dati personali all'estero. Alla luce di tali implicazioni, il CEPD ritiene che la Commissione europea dovrebbe garantire che non vi siano lacune nella protezione offerta dall'adeguatezza UE-Giappone e che questo specifico tipo di adeguatezza sia conforme ai requisiti dell'articolo 45 del RGPD.

29. Il CEPD accoglie con favore gli sforzi compiuti dalla Commissione europea e dalla PPC giapponese per allineare il più possibile il quadro giuridico giapponese a quello europeo. **I miglioramenti** introdotti dalle Norme integrative per colmare alcune delle differenze tra i due regimi sono molto importanti e meritori.

30. Tuttavia, a seguito di una attenta analisi del progetto di decisione di adeguatezza della Commissione nonché del quadro giuridico giapponese per la protezione dei dati, il CEPD rileva la **persistenza di un certo numero di preoccupazioni, congiuntamente alla necessità di ulteriori chiarimenti**. Inoltre, questa specifica tipologia di adeguatezza, che combina un quadro nazionale esistente con ulteriori norme specifiche, solleva anche interrogativi circa la sua attuazione operativa. Considerato quanto sopra, il CEPD raccomanda alla Commissione europea di rispondere alle preoccupazioni e alle richieste di chiarimenti sottopostegli dal CEPD, e di fornire ulteriori elementi di prova e spiegazioni in merito alle questioni sollevate. Il CEPD invita inoltre la Commissione europea a procedere a un riesame della presente decisione di adeguatezza (almeno) ogni due anni, e non ogni quattro anni come suggerito nell'attuale progetto di decisione di adeguatezza.

2 INTRODUZIONE

2.1 Quadro giuridico giapponese per la protezione dei dati

31. Il quadro giuridico giapponese per la protezione dei dati è stato modernizzato molto di recente, nel 2017. Tale quadro giuridico comprende diversi elementi, fra cui svolge un ruolo centrale la legge sulla protezione delle informazioni personali (APPI). Un altro elemento importante della normativa è il decreto ministeriale di applicazione della APPI (il "decreto ministeriale"), che specifica alcuni principi fondamentali della APPI.

[9] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

32. Sulla base di una decisione ministeriale, adottata il 12 giugno 2018[10], e dell'articolo 6 della APPI, alla PPC è stato conferito il potere di "*adottare le misure necessarie per colmare le differenze fra i sistemi e le attività del Giappone e del paese straniero interessato al fine di garantire la corretta gestione delle informazioni personali ricevute da ciascun paese*"[11]. La decisione ministeriale suggerisce inoltre che le norme adottate dalla PPC a integrazione di o in aggiunta a quelle previste nella APPI sarebbero vincolanti e azionabili nei confronti degli operatori economici giapponesi[12].

33. Di conseguenza, la PPC ha intrapreso negoziati con la Commissione europea e ha adottato, nel giugno 2018, norme più restrittive da applicare ai dati trasferiti dall'UE, rispetto a quelle della APPI e del decreto ministeriale. Si tratta delle Norme integrative, ai sensi della legge sulla protezione delle informazioni personali, per la gestione dei dati personali trasferiti dall'UE sulla base di una decisione di adeguatezza - in appresso le "Norme integrative"[13]. Tali Norme integrative sono allegate anche al progetto di decisione della Commissione pubblicato nel luglio 2018.

34. È importante notare che le Norme integrative sono applicabili solo ai dati personali trasferiti dall'Unione europea in Giappone sulla base della decisione di adeguatezza e mirano ad accrescere la protezione applicabile a tali dati. Ne consegue che esse non si applicano ai dati personali dei singoli in Giappone o provenienti da paesi diversi da quelli del SEE.

35. Il CEPD desidera evidenziare che la APPI modificata è entrata in vigore il 30 maggio 2017 e la PPC nella sua forma attuale è stata istituita nel 2016. Inoltre, le Norme integrative negoziate dalla PPC con la Commissione europea devono ancora entrare in vigore, essendo ciò subordinato al riconoscimento dell'adeguatezza dell'ordinamento giuridico giapponese rispetto a quello dell'Ue da parte della Commissione europea.

2.2 Ambito della valutazione del CEPD

36. Il progetto di decisione di adeguatezza della Commissione europea è il risultato di una valutazione delle norme giapponesi di protezione dei dati, seguita da negoziati con le autorità giapponesi. Il risultato di tali negoziazioni è in particolare rappresentato dai due allegati al progetto di decisione di adeguatezza: il primo prevede ulteriori tutele che gli operatori economici giapponesi dovranno applicare al trattamento dei dati personali trasferiti dall'UE, mentre il secondo contiene le garanzie e gli impegni assunti dal governo giapponese in materia di accesso ai dati da parte delle pubbliche autorità.

37. Il CEPD ha esaminato il quadro giuridico giapponese per la protezione dei dati, le Norme integrative negoziate dalla Commissione europea e le garanzie e gli impegni assunti dal governo giapponese. Il CEPD è chiamato a fornire un parere indipendente sui riscontri della Commissione europea, individuare eventuali carenze nel quadro giuridico in materia di adeguatezza, e proporre variazioni o modifiche per ovviare a tali carenze.

38. Come menzionato nei criteri di riferimento per l'adeguatezza pubblicati dal CEPD, "*le informazioni fornite dalla Commissione europea dovrebbero essere esaurienti e permettere al comitato di effettuare un'autonoma valutazione del livello di protezione dei dati nel paese terzo"*[14].

[10] Il CEPD rileva che, secondo il progetto di decisione di adeguatezza, tale decisione ministeriale è stata adottata il 12 giugno 2018. Tuttavia, al CEPD è stata fornita solo la bozza della decisione ministeriale, datata aprile 2018.
[11] Decisione ministeriale del 25 aprile 2018.
[12] Per ulteriori informazioni vedere la successiva sezione 1.3.4.
[13] Norme integrative, allegato I della decisione di esecuzione della Commissione del XXXX, ai sensi del regolamento 2016/679 del Parlamento europeo e del Consiglio, sulla adeguata protezione dei dati personali da parte del Giappone, inviata al CEPD nel settembre 2018.
[14] WP254, pag. 3.

39. Tuttavia il CEPD ha ricevuto la maggior parte dei documenti sotto forma di traduzioni in inglese, cui si fa riferimento nel progetto di decisione di adeguatezza, e tali documenti formano una parte essenziale dell'ordinamento giuridico giapponese. Il CEPD, pertanto, rende il presente parere sulla base dell'analisi dei documenti disponibili in inglese. Il CEPD ha preso in considerazione il quadro giuridico applicabile per la protezione dei dati dell'Unione europea, che comprende l'articolo 8 della Convenzione europea sui diritti umani (in appresso: la CEDU) a tutela del diritto alla vita privata e familiare, nonché gli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea (in appresso: la Carta) che tutelano rispettivamente il diritto alla vita privata e alla vita familiare, il diritto alla protezione dei dati personali e il diritto a un ricorso effettivo e a un giudice imparziale. In aggiunta a quanto sopra, il CEPD ha considerato i requisiti del RGPD, tenendo contestualmente conto della pertinente giurisprudenza.

40. L'obiettivo di questa attività è assicurare che il quadro giuridico giapponese per la protezione dei dati sia sostanzialmente equivalente a quello dell'Unione europea. Il concetto di "livello di protezione adeguato", che già esisteva nella direttiva 95/46, è stato ulteriormente sviluppato dalla CGUE. È importante ricordare l'orientamento fissato dalla CGUE nella sentenza Schrems, vale a dire che - mentre il "livello di protezione" nel paese terzo deve essere "sostanzialmente equivalente" a quello garantito nella UE - "gli strumenti dei quali tale paese terzo si avvale, al riguardo, per assicurare un siffatto livello di protezione, possono essere diversi da quelli attuati all'interno dell'[UE]"[15]. Pertanto, l'obiettivo non è replicare punto per punto la legislazione europea, ma stabilire i requisiti sostanziali e fondamentali della normativa in esame. L'adeguatezza può essere conseguita anche combinando il riconoscimento di diritti agli interessati, la definizione di obblighi in capo a chi effettua il trattamento o esercita il controllo sul trattamento, e la garanzia di un controllo da parte di organismi indipendenti. Le norme in materia di protezione dei dati, tuttavia, sono efficaci solo se sono azionabili e sono rispettate nella pratica. È pertanto necessario considerare non solo il contenuto delle norme applicabili ai dati personali trasferiti verso un paese terzo o un'organizzazione internazionale, ma anche il sistema in atto per garantirne l'efficacia. L'esistenza di efficienti meccanismi di applicazione è di fondamentale importanza per garantire l'efficacia delle norme sulla protezione dei dati[16].

2.3 Osservazioni e preoccupazioni di carattere generale

2.3.1 Peculiarità di questo tipo di decisione di adeguatezza

41. L'adeguatezza UE-Giappone è la prima ad essere esaminata rispetto al nuovo contesto giuridico del RGPD. Ciò rende il lavoro del CEPD ancora più importante alla luce degli effetti di questo progetto di decisione di adeguatezza sulle future richieste di valutazione di adeguatezza.

42. L'adeguatezza UE - Giappone sarebbe anche la prima di natura reciproca. Quando e se la UE riconoscerà che il Giappone è in grado di fornire un livello di protezione sostanzialmente equivalente a quello del RGPD, anche il Giappone emetterà la propria decisione di adeguatezza ai sensi dell'articolo 24 della APPI, riconoscendo che l'UE offre un livello di protezione adeguato secondo il quadro giuridico giapponese per la protezione dei dati. Pertanto, questa adeguatezza Giappone – UE, così come prevista, ha un carattere particolare, e di ciò il CEPD ha tenuto conto nella sua valutazione. Come menzionato sopra, la PPC giapponese ha negoziato con la Commissione europea norme specifiche, più rigorose, applicabili solo ai dati personali trasferiti dall'UE. Tali norme più rigorose sono vincolanti e azionabili ai sensi della decisione ministeriale e devono essere rispettate da tutti gli operatori

[15] Sentenza del 6 ottobre 2015, causa C362/14, Maximillian Schrems/Data Protection Commissioner (punti 73, 74).
[16] WP254, pag. 2.

economici che gestiscono informazioni personali (in appresso: PIHBO) in Giappone quando trattano dati personali provenienti dall'UE nel quadro del presente progetto di decisione di adeguatezza.

43. La Commissione europea ha pertanto basato i suoi riscontri di adeguatezza non solo sull'attuale quadro giuridico giapponese generale per la protezione dei dati, ma anche sulle suddette norme specifiche. La necessità di disporre di Norme integrative per completare la APPI è indicativa del fatto che la Commissione europea riconosce come la legislazione giapponese in materia di protezione dei dati non sia, di per sé, sostanzialmente equivalente al RGPD.

44. **Alla luce di quanto precede, il CEPD invita la Commissione europea a garantire che tale nuova architettura dell'adeguatezza, la prima ad essere adottata in vigenza del RGPD, e fondata su Norme integrative, costituisca un sistema duraturo e affidabile che non farà sorgere questioni pratiche né con riguardo al suo rispetto concreto ed effettivo da parte delle entità giapponesi né con riguardo alla sua applicazione da parte della PPC.**

2.3.2 Certezza delle traduzioni

45. Come la Commissione europea, il CEPD ha lavorato sulla base delle traduzioni in lingua inglese fornite dalle autorità giapponesi[17]. Il CEPD chiede alla Commissione europea di chiarire che essa ha basato il suo progetto di decisione di adeguatezza sulle traduzioni in lingua inglese ricevute e di verificare regolarmente la qualità e la certezza di tali traduzioni.

2.3.3 Adeguatezza settoriale

46. La valutazione di adeguatezza contenuta nel progetto di decisione in questione è limitata alla protezione delle informazioni personali da parte dei PIHBO ai sensi della APPI. Questo significa che l'adeguatezza è settoriale, in quanto essa si applica solo al settore privato, essendone esclusi i trasferimenti di dati personali tra le autorità pubbliche e gli organismi pubblici. A oggi, la Commissione europea menziona brevemente questa specificità dell'ambito di adeguatezza nel considerando 10 del progetto di decisione di adeguatezza.

47. **Il CEPD invita la Commissione europea a menzionare esplicitamente la natura settoriale della decisione di adeguatezza nel titolo della decisione di esecuzione nonché nell'articolo 1 di quest'ultima, in conformità con l'articolo 45, paragrafo 3, RGPD.**

2.3.4 Natura vincolante delle Norme integrative e degli orientamenti della PPC

48. L'articolo 6 della APPI recita che "il governo adotta… le necessarie misure legislative e le altre azioni in modo tale da essere in grado di agire con attenzione per proteggere le informazioni personali che richiedono in modo specifico che sia garantita la rigorosa attuazione della loro corretta gestione al fine di ottenere una migliore protezione dei diritti e interessi di una persona, e adotta le misure necessarie in collaborazione con i governi di altri paesi per la costruzione di un sistema conforme a livello internazionale in materia di dati personali attraverso la promozione della cooperazione con un'organizzazione internazionale e altri quadri giuridici internazionali". Sebbene questo articolo della APPI identifichi senza ambiguità la competenza del governo ad adottare tali misure giuridiche, esso non fa diretto riferimento alla PPC in quanto organismo competente ad adottare norme specifiche[18].

[17] La Commissione europea ha verificato tali traduzioni.

[18] Secondo un articolo pubblicato nel luglio 2018, quando le norme supplementari erano allo stato di progetto, era probabile che la natura giuridica vincolante di tali norme sarebbe stata oggetto di dibattito interno nel paese. Vedi Fujiwara S., Comparison between the EU and Japan's Data Protection Legal Frameworks', Jurist, vol. 1521 (luglio 2018): pag. 19.

A causa della ridotta tempistica, il CEPD non è stato in grado di raccogliere, rivedere ed esaminare evidenze su questo punto.

49. **In considerazione dell'importanza della questione, il CEPD prende nota dei ripetuti impegni e rassicurazioni della Commissione europea e delle autorità giapponesi per quanto riguarda la natura vincolante ed esecutiva delle Norme integrative. Il CEPD invita la Commissione europea a monitorare in modo continuo la loro natura vincolante e l'efficace applicazione in Giappone, in quanto il loro valore giuridico è un elemento essenziale dell'adeguatezza UE - Giappone.**

50. Inoltre la Commissione europea fa riferimento in diverse sezioni del suo progetto di decisione di adeguatezza agli Orientamenti della PPC (in appresso: "orientamenti").

51. Sebbene la Commissione europea, nel considerando 16 del suo progetto di decisione di adeguatezza, chiarisca che gli orientamenti forniscono un'interpretazione autorevole della APPI, nello stesso considerando fa riferimento alla natura vincolante di tali orientamenti: "Secondo le informazioni ricevute dalla PPC, tali orientamenti sono considerati norme vincolanti che formano parte integrante del quadro giuridico, in combinato disposto con il testo della APPI, con il decreto ministeriale, con le norme della PPC e con un insieme di domande e risposte preparato dalla PPC"[19].

52. Tuttavia, l'interpretazione del CEPD, sulla base delle informazioni fornite dalla stessa PPC, è che gli orientamenti non siano giuridicamente vincolanti. Forniscono semmai un' "interpretazione autorevole" del diritto. La PPC sostiene che gli orientamenti sono seguiti dai PIHBO nella prassi, utilizzati dalla PPC nei confronti dei PIHBO per far rispettare la legge e dai giudici quando pronunciano le loro sentenze. Tuttavia questi elementi non costituiscono prova sufficiente del fatto che gli orientamenti siano norme giuridicamente vincolanti.

53. **Il CEPD accoglierebbe con favore un chiarimento nella decisione di adeguatezza in relazione alla natura vincolante degli orientamenti della PPC e chiede alla Commissione europea di monitorare attentamente questo aspetto.**

54. Secondo la PPC, gli orientamenti sono seguiti nella pratica in ogni caso poiché questa è la consuetudine locale. La PPC menziona il fatto che i giudici giapponesi utilizzano gli orientamenti della PPC per pronunciare le loro sentenze quando applicano le norme della APPI. La Commissione europea fa riferimento ad una sentenza[20] risalente al 2006 per dimostrare che i giudici giapponesi basano le loro conclusioni sugli orientamenti. Nonostante il fatto che al CEPD non sia stata fornita questa sentenza, il CEPD gradirebbe che la Commissione europea fornisca, se disponibile, una sentenza più recente, in materia di protezione dei dati o in altra materia in cui i tribunali giapponesi hanno utilizzato gli orientamenti della PPC o altri orientamenti simili come base della loro decisione.

2.3.5 Revisione periodica della decisione di adeguatezza

55. L'articolo 45, paragrafo 3, RGPD stabilisce che deve essere effettuato un riesame periodico almeno ogni quattro anni. Secondo i criteri di riferimento per l'adeguatezza del CEPD[21], si tratta di un'indicazione temporale generica, che deve essere adattata a ciascun paese terzo o a ciascuna

[19] Decisione di esecuzione della Commissione del XXXX, ai sensi del regolamento 2016/679 del Parlamento europeo e del Consiglio sulla adeguata protezione dei dati personali da parte del Giappone, come inviata al CEPD il 13 novembre 2018, considerando 16.
[20] Decisione di esecuzione della Commissione del XXXX, ai sensi del regolamento 2016/679 del Parlamento europeo e del Consiglio sulla adeguata protezione dei dati personali da parte del Giappone, come inviata al CEPD il 13 novembre 2018, pagina 5, nota a piè di pagina 16, "Tribunale distrettuale di Osaka, sentenza del 19 maggio 2006, Hanrei Jiho, vol. 1948, pag. 122.
[21] WP254, pag. 3.

organizzazione internazionale oggetto di una decisione di adeguatezza. A seconda delle circostanze particolari del caso, potrebbe essere giustificata una frequenza maggiore. Inoltre, determinati avvenimenti o nuove informazioni sul quadro giuridico del paese terzo o dell'organizzazione internazionale o una modifica dello stesso potrebbero rendere necessario anticipare il riesame rispetto al previsto. Appare inoltre opportuno procedere a breve termine a un primo riesame di una decisione di adeguatezza interamente nuova e adattare progressivamente la periodicità del riesame in base all'esito.

56. Tenendo conto di una serie di fattori, tra i quali la circostanza che la APPI è entrata in vigore nel 2017, che la PPC è stata istituita nel 2016 e che non vi è a tutt'oggi alcuna informazione né evidenza in merito all'applicazione pratica delle Norme integrative, **il CEPD invita la Commissione europea a procedere ad un riesame della presente valutazione di adeguatezza (almeno) ogni due anni e non ogni quattro anni come suggerito nell'attuale progetto di decisione di adeguatezza.**

2.3.6 Impegni internazionali assunti dal Giappone

57. Secondo l'articolo 45, paragrafo 2, lettera c), del RGPD e dei criteri di riferimento per l'adeguatezza[22], nel valutare l'adeguatezza del livello di protezione, la Commissione europea prende in considerazione, fra l'altro, gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale o altri obblighi derivanti dalla loro partecipazione a sistemi multilaterali o regionali, in particolare in relazione alla protezione dei dati personali, nonché l'attuazione di tali obblighi. Sarebbe inoltre opportuno prendere in considerazione l'adesione del paese terzo alla Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, del 28 gennaio 1981 (la "convenzione n. 108+")[23] e il suo protocollo aggiuntivo.

58. **A questo proposito, il CEPD rileva che il Giappone è un osservatore del comitato consultivo della convenzione 108+.**

2.3.7 Poteri delle autorità di protezione dei dati[24] di agire in giudizio con riguardo alla validità di una decisione di adeguatezza

59. Il CEPD sottolinea che, sebbene il considerando 179 del progetto di decisione di adeguatezza citi solo casi in cui un'autorità di protezione dei dati ha ricevuto un reclamo in cui si contesta la compatibilità della decisione di adeguatezza rispetto ai diritti fondamentali di ogni individuo alla vita privata e alla protezione dei dati, questa affermazione è da intendersi come un esempio di situazioni in cui un'autorità di protezione dei dati può proporre la questione dinanzi ad un giudice nazionale, il che potrebbe avvenire anche in assenza di un reclamo, piuttosto che come una limitazione ai poteri conferiti in questa materia alle autorità di protezione dei dati ai sensi del RGPD e delle legislazioni nazionali degli Stati membri. Infatti, le disposizioni del RGPD [che] includono sia il potere di sospendere i trasferimenti di dati anche quando si basano su una decisione di adeguatezza sia quello di proporre un ricorso concernente la validità di una decisione di adeguatezza, non sono limitate ai casi in cui le autorità hanno ricevuto un reclamo, qualora il rispettivo diritto nazionale conferisca loro tale potere in forma più ampia e a prescindere da un reclamo, ai sensi delle pertinenti disposizioni del RGPD.

60. **Il CEPD invita la Commissione europea a chiarire nel suo progetto di decisione di adeguatezza che il potere delle autorità di controllo di proporre un ricorso contro la validità di una decisione di adeguatezza a seguito di un reclamo è solo un'esemplificazione dei poteri più ampi di cui le autorità**

[22] WP254, pag. 2.
[23] Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, convenzione n. 108+, 18 maggio 2018.
[24] Sentenza del 6 ottobre 2015, causa C362/14, Maximillian Schrems/Data Protection Commissioner.

di protezione dei dati sono investite ai sensi del RGPD, e che includono il potere di sospendere i trasferimenti e di proporre un ricorso concernente la validità di una decisione di adeguatezza in assenza di reclamo, qualora il rispettivo diritto nazionale lo preveda.

3 ASPETTI COMMERCIALI

3.1 Principi di contenuto

61. Il capitolo 3 dei criteri di riferimento per l'adeguatezza è dedicato ai "principi di contenuto". Questi ultimi devono essere parte del sistema di un paese terzo o di un'organizzazione internazionale affinché il livello di protezione fornito sia considerato sostanzialmente equivalente a quello garantito dalla legislazione dell'UE. Il CEPD riconosce il fatto che l'ordinamento giuridico giapponese persegue un approccio diverso da quello del RGPD al fine di rendere effettivo il diritto alla vita privata. Sebbene il diritto alla vita privata non sia sancito nella costituzione giapponese di per sé, esso è stato riconosciuto come diritto costituzionale attraverso la giurisprudenza, così come menzionato anche nella decisione della Commissione europea[25].

62. Proprio a causa del fatto che l'approccio giapponese differisce notevolmente da quello europeo, si deve valutare attentamente se il sistema nel suo complesso, e non solo per singoli aspetti, fornisca in definitiva un livello di protezione "sostanzialmente equivalente". Questo significa che potenziali "carenze" riguardanti un principio di contenuto potrebbero essere compensate da altri aspetti che realizzano un adeguato sistema di "pesi e contrappesi".

3.1.1 Nozioni

63. Ai sensi dei criteri di riferimento per l'adeguatezza, nel quadro giuridico del paese terzo dovrebbero essere presenti nozioni e/o principi basilari in materia di protezione dei dati. Sebbene tali nozioni e principi non devono necessariamente riprendere la terminologia del GDPR, essi dovrebbero rispecchiare ed essere coerenti con le nozioni racchiuse nel diritto europeo in materia di protezione dei dati. Ad esempio, il regolamento contiene le seguenti nozioni fondamentali: "dati personali", "trattamento di dati personali", "titolare del trattamento", "responsabile del trattamento", "destinatario" e "dati sensibili"[26].

64. Anche la APPI contiene un certo numero di definizioni, quali, fra le altre, quelle di "informazioni personali", "dati personali", "operatore economico che gestisce informazioni personali". **Sembra tuttavia che la APPI non contenga una definizione di "gestione dei dati personali" analoga a "trattamento dei dati personali".**

65. Per quanto riguarda la definizione di "gestione dei dati personali", la PPC ha risposto per iscritto alle domande del CEPD sul punto. La Commissione europea ha citato questa risposta nel progetto di decisione della Commissione: "*Anche se la APPI non utilizza il termine 'trattamento', essa si basa sul concetto equivalente di 'gestione' che, secondo le informazioni ricevute dalla PPC, copre 'ogni azione compiuta sui dati personali' fra cui l'acquisizione, l'inserimento, l'accumulo, l'organizzazione, la*

[25] Al CEPD non è stata fornita la traduzione in inglese di tale sentenza. Decisione di esecuzione della Commissione del XXXX, ai sensi del regolamento 2016/679 del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte del Giappone, come inviata al CEPD il 13 novembre 2018, pagina 13, nota a piè di pagina 9

[26] WP254, pag. 4.

conservazione, la modifica/il trattamento, il rinnovo, l'uscita, la rassicurazione, l'uscita, utilizzo o la fornitura di informazioni personali"[27].

66. Tuttavia, poiché il testo di riferimento per questa definizione non è stato fornito, il CEPD invita **la Commissione europea a monitorare attentamente che la definizione della suddetta nozione, come fornita dalla PPC, sia effettivamente rispettata nella pratica.**

3.1.1.1 Nozione di responsabile del trattamento dei dati e obblighi di un "fiduciario"

67. Come menzionato sopra, i criteri di riferimento per l'adeguatezza richiedono che nel quadro giuridico del paese terzo siano presenti nozioni e/o principi basilari in materia di protezione dei dati .

68. La APPI contiene una definizione di "operatore economico che gestisce informazioni personali" che, secondo la Commissione europea, comprende le nozioni sia di titolare del trattamento dei dati sia di responsabile del trattamento dei dati previste dal RGPD e non distingue fra le due[28]. Tuttavia, la APPI contiene anche il termine "fiduciario" nel suo articolo 22, che in qualche modo ricorda la nozione di responsabile del trattamento dei dati ai sensi del RGPD.

69. Come ha spiegato la PPC nelle risposte fornite al CEPD, che figurano anche nel progetto di decisione di adeguatezza della Commissione europea, un fiduciario è considerato equivalente ad un responsabile del trattamento dei dati ai sensi del RGPD – in quanto incaricato da un PIHBO della gestione del trattamento dei dati personali. Tale fiduciario ha gli stessi obblighi e diritti di ogni PIHBO, compresi quelli previsti dalle Norme integrative per i dati personali trasferiti dall'UE. Il PIHBO che affida la gestione di dati personali a un fiduciario è tenuto a "esercitare i necessari e opportuni controlli"[29] sul fiduciario stesso.

70. **Il CEPD invita la Commissione europea a spiegare lo status e gli obblighi del fiduciario quando quest'ultimo cambia le finalità e i mezzi di trattamento e a chiarire se il consenso dell'interessato resti necessario per procedere a tale cambiamento nelle finalità o nella definizione dei mezzi[30].**

3.1.1.2 Concetto di dati personali conservati

71. La APPI contiene la nozione di "dati personali conservati", considerati una sotto-categoria di dati personali. Secondo la APPI, le disposizioni relative ai diritti dell'interessato[31] si applicano solo ai dati personali conservati. La definizione di dati personali conservati è contenuta nell'articolo 2, paragrafo 7, della APPI.

72. I dati personali conservati sono i dati personali diversi da quelli (i) di cui è prevista la cancellazione entro un termine massimo di 6 mesi[32] oppure (ii) che rientrano nel campo di applicazione delle eccezioni di cui all'articolo 4 del decreto ministeriale e che sono suscettibili di nuocere al pubblico o ad altri interessi se la loro presenza o assenza viene resa nota.

---

[27] Decisione di esecuzione della Commissione del XXXX, ai sensi del regolamento 2016/679 del Parlamento europeo e del Consiglio sulla adeguata protezione dei dati personali da parte del Giappone, come inviata al CEPD il 13 novembre 2018, considerando 17.

[28] Decisione di esecuzione della Commissione del XXXX, ai sensi del regolamento 2016/679 del Parlamento europeo e del Consiglio sulla adeguata protezione dei dati personali da parte del Giappone, come inviata al CEPD il 13 novembre 2018, considerando 35.

[29] Articolo 22 della versione modificata della legge sulla tutela delle informazioni personali (APPI), entrata in vigore il 30 maggio 2017.

[30] Art. 23, paragrafo 5, punto (i), della APPI. Vedere anche la successiva sezione sul principio di trasparenza.

[31] Articoli 27-30, della APPI.

[32] Modifica al decreto ministeriale di esecuzione della legge sulla tutela delle informazioni personali (decreto ministeriale), entrato in vigore il 30 maggio 2017, articolo 5.

73. La Norma integrativa 2 prevede che "*i dati personali ricevuti dall'UE sulla base di una decisione di adeguatezza devono essere gestiti come dati personali conservati a prescindere dal termine previsto per la loro cancellazione.*"

74. Tuttavia, i dati personali che rientrano nelle deroghe di cui all'articolo 4 del decreto ministeriale non devono essere trattati come dati personali conservati e i diritti degli interessati non trovano applicazione in questo caso.

75. L'articolo 23, RGPD, prevede, come l'articolo 4 del decreto ministeriale, che il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento può limitare la portata degli obblighi posti in capo ad esso e dei diritti dell'interessato. Ciò può avvenire mediante misure legislative. Tali limitazioni devono rispettare l'essenza dei diritti e delle libertà fondamentali e devono rappresentare una misura necessaria e proporzionata in una società democratica.

76. Per quanto riguarda la sostanza delle deroghe di cui all'articolo 4 del decreto ministeriale, al CEPD non è stata fornita documentazione sufficiente su tali limitazioni né elementi aggiuntivi per chiarire il campo di applicazione di queste disposizioni[33]. Il CEPD non è in grado di valutare se tali limitazioni ai diritti degli interessati siano limitate a quanto sarebbe considerato strettamente necessario e proporzionato ai sensi del diritto dell'UE, e se quindi tali diritti siano sostanzialmente equivalenti a quelli riconosciuti agli interessati dell'UE.

77. **A causa della mancanza di alcuni documenti pertinenti, il CEPD gradirebbe anche rassicurazioni da parte della Commissione europea relative al fatto che le limitazioni ai diritti dei singoli (in particolare i diritti di accesso, rettifica e opposizione) sono necessarie e proporzionate in una società democratica e rispettano il contenuto essenziale dei diritti fondamentali.**

78. Un requisito essenziale ai sensi del RGPD è che i dati personali siano protetti durante tutto il loro "ciclo di vita".

79. Tenendo conto del fatto che le Norme integrative si applicano solo ai dati personali trasferiti dall'UE, il CEPD gradirebbe ricevere ulteriori informazioni circa l'attuazione pratica di queste norme da parte dei PIHBO, specialmente quando questi dati vengono comunicati ulteriormente a un altro PIHBO dopo la loro prima trasmissione verso il Giappone.

80. La Commissione europea ha chiarito al considerando 15 del suo progetto di decisione di adeguatezza che i PIHBO che ricevono e/o trattano ulteriormente dati personali provenienti dall'UE saranno soggetti all'obbligo giuridico di conformarsi alle Norme integrative e che a tal fine dovranno assicurare di essere in grado di identificare tali dati personali lungo tutto il rispettivo "ciclo di vita".

81. Nelle sue risposte, la PPC[34] ha spiegato che tale identificazione sarà effettuata mediante metodi tecnici (tagging) o metodi organizzativi (memorizzando i dati provenienti dall'UE in una banca dati dedicata).

82. Nella nota a piè pagina n. 14 del suo progetto di decisione di adeguatezza, la Commissione europea spiega che i PIHBO devono registrare le informazioni sull'origine dei dati Ue per il tempo necessario al fine di poter rispettare le Norme integrative. Ciò è sancito anche all'articolo 26, paragrafi 1, 3 e 4 della APPI, che afferma che un PIHBO è soggetto all'obbligo di confermare e registrare la fonte di questi dati e tutte le circostanze relative all'acquisizione degli stessi.

[33] Al CEPD non è stata fornita la decisione della Corte Suprema cui si fa riferimento al considerando 53 del progetto di decisione di adeguatezza.
[34] Allegato III del presente parere.

83. Tuttavia, il CEPD osserva che l'articolo 18 delle norme della PPC[35] specifica che gli obblighi di registrazione dei PIHBO sono limitati ad un massimo di tre anni per i casi che ricadono al di fuori delle specifiche modalità di tenuta dei registri descritte all'articolo 16 delle norme della PPC (utilizzo di un documento scritto, un supporto elettromagnetico o un microfilm). Quanto detto è affermato anche dalla Commissione europea nel considerando 71 del suo progetto di decisione di adeguatezza: "*Come specificato all'articolo 18 delle norme della PPC, tali registrazioni devono essere conservate per un periodo da uno a tre anni, a seconda dei casi*".

84. Anche se, come afferma la Commissione europea nella nota a piè pagina 14 del suo progetto di decisione di adeguatezza, ai PIHBO non è fatto divieto di conservare le registrazioni sull'origine dei dati per più di tre anni al fine di essere in grado di adempiere agli obblighi posti a loro carico ai sensi della Norma integrativa n. 2, ciò non risulta chiaramente né dalla legislazione giapponese né dalle Norme integrative. Il CEPD ritiene che sussista il rischio che i PIHBO, di fatto, rispettino le prescrizioni dell'articolo 18 delle norme della PPC anche quando trattano dati provenienti dall'UE. Ciò principalmente perché a oggi, secondo il CEPD e sulla base dei documenti disponibili, non esiste alcuna disposizione che imponga ai PIHBO di rispettare invece le Norme integrative. Ciò comporterebbe che i dati trasferiti dall'UE non sarebbero più protetti dalle tutele aggiuntive contenute nelle Norme integrative.

85. **Il CEPD invita la Commissione europea a vigilare attentamente sull'effettiva tutela dei dati personali trasferiti dall'UE in Giappone sulla base del progetto di decisione di adeguatezza, durante tutto il loro ciclo di vita, anche se la legislazione giapponese impone l'obbligo di registrazione dell'origine dei dati per un massimo di tre anni.**

3.1.2 Criteri di liceità e correttezza del trattamento per fini legittimi

86. Secondo i criteri di riferimento per l'adeguatezza, ai sensi del RGPD, i dati devono essere trattati in modo lecito, corretto e legittimo[36]. Le basi giuridiche che consentono il trattamento lecito, corretto e legittimo dei dati personali dovrebbero essere definite in maniera sufficientemente chiara. Il quadro europeo riconosce alcuni criteri di legittimità tra cui, per esempio, le disposizioni del diritto nazionale, il consenso dell'interessato, l'esecuzione di un contratto o il legittimo interesse del titolare del trattamento o di un terzo a condizione che non prevalgano gli interessi dell'interessato.

87. AI sensi della APPI, il consenso svolge un ruolo centrale nell'ordinamento giuridico giapponese in materia di protezione dei dati. Il consenso è la base giuridica primaria per il trattamento dei dati personali in Giappone, e anche una delle principali basi giuridiche per il trasferimento dei dati personali dal Giappone ad un paese terzo. Inoltre, è richiesto il consenso per la modifica della finalità del trattamento.

88. Ai sensi della Norma integrativa n. 3, la base giuridica per il trattamento dei dati personali trasferiti dall'UE in Giappone sarà la base giuridica ai sensi della quale i dati vengono trasferiti in Giappone. Se il PIHBO vuole trattare ulteriormente tali dati per una diversa finalità, deve previamente ottenere il consenso dell'interessato.

89. Il CEPD ritiene che la qualità del consenso, specialmente a causa del suo ruolo centrale nel quadro giuridico giapponese, deve soddisfare i requisiti fondamentali della nozione di consenso, vale a dire secondo il diritto dell'UE, una "*manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato...*" L'interessato può revocare tale consenso in quanto tutela essenziale per garantire

[35] Norme di applicazione della legge sulla tutela delle informazioni personali (norme della PPC), entrate in vigore il 30 maggio 2017, articolo 16.
[36] WP254, pag. 4.

la sua libera volontà nel tempo[37]. Il diritto di revoca, in quanto elemento inderogabile del consenso, sembra mancare nel quadro giuridico giapponese. Invero, secondo gli orientamenti della PPC[38], la revoca è meramente "auspicabile" e subordinata alle "caratteristiche, dimensioni e status delle attività economiche".

3.1.3 Principio di trasparenza

90. Ai sensi dell'articolo 5, RGPD, la trasparenza è un principio fondamentale del sistema di protezione di dati dell'UE[39]. I criteri di riferimento per l'adeguatezza indicano espressamente la "trasparenza" come uno dei principi di contenuto di cui tenere conto quando si valuta il livello di protezione sostanzialmente equivalente fornito da un paese terzo. Il principio di trasparenza e correttezza mira a garantire che l'interessato abbia il controllo sui propri dati e, a tal fine, di norma devono essergli fornite le informazioni in modo proattivo. Nel caso dello scudo per la privacy, il gruppo di lavoro dell'articolo 29[40], nel suo parere 1/2016, ha fatto riferimento all'allegato II, punto II.1.b, dell'accordo sullo scudo per la privacy (informazione all'interessato) e ha dichiarato che se i dati non vengono raccolti direttamente presso l'interessato, un ente dovrebbe informare l'interessato "nel momento in cui l'ente aderente allo scudo registra i dati" (sezione 2.2.1.a). Un ulteriore criterio è aver pubblicato la politica della privacy [*privacy policy*] (vedere la sezione 2.2.1.b). Pertanto, già nel vigore della direttiva 95/46/CE era stato ritenuto necessario informare direttamente gli interessati.

91. Una prima preoccupazione che si solleva riguarda le modalità con cui gli interessati vengono informati ai sensi della APPI. In base all'articolo 27, paragrafo 1, della APPI, un PIHBO è obbligato a fornire le informazioni indicate all'articolo 27, paragrafo 1, della APPI mettendole "in uno stato in cui un interessato può conoscerle". Tuttavia, questa formulazione non chiarisce in quale misura il PIHBO sia soggetto a un obbligo positivo di adottare misure per poter realmente informare l'interessato.

92. **Il CEPD invita la Commissione a chiarire il significato dell'espressione "può conoscerle" e se la APPI preveda di regola l'obbligo di informare realmente gli interessati.**

93. Inoltre, secondo i criteri di riferimento per l'adeguatezza, possono esistere limiti alle informazioni da fornire all'interessato, analogamente all'articolo 23 del RGPD. Nella stessa prospettiva, l'articolo 14, paragrafo 5, del RGPD prevede un'eccezione al diritto di essere informati quando comunicare tali informazioni rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità del trattamento. Tuttavia, anche in questo caso, il titolare del trattamento deve fornire una qualche sorta di informazioni, ad esempio mettendo a disposizione del pubblico informazioni "di ordine

[37] RGPD, articolo 4, paragrafo 11. Per ulteriori informazioni vedere anche le pertinenti linee guida del CEPD sul consenso WP259, 10 aprile 2018.
[38] Data Protection Legal and Technical Research and Analysis Consortium (Consorzio di ricerca e analisi giuridica e tecnica sulla protezione dei dati, DPC), An assessment of the level of protection of personal data provided under Japanese law (Valutazione del livello di protezione dei dati personali fornito dal diritto giapponese), pag. 46: "Inoltre, dal punto di vista della tutela dei diritti e degli interessi di un titolare quale il consumatore, è auspicabile, qualora si riceva la richiesta di un titolare relativa a dati personali conservati, rispondere inoltre alla domanda del titolare o interrompendo l'invio diretto di e-mail ecc. oppure cessando volontariamente l'utilizzo ecc. considerando le caratteristiche, la dimensione e lo status delle attività economiche".
[39] WP 254, capitolo 3, punto 7, pag. 5; vedere anche il considerando 39 del RGPD.
[40] Questo gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. Era un organismo consultivo indipendente europeo per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE. Il WP29 è ora diventato il CEPD.

generale". Inoltre, quando il rischio cessa, l'interessato deve essere informato[41]. Questi aspetti sono importanti per garantire il fondamentale principio della correttezza.

94. Ai sensi dell'articolo 23 della APPI, un PIHBO in generale deve informare previamente l'interessato circa la comunicazione a terzi dei suoi dati, o implicitamente quando ne ottiene il consenso o espressamente mediante una notifica di opposizione. Il CEPD ne deduce che non vi è alcuna comunicazione all'interessato che lo informi del fatto che i suoi dati non costituiscono dati personali conservati ai sensi della APPI perché rientrano nelle eccezioni di cui all'articolo 4 del decreto ministeriale. Di conseguenza, questi interessati non potranno godere pienamente dei loro diritti. Gli interessati non sono informati nemmeno nei casi di cui all'articolo 18, paragrafo 4, della APPI.

95. **Il CEPD riconosce la possibilità di limitare i diritti per scopi legittimi perseguiti dai PIHBO e dalle pubbliche autorità. Al contempo, il CEPD ritiene che vi dovrebbe essere almeno una previa informazione generale sulla possibile limitazione dei diritti per le finalità previste dalla legge e che all'interessato dovrebbe essere comunicata la cessazione del rischio che ha causato la limitazione dell'informazione.**

96. Infine, altri aspetti della trasparenza sono ulteriormente sviluppati nei paragrafi seguenti con riguardo ai rischi che comporta il trasferimento verso un paese terzo[42] e all'informativa sulla logica del trattamento nel contesto di un processo decisionale automatizzato, compresa la profilazione[43].

3.1.4 Restrizioni imposte ai trasferimenti ulteriori

97. Il CEPD accoglie con favore gli sforzi compiuti dalle autorità giapponesi e dalla Commissione europea per migliorare il livello di protezione dei trasferimenti ulteriori di cui alla Norma integrativa n. 4, che esclude che i dati personali trasferiti dall'UE siano ulteriormente trasferiti a un paese terzo sulla base del sistema APEC CBPR. Inoltre, il CEPD riconosce che nei considerando 177 e 184 del suo nuovo progetto di decisione di adeguatezza, la Commissione europea si è impegnata a sospendere la decisione di adeguatezza laddove i trasferimenti ulteriori non garantiscano più la continuità della protezione. Tuttavia, il CEPD vorrebbe sollevare due punti relativi a questi trasferimenti di dati personali dell'UE dal Giappone verso paesi terzi.

98. **L'utilizzo del consenso nell'ordinamento giuridico giapponese come base per il trasferimento dei dati dal Giappone verso un paese terzo solleva preoccupazioni, in quanto il CEPD ritiene che le informazioni fornite all'interessato dell'UE prima della prestazione del consenso non sembrano complete.**

99. L'articolo 24 della APPI vieta il trasferimento di dati personali a un terzo che si trova al di fuori del territorio del Giappone senza il previo consenso della persona interessata. La Norma integrativa n. 4 sancisce che agli interessati dell'UE devono essere fornite le informazioni sulle circostanze relative al trasferimento necessarie per decidere se acconsentire o meno.

100. La Commissione europea conclude nel suo progetto di decisione di adeguatezza che la Norma integrativa n. 4 garantisce che il consenso dell'interessato dell'UE sia particolarmente ben informato[44], in quanto l'interessato sarà avvertito del fatto che i dati saranno trasferiti all'estero e del paese di

[41] Tele2, cause riunite C 203/15 e C 698/15, sentenza della Corte del 21 dicembre 2016, racc. 121 e Digital Rights Ireland, cause riunite C-293/12 e C-594/12, sentenza della Corte del 8 aprile 2014, racc. 54-62.
[42] Vedere sezione 2.1.4.
[43] Vedere sezione 2.1.6.
[44] Decisione di esecuzione della Commissione del XXXX, ai sensi del regolamento 2016/679 del Parlamento europeo e del Consiglio sulla adeguata protezione dei dati personali da parte del Giappone, come inviata al CEPD il 13 novembre 2018, considerando 76.

destinazione specifico. Ciò consentirebbe agli interessati di valutare i rischi per la vita privata connessi al trasferimento.

101. Ai sensi del principio di trasparenza di cui ai criteri di riferimento per l'adeguatezza, occorre garantire un certo livello di correttezza nel fornire informazione ai singoli . Nel contesto dei trasferimenti ulteriori basati sul consenso, il CEPD ritiene che per garantire tale grado adeguato di correttezza, gli interessati dovrebbero essere informati esplicitamente circa i possibili rischi di tali trasferimenti, derivanti dalla mancanza di una adeguata protezione nel paese terzo e dall'assenza di garanzie adeguate precedenti al consenso. Tale informazione dovrebbe segnalare ad esempio che nel paese terzo potrebbe non esserci un'autorità di controllo e/o principi per il trattamento dei dati e/o che nel paese terzo agli interessati potrebbero non essere riconosciuti diritti[45]. Secondo il CEPD, fornire tali informazioni è essenziale al fine di consentire all'interessato di prestare il proprio consenso con piena conoscenza di questi specifici fatti relativi al trasferimento[46].

102. Il consenso informato è importante anche per quanto riguarda le esclusioni settoriali. La decisione di adeguatezza non riguarda taluni tipi di trattamento da parte di determinati organismi, quali le università che trattano dati personali a fini accademici. In questo caso la preoccupazione del CEPD riguarda la specifica ipotesi dei dati trasferiti dall'UE ai sensi della decisione di adeguatezza - ad esempio i dati sulle risorse umane relativi a studenti Erasmus in Giappone - che sono poi utilizzati per una diversa finalità che non rientra nell'ambito di applicazione della decisione di adeguatezza (ad esempio a fini di ricerca), con il consenso dell'interessato - e non sono quindi più coperti dalla protezione aggiuntiva fornita dalle Norme integrative.

103. La Commissione europea dichiara al considerando 38 del suo progetto di decisione che una tale ipotesi rientrerebbe nell'ambito dei trasferimenti ulteriori e che, laddove ciò avvenga, il PIHBO deve fornire agli interessati tutte le informazioni necessarie prima di ottenere il loro consenso, compreso il fatto che l'informazione personale non ricadrebbe nella tutela delle norme della APPI.

104. La Norma integrativa n. 4 richiede solo che il PIHBO ottenga il consenso dell'interessato dopo che a questi siano state fornite le informazioni sulle circostanze relative al trasferimento necessarie affinché prenda una decisione in relazione al proprio eventuale consenso.

105. **Il CEPD invita la Commissione europea a garantire che le informazioni che devono essere fornite agli interessati "sulle circostanze relative al trasferimento" comprendano l'indicazione dei rischi posti potenzialmente dal trasferimento a causa della mancanza di una adeguata protezione nel paese terzo e dell'assenza di garanzie adeguate, o, nel caso di esclusioni settoriali, dell'assenza delle tutele apprestate dalle Norme integrative e dalla APPI.**

106. **Possono verificarsi trasferimenti ulteriori di dati personali verso paesi terzi che saranno oggetto di un'eventuale successiva decisione di adeguatezza da parte del Giappone.**

107. Fatte salve le eccezioni di cui all'articolo 23, paragrafo 1, della APPI, i dati inizialmente trasferiti dall'UE in Giappone possono poi essere trasferiti dal Giappone verso un paese terzo senza il consenso in due casi:

- Se il PIHBO e il terzo destinatario hanno adottato congiuntamente misure che apprestano un livello di protezione equivalente a quello della APPI in combinato disposto con le Norme

[45] Linee guida del CEPD 2/2018 sulle eccezioni all'articolo 49 ai sensi del regolamento (UE) 2016/679, 25 maggio 2018, pag. 8.
[46] Linee guida del CEPD 2/2018 sulle eccezioni all'articolo 49 ai sensi del regolamento (UE) 2016/679, 25 maggio 2018, pag. 9.

integrative per mezzo di un contratto, di altre forme di accordi vincolanti o di accordi vincolanti all'interno di un gruppo societario[47].

- Se il paese terzo è stato riconosciuto dalla PPC, ai sensi dell'articolo 24 della APPI e dell'articolo 11 delle norme della PPC[48], come paese che fornisce un livello di protezione equivalente a quello garantito in Giappone.

108. Il CEPD considera l'articolo 24 della APPI una norma più specifica che deroga alla norma generale di cui all'articolo 23 della APPI. Pertanto, la CEPD non condivide la valutazione della Commissione europea contenuta nella nuova ultima frase del considerando 78 del progetto di decisione di adeguatezza, secondo cui anche in tali casi il trasferimento al terzo resta soggetto al requisito dell'ottenimento del consenso ai sensi dell'articolo 23, paragrafo 1, della APPI.

109. Ai sensi dell'articolo 11, paragrafo 1, delle norme della PPC, una decisione di adeguatezza da parte della PPC richiede standard sostanziali equivalenti a quelli previsti dalla APPI, di cui sia garantita l'attuazione nel paese terzo sotto il controllo effettivo di un'autorità indipendente. Inoltre, la PPC può imporre condizioni necessarie per tutelare i diritti e gli interessi dei singoli in Giappone, ai sensi dell'articolo 11, paragrafo 2, delle norme della PPC.

110. La Norma integrativa n. 4 sancisce che i dati personali dell'UE possono essere trasferiti verso un paese terzo ai sensi di una decisione giapponese di adeguatezza senza ulteriori restrizioni. Ma l'articolo 44 del RGPD stabilisce che qualunque trasferimento di dati personali verso un paese terzo deve rispettare le condizioni di cui al capo V del RGPD, compresi trasferimenti successivi da un paese terzo verso un altro paese terzo. Il livello di protezione delle persone fisiche i cui dati personali vengono trasferiti non deve essere pregiudicato dal trasferimento ulteriore[49]. Sebbene tale interpretazione sia condivisa in linea di principio anche dalla Commissione europea nel suo progetto di decisione di adeguatezza[50], sembra non essere del tutto seguita. La Commissione europea ha negoziato il divieto di trasferimento di dati provenienti dall'UE verso un paese terzo sulla base del sistema Asia Pacific Economic Cooperation (APEC) – Cross Border Privacy Rules (CBPRs) [Cooperazione economica Asia-Pacifico - Norme transfrontaliere in materia di privacy]. In considerazione dello strumento comparativo, sviluppato nel 2014 nel quadro della direttiva UE fra le BCR [Binding Corporate Rules - norme vincolanti di impresa] e le CBPR, che mostra i requisiti di entrambi i sistemi, i loro elementi comuni e le loro differenze (WP29 Parere 02/2014), il CEPD nutre preoccupazioni in relazione all'utilizzo delle CBPR come strumento per i trasferimenti successivi dei dati personali trasferiti dall'UE verso paesi diversi dal Giappone.

111. La Commissione europea sembra accettare i trasferimenti successivi di dati personali trasferiti dall'UE in Giappone sulla base di una decisione di adeguatezza del Giappone, senza che la PPC abbia la possibilità di imporre le Norme integrative quali condizioni per tutelare i diritti e gli interessi dei singoli dell'UE, se necessario. Il CEPD deduce dall'articolo 44 del RGPD che la protezione rafforzata dei dati trasferiti dall'UE in Giappone come prevista dalle Norme integrative debba sempre essere estesa anche al caso in cui dati personali trasferiti dall'UE in Giappone siano ulteriormente trasferiti in un

[47] Norma integrativa n. 4, punto (ii).
[48] Norme di esecuzione della legge sulla protezione delle informazioni personali, 30 maggio 2017. La Commissione europea ha comunicato al CEPD una traduzione in inglese del nuovo articolo 11, ma tale articolo non è stato ancora pubblicato.
[49] WP 254, pag. 5.
[50] Decisione di esecuzione della Commissione del XXXX, ai sensi del regolamento 2016/679 del Parlamento europeo e del Consiglio sulla adeguata protezione dei dati personali da parte del Giappone, come inviata al CEPD il 13 novembre 2018, considerando 75.

paese terzo se il quadro giuridico di protezione dei dati di tale paese non è riconosciuto come sostanzialmente equivalente al RGPD.

112. **Pertanto, il CEPD invita la Commissione europea a svolgere la propria funzione di controllo garantendo il mantenimento del livello di protezione dei dati dell'UE ovvero valutando la sospensione della decisione di adeguatezza in esame se i dati personali trasferiti dall'UE in Giappone sono ulteriormente trasferiti verso paesi terzi in base a un'eventuale successiva decisione di adeguatezza del Giappone, laddove tali paesi terzi non siano stati sottoposti a una previa valutazione o decisione di adeguatezza da parte dell'UE.**

3.1.5 Marketing diretto

113. Ai sensi della Norma integrativa n. 3, a un PIHBO è fatto divieto di trattare i dati per finalità di marketing diretto se questi sono stati trasferiti dall'Unione europea per un'altra finalità e l'interessato dell'UE non ha dato il proprio consenso alla modifica della finalità di utilizzo.

114. Ai sensi dei criteri di riferimento per l'adeguatezza, se il trattamento dei dati avviene per finalità di marketing diretto, l'interessato dovrebbe essere in grado, in qualsiasi momento e gratuitamente, di opporsi a tale trattamento con riferimento ai dati che lo riguardano. Ai sensi dell'articolo 16 della APPI, a un PIHBO è consentito trattare informazioni personali solo se l'interessato presta il proprio consenso. La revoca del consenso potrebbe avere lo stesso risultato del diritto incondizionato di opporsi al marketing diretto.

115. Il quadro giuridico di protezione dei dati del Giappone non prevede un diritto incondizionato di opposizione e, come spiegato sopra nella sezione sul consenso, la revoca del consenso ai sensi degli orientamenti della PPC è semplicemente auspicabile e soggetta a condizioni, cosicché non può essere considerata equivalente al diritto di opporsi in qualsiasi momento di cui ai criteri di riferimento per l'adeguatezza. **Il CEPD invita la Commissione europea a fornire rassicurazioni circa il diritto di revoca del consenso e a monitorare i casi che riguardano il marketing diretto.**

3.1.6 Processo decisionale automatizzato e profilazione

116. Secondo i criteri di riferimento per l'adeguatezza, le decisioni basate unicamente sul trattamento automatizzato (processo decisionale automatizzato relativo alle persone fisiche), compresa la profilazione, che producono effetti giuridici sull'interessato o incidono significativamente sulla sua persona sono ammesse soltanto a determinate condizioni stabilite dal quadro giuridico del paese terzo. Pertanto, ogni volta che ha luogo un processo decisionale automatizzato e attività di profilazione nelle circostanze sopra citate, deve sussistere un corrispondente fondamento giuridico.

117. Nel quadro europeo le condizioni relative al processo decisionale automatizzato comprendono, per esempio, la necessità di ottenere il consenso esplicito[51] dell'interessato o la necessità di tale decisione per la conclusione di un contratto. Se la decisione non è conforme a tali condizioni in quanto previste dal regime giuridico del paese terzo, l'interessato dovrebbe avere il diritto di non essere soggetto a una decisione del genere. Inoltre, il diritto del paese terzo dovrebbe, in ogni caso, prevedere le necessarie garanzie, compreso il diritto di essere informato sui motivi particolari sottesi alla decisione e sulla sua logica, di rettificare informazioni inaccurate o incomplete e a contestare la decisione qualora questa sia stata adottata sulla base di un fondamento di fatto errato.

[51] Per osservazioni critiche sulla nozione di consenso nel quadro giuridico di protezione dei dati del Giappone, vedere: 2.1. Generale e 2.2.8. Marketing diretto.

118. La decisione della Commissione menziona solo il settore bancario, dove sarebbero applicabili norme settoriali[52] in materia di decisioni automatizzate. Le Comprehensive Guidelines for Supervision over Major Banks [Linee guida generali per la vigilanza sulle grandi banche] citate al considerando 93 del progetto di decisione di adeguatezza indicano che alla persona interessata devono essere fornite spiegazioni specifiche sui motivi del rigetto di una richiesta di mutuo.

119. Le argomentazioni della Commissione europea con riguardo al progetto di decisione di adeguatezza (considerando 94), secondo le quali è improbabile che la mancanza nella APPI di norme specifiche in materia di processo decisionale automatizzato possa pregiudicare il livello di protezione, sembrano (per esempio) non prendere in considerazione il caso in cui un dato personale trasferito dall'UE sia successivamente trattato da un altro titolare del trattamento giapponese (diverso dall'originario importatore dei dati giapponese).

120. Sembra quindi che in Giappone non vi siano regole generali, cioè non settoriali, che disciplinino i processi decisionali automatizzati e la profilazione.

121. **Il CEPD invita la Commissione europea a monitorare la casistica relativa ai processi decisionali automatizzati e alla profilazione.**

3.2 Meccanismi procedurali e applicativi

122. Sulla base dei criteri di riferimento per l'adeguatezza, il CEPD ha analizzato i seguenti aspetti del regime giuridico e in materia di protezione dei dati giapponese, per come risultano dal progetto di decisione di adeguatezza: la presenza e l'effettivo funzionamento di un'autorità di controllo indipendente; l'esistenza di un sistema atto a garantire un buon livello di conformità e un sistema di accesso ad idonei meccanismi di ricorso che conferiscano agli interessati dell'UE i mezzi per esercitare i propri diritti e per proporre ricorsi senza dover affrontare ostacoli di difficile superamento nella presentazione di ricorsi giudiziari e amministrativi.

123. Basandosi sui parametri stabiliti dalla CGUE nella sentenza Schrems[53] e su quelli delineati nel considerando 104 e nell'articolo 45 del RGPD, il CEPD ritiene che, sebbene in Giappone esista un sistema coerente con quello europeo, tale sistema potrebbe essere in concreto di difficile accesso per gli interessati dell'UE i cui dati saranno trasferiti ai sensi della decisione di adeguatezza in esame, considerando la presenza di barriere linguistiche e istituzionali.

124. Nelle sezioni seguenti si esamineranno i summenzionati aspetti del quadro giuridico giapponese, prima di evidenziare alcune raccomandazioni per la Commissione.

3.2.1 Autorità di controllo competente indipendente

125. La PPC è stata istituita il 1° gennaio 2016 in seguito alle modifiche della APPI del 2015, e ha preso il posto del suo predecessore - la Commissione speciale per la protezione delle informazioni personali (istituita nel 2013 ai sensi della legge "mio numero"). Sebbene si tratti di un'istituzione giovane, sin dalla sua nascita la PPC si è notevolmente impegnata nella costruzione dell'infrastruttura necessaria per rendere effettiva l'attuazione della APPI come modificata. A tal proposito sono degni di nota la redazione delle norme della PPC, gli orientamenti della PPC volti a fornire linee guida ai PIHBO sull'interpretazione della APPI, la pubblicazione di un documento contenente domande e risposte[54] e l'istituzione di una linea di assistenza telefonica intesa a fornire consulenza agli operatori economici e

[52] Queste norme settoriali non sono state fornite al CEPD.

[53] Causa 362/14 (2015) Maximilian Schrems/Data Protection Commissioner, (punti 73 e 74).

[54] La Commissione europea non ha fornito al CEPD la versione inglese di tale documento.

ai cittadini sulle disposizioni in materia di protezione dai dati nonché di un servizio di mediazione per gestire i reclami.

126. L'istituzione e il funzionamento della PPC sono disciplinati al Capo V della APPI. Sebbene la PPC rientri nella competenza del primo ministro, l'articolo 62 impone che la PPC eserciti le proprie funzioni autonomamente. Il CEPD accoglie con favore il chiarimento della Commissione europea nel progetto di decisione di adeguatezza modificato, distribuito il 13 novembre 2018, che ha descritto ulteriormente il grado di libertà della PPC da influenze interne ed esterne.

3.2.2 Il sistema di protezione dei dati deve garantire un buon livello di conformità

127. Il progetto di decisione di adeguatezza contiene un'ampia disamina dei poteri conferiti alla PPC ai sensi degli articoli 40, 41 e 42 della APPI, intesi a garantire il controllo e l'applicazione della normativa. L'articolo 40 conferisce alla PPC il potere di chiedere ai PIHBO di presentare relazioni e documentazione relativa alle operazioni di trattamento nonché quello di effettuare ispezioni in loco. Ai sensi dell'articolo 42, la PPC ha il potere - laddove ravvisi la necessità di proteggere diritti individuali o riscontri la violazione delle disposizioni di legge - di emettere raccomandazioni e, qualora non sia sufficiente, di ordinare ai PIHBO di sospendere l'atto in violazione o di adottare le misure necessarie per sanare la violazione.

128. Nell'ottobre 2018, la PPC ha adottato uno dei suoi primi atti ai sensi dell'articolo 41 della APPI modificata, emettendo un "orientamento" diretto a un PIHBO recante luna serie di indicazioni per la società: rafforzare le proprie misure di sicurezza e vigilare efficacemente sui fornitori di applicazioni, fornendo contestualmente agli utenti spiegazioni chiare e comprensibili sulle modalità di utilizzo delle loro informazioni personali; ottenere il previo consenso degli interessati quando l'informazione viene condivisa con un terzo; rispondere adeguatamente alle richieste degli utenti di cancellazione delle loro informazioni. Nella risposta fornita al CEPD[55], i funzionari della PPC hanno comunicato che la società aveva annunciato l'intenzione di collaborare e che, in caso di mancata collaborazione, la PPC avrebbe inviato alla società una "raccomandazione" ai sensi dell'articolo 42, paragrafo 1, della APPI.

129. Le indagini svolte dalla PPC sul summenzionato PIHBO costituiscono un indice molto positivo dell'impegno dell'autorità di controllo inteso a garantire un buon livello di conformità nel paese.

130. Sebbene vi siano miglioramenti rispetto al quadro giuridico vigente prima delle modifiche del 2015, il CEPD rileva che la PPC ha minori poteri rispetto alle autorità europee di protezione dei dati ai sensi del RGPD, in particolare per quanto riguarda l'**applicazione della legge**. Ad esempio, le sanzioni amministrative pecuniarie[56] sono alquanto lievi. La decisione della Commissione europea sottolinea nel considerando 108 che, nei casi di non conformità o di alcune violazioni della APPI, sono previste sanzioni penali e che il presidente della PPC può trasmettere gli atti alla procura. Tuttavia, la decisione della Commissione europea non tiene conto del fatto che l'azione penale in Giappone è discrezionale e in alcuni casi può essere soggetta a lunghi processi di revisione[57]. Inoltre, la pena della reclusione (con o senza obbligo di lavoro) associata alle violazioni della APPI ai sensi del Capo VII, può essere di

[55] Allegato III.

[56] Sono previste al capitolo VII della APPI. La pena massima è prevista dall'art. 83 (fornire o utilizzare in modo occulto una banca dati di informazioni personali a beneficio illecito proprio o di terzi) ed è pari a un anno di reclusione con obbligo di lavoro o a una multa non superiore a 500 000 JPY (circa 3900 EUR). Secondo le spiegazioni fornite dalla Commissione, le multe sono cumulative per infrazione. Ciononostante, il CEPD rileva che, anche in caso di cumulo materiale delle sanzioni pecuniarie, è probabile che l' importo totale rimanga notevolmente contenuto rispetto agli standard europei.

[65] Oda H., Japanese Law, Oxford University Press (III edizione), 2009: 439 – 440.

difficile applicazione poiché colpisce le persone fisiche e in ogni caso non punisce il PIHBO in quanto persona giuridica che non adempie ai suoi obblighi di responsabilizzazione.

131. **In considerazione di quanto sopra, il CEPD invita la Commissione europea a monitorare attentamente l'efficacia delle sanzioni e dei relativi rimedi nel sistema di protezione dei dati del Giappone.**

3.2.3 Il sistema di protezione dei dati deve fornire aiuto e sostegno agli interessati nell'esercizio dei loro diritti nonché meccanismi di ricorso appropriati

132. La PPC fornisce sul suo sito web informazioni e orientamenti esaurienti intesi ad aumentare la consapevolezza fra i PIHBO degli obblighi e delle responsabilità loro incombenti ai sensi del quadro giuridico di protezione dei dati nonché una linea di assistenza telefonica per fornire informazioni e assistenza ai cittadini del Giappone con riguardo ai loro diritti individuali ai sensi della APPI. Il sito web presenta anche una sezione, detta "Stanza dei bambini", espressamente destinata al pubblico dei bambini e dei giovani. Il CEPD rileva che queste informazioni - insieme con la linea di assistenza telefonica, gli orientamenti e la documentazione delle domande e risposte - sono disponibili in giapponese[58]. Pertanto, il CEPD è fortemente convinto che sarebbe utile se la PPC creasse una pagina dedicata nella versione inglese del suo sito web, intesa a fornire informazioni agli interessati dell'UE i cui dati verranno trasferiti in Giappone ai sensi della decisione di adeguatezza della Commissione europea sui diritti individuali previsti dal quadro giuridico del Giappone in materia di protezione dei dati e dalle Norme integrative.

133. Il CEPD accoglie con favore il chiarimento reso dalla Commissione europea nel considerando 104 del progetto di decisione di adeguatezza modificato distribuito il 13 novembre 2018 riguardante il servizio di mediazione gestito dalla PPC ai sensi dell'articolo 61, punto (ii), della APPI. Tuttavia, il CEPD intende sollevare tre punti in relazione a ciò. In primo luogo, il servizio di mediazione non è pubblicizzato nella versione inglese del sito web della PPC. In secondo luogo, il servizio è accessibile solo telefonicamente ed è disponibile solo in giapponese. Infine, la mediazione è una procedura meramente facilitativa che non ha come esito un accordo vincolante tra le parti con conseguenze sull'efficacia delle opzioni di ricorso a disposizione degli interessati[59].

134. Infine, il CEPD rileva che il progetto di decisione di adeguatezza pone l'accento sui rimedi disponibili attraverso procedimenti civili o penali, ma non riconosce l'esistenza in Giappone di **ostacoli istituzionali al contenzioso**, quali le spese di giustizia (le spese legali sono suddivise in egual misura fra le parti, a prescindere dalla soccombenza[60]) la penuria di avvocati nel paese[61], il fatto che gli avvocati stranieri non possono esercitare la professione forense nel paese, nonché il requisito dell'onere della prova nella responsabilità extracontrattuale. Il CEPD teme che tali fattori possano - in concreto - ostacolare l'accesso dei singoli alla giustizia e pregiudicare il loro diritto a perseguire rimedi giuridici con rapidità e senza sostenere costi proibitivi.

[58] https://www.ppc.go.jp/en/contactus/piinquiry/.

[59] Kojima T., *Civil Procedure and ADR in Japan*, Chuo University Press, 2004; e Menkel-Meadow C., *Dispute Processing and Conflict Resolution: Theory, Practice and Policy*, Ashgate (2003) (a cura di).

[60] Wagatsuma (2012), 'Recent Issues of Cost and Fee Allocation in Japanese Civil Procedure' in Reimann (a cura di), Cost and Fee Allocation in Civil Procedure – Ius Gentium; comparative Perspectives on Law and Justice Vol. 11, pagg. 195 – 200.

[61] In base alle ultime cifre, il numero di avvocati in Giappone è 38.980 (circa 290 avvocati per milione di persone [Federazione degli Ordini degli avvocati del Giappone] (2017) White Paper on Attorneys [Libro bianco sugli avvocati], pagg. 8-9.

135. In considerazione di quanto sopra, **il CEPD nutre la preoccupazione che sussista il rischio per gli interessati dell'UE di incontrare difficoltà nell'accesso ai ricorsi giudiziari e amministrativi** e, pertanto, gradirebbe che la Commissione europea discuta con la PPC circa la possibilità di istituire un servizio online, almeno in inglese, **inteso a fornire assistenza ai singoli dell'UE e a gestire i loro reclami[62].** Oltre a quanto sopra, il CEPD accoglierebbe con favore la possibilità di permettere alle autorità per la protezione dei dati dell'UE di agire quali intermediari dei reclami degli interessati dell'UE nei confronti delle organizzazioni che operano in Giappone e della PPC.

4 SULL'ACCESSO DA PARTE DI PUBBLICHE AUTORITA' AI DATI TRASFERITI AL GIAPPONE

136. L'intenzione della COM è riconoscere, con la decisione di adeguatezza, che "il Giappone garantisce un livello adeguato di protezione per i dati personali trasferiti dall'Unione europea agli operatori economici che gestiscono informazioni personali in Giappone", come recita l'articolo 1 del progetto di decisione di adeguatezza. Conformemente all'articolo 45, paragrafo 2, RGPD, la COM ha anche analizzato i limiti e le garanzie per quanto riguarda l'accesso ai dati personali da parte di pubbliche autorità. Il presente capitolo si concentra sulla valutazione dell'accesso ai dati personali da parte delle autorità preposte all'applicazione della legge e degli altri enti governativi per finalità di sicurezza nazionale. L'analisi del CEPD si basa sul progetto di decisione di adeguatezza, sul suo allegato II, in cui il governo del Giappone fornisce una panoramica del quadro giuridico pertinente, e sui testi normativi giapponesi, nella misura in cui essi sono stati forniti dalla COM. Pertanto, nel contesto specifico della presente valutazione, il CEPD ha tenuto conto di elementi concernenti la normativa giapponese che non fanno parte dei riscontri della Commissione europea, ma che sono rilevanti per valutare le condizioni e le garanzie ai sensi delle quali le pubbliche autorità del Giappone sono abilitate ad accedere a dati personali trasferiti dall'Unione europea.

4.1 Accesso ai dati per attività connesse all'applicazione della legge

4.1.1 Procedure di accesso ai dati in materia di diritto penale

137. Il progetto di decisione di adeguatezza indica tre modalità previste dal diritto del Giappone tramite le quali le autorità preposte all'applicazione della legge possono accedere ai dati in Giappone:

4.1.1.1 Richieste di accesso in base a un mandato del giudice

138. Secondo il progetto di decisione di adeguatezza, affinché il governo del Giappone, e in particolare affinché le autorità preposte all'applicazione della legge penale possano richiedere l'accesso alle prove in formato elettronico nel contesto di indagini penali, esse devono sempre ottenere un mandato, salvo qualora utilizzino la procedura di divulgazione volontaria - vedi oltre.

4.1.1.1.1 Requisito della "causa adeguata", necessità e proporzionalità dei mandati

139. Il CEPD riconosce che, ai sensi della costituzione del Giappone, qualsiasi raccolta di dati personali con mezzi coattivi deve fondarsi su un mandato giudiziario. Più in particolare, il progetto di decisione di adeguatezza indica che in tutti i casi di "perquisizione e sequestro", i mandati giudiziari devono essere emessi per una "causa adeguata", che la Corte suprema ritiene sussistente solo nel caso in cui si ritenga che la persona interessata (l'indagato o l'imputato) abbia commesso un reato e la perquisizione o il sequestro siano necessari per l'indagine penale. La COM fa qui riferimento alla sentenza della Corte suprema del 18 marzo 1969, causa n. 100 (1968(Shi)). Il CEPD ricorda che secondo la giurisprudenza

[62] Analogo a quello previsto nell'allegato II della decisione di adeguatezza in esame per i reclami dei residenti nell'UE relativi all'accesso ai loro dati da parte delle pubbliche autorità del Giappone.

della CGUE[63] soltanto un giudice, e non ad esempio un pubblico ministero, può autorizzare la raccolta dei dati relativi in particolare al traffico e alla ubicazione.

140. Tenuto anche conto della giurisprudenza della CGUE, secondo la quale l'accesso ai dati può essere subordinato a un mandato, come nella causa Tele2, il CEPD si rammarica del fatto che non sono state fornite ulteriori informazioni al fine di valutare in che modo siano applicati in concreto i criteri di accertamento della necessità di un mandato - gravità e modalità del reato; valore e importanza delle cose sequestrate come prove; probabilità di occultamento o distruzione delle cose sequestrate; entità degli inconvenienti causati dal sequestro; altre condizioni correlate - e il concetto di matrice costituzionale di "causa adeguata". Pertanto, il CEPD invita la Commissione a monitorare se l'emissione dei mandati soddisfa in concreto i criteri enunciati dalla CGUE.

4.1.1.1.2 Categorie di reati per i quali può essere emesso un mandato

141. La procedura del mandato si applica solo in caso di "indagine obbligatoria". In linea di principio, tali mandati possono essere emessi solo nei casi in cui si è verificata una violazione di legge. A tal proposito, il CEPD rileva la recente "legge sulla repressione della criminalità organizzata e sul controllo dei proventi di reato", adottata il 15 giugno 2017 nel contesto dell'adesione del Giappone alla Convenzione internazionale delle Nazioni Unite contro la criminalità organizzata internazionale (UNTOC)[64]. In mancanza di una versione in inglese disponibile di tale normativa, e considerato il requisito previsto dal diritto dell'UE secondo cui alcuni dati sono raccolti soltanto nel contesto delle indagini, dell'accertamento e del perseguimento di reati gravi[65], nonché date le preoccupazioni manifestate da vari commentatori, compreso il relatore speciale delle Nazioni Unite Joseph Cannataci[66], con riguardo all'ampiezza dell'ambito di applicazione, che si basa su una definizione di "gruppo criminale organizzato" ritenuta generica e troppo estesa, il CEPD non è in grado di concludere che l'accesso a prove in formato elettronico ai sensi della pertinente legislazione giapponese sia limitato alle soglie previste dal diritto dell'UE.

142. Si deve altresì rilevare che su alcuni tipi di reati è competente la polizia prefettizia, con i propri provvedimenti speciali di polizia. Le norme interne applicabili alla polizia prefettizia non sono state messe a disposizione del CEPD.

143. Secondo il progetto di decisione di adeguatezza, la raccolta di informazioni in formato elettronico in materia di applicazione del diritto penale ricade nelle competenze della polizia prefettizia.

4.1.1.2 Mandati di intercettazione

144. L'allegato II del progetto di decisione di adeguatezza indica che la legge sulle intercettazioni nelle indagini penali prevede delle particolarità per l'intercettazione delle comunicazioni. La normativa è stata fornita con grande ritardo, il che non ne ha consentito un'analisi approfondita. Pertanto, sebbene sembri che tale quadro giuridico preveda numerose garanzie, il CEPD non è in grado di valutare se le condizioni previste in tale elemento della legislazione siano assistite da garanzie sostanzialmente equivalenti a quelle richieste nell'UE, sia dalla Carta come interpretata dalla CGUE, sia dalla CEDU come interpretata dalla Corte di Strasburgo.

[63] Vedi cause 203/15 e C 293/12 e C 594/12 della CGUE.
[64] Cfr. https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html .
[65] Vedere le cause riunite C 293/12 e C 594/12 e la causa C 203/15.
[66] Relatore Speciale delle Nazioni Unite sul diritto alla vita privata, nonché Graham Greenleaf, ricercatore in giurisprudenza della UNSW.

4.1.1.3 La procedura di "divulgazione volontaria" sulla base del foglio di richiesta

145. Tale forma non obbligatoria di collaborazione consente alle pubbliche autorità di chiedere ai titolari del trattamento (escluse le società di telecomunicazioni) di fornire loro i dati che detengono. In caso di mancata risposta, non è prevista l'esecuzione coattiva. Non è tuttora chiaro quali siano le autorità che possono avvalersi di tale tipo di procedura, ma sembra che siano limitate a quelle che indagano sui reati.

4.1.1.3.1 Condizioni di emissione dei "fogli di richiesta"

146. Il CEPD riconosce che la Corte suprema giapponese, facendo riferimento alla Costituzione, ha delineato le limitazioni all'utilizzo delle "divulgazioni volontarie"[67]. Dalla lettura del progetto di decisione di adeguatezza, sembra che, concretamente, una "divulgazione volontaria" può essere chiesta dalle autorità competenti solo mediante l'emissione di un "foglio di richiesta". L'invio di tale "foglio di richiesta" risulta essere ammesso solo come parte di un'indagine penale, e pertanto presuppone sempre un concreto sospetto di reato già commesso. Tali indagini sono generalmente svolte dalla polizia prefettizia, caso in cui si applicano le limitazioni di cui all'articolo 2, paragrafo 2, della legge di polizia, ossia la necessità che l'indagine sia pertinente ai fini delle attività di polizia. Tuttavia, il CEPD chiede ulteriori chiarimenti con riguardo ai criteri che consentono di emettere un foglio di richiesta (ad esempio la giurisprudenza che illustra l'applicazione di tali criteri), e sul rapporto fra la procedura di divulgazione volontaria e il sequestro dei dati sulla base di un mandato. Invero, sembra che, anche quando i dati non potrebbero essere ottenuti mediante la procedura volontaria, essi potrebbero comunque essere ottenuti con un mandato, se sono indispensabili per le autorità investigative[68].

4.1.1.3.2 Giurisprudenza disponibile sulle limitazioni all'uso della divulgazione volontaria

147. I casi citati nel progetto di decisione di adeguatezza[69] per illustrare le limitazioni all'uso delle procedure di divulgazione volontaria riguardano casi in cui l'imputato era stato fotografato o ripreso in uno spazio pubblico direttamente dalla polizia, e pertanto forniscono indicazioni limitate sulle situazioni in cui le autorità competenti possono chiedere a un titolare del trattamento di divulgare i dati, con particolare riferimento ai criteri elencati nell'allegato II relativo alla "adeguatezza dei metodi", che sembra riguardare la valutazione dell'eventuale "adeguatezza" o ragionevolezza dell'indagine volontaria al fine di conseguire lo scopo dell'indagine. Lo stesso può dirsi per quanto riguarda il criterio generale che, per valutare la legittimità delle indagini volontarie, chiede "se si possono ritenere ragionevoli in conformità a convenzioni socialmente accettate". Inoltre, l'agenzia nazionale di polizia, che è l'autorità federale responsabile di tutte le questioni riguardanti la polizia criminale, ha rilasciato istruzioni destinate alla polizia prefettizia sul "corretto uso di richieste scritte in materia di indagini". Fra l'altro, l'ispettore capo deve ottenere l'autorizzazione interna da un funzionario di alto livello. Il CEPD non dispone di informazioni sulla vincolatività di tali istruzioni. Tuttavia, il CEPD afferma che l'uso di questa procedura deve essere proporzionato o necessario.

4.1.1.3.3 Diritti e obblighi dei titolari del trattamento nel contesto della divulgazione volontaria

148. Inoltre, spetta ai titolari del trattamento acconsentire a fornire i dati (ma sembra non siano tenuti a chiedere il consenso degli interessati o a informarli), laddove tali richieste non siano incompatibili con altri obblighi giuridici (quali gli obblighi di riservatezza). La relazione fornita dalla Commissione sembra indicare che, dopo aver raggiunto un elevato tasso di ottemperanza, i titolari del trattamento hanno

[67] Vedi allegato II, pagina 8.
[68] Vedi allegato II, pagina 7.
[69] Vedere allegato II, pagina 8 - due sentenze della Corte suprema del 24 dicembre 1969 (1965 (A) n. 1187) e del 15 aprile 2008 (2007 (A) n. 839).

iniziato a prendere in considerazione la protezione dei dati dei loro clienti e hanno quindi iniziato a rispondere con meno frequenza a tali richieste.

149. Resta inoltre incerto se i titolari del trattamento ricevano incentivi per adempiere alle richieste (ad esempio, se ricevono vantaggi quando adempiono, o se ottengono un'esimente dall'imputazione penale, ecc.). In particolare, non vi è alcuna menzione di principi quale il "divieto di auto-incriminazione".

150. Il CEPD gradirebbe informazioni aggiuntive, se disponibili, cifre sul numero e la tipologia delle richieste, nonché sulle risposte fornite dai titolari del trattamento che hanno ricevuto le richieste. In mancanza di giurisprudenza e di cifre, il CEPD invita la Commissione a monitorare l'efficienza e l'applicazione concreta della procedura in esame.

151. Tuttavia, il CEPD non può accertare tali elementi in quanto non dispone della giurisprudenza e delle cifre relative alla procedura in esame. Di conseguenza, il CEPD non è in grado di fornire una valutazione riguardante l'efficienza e la concreta applicazione di questa procedura senza ulteriori elementi riguardanti la relativa prassi.

4.1.1.4 Conclusione sulle procedure di accesso ai dati per finalità di applicazione della legge

152. In conclusione, il CEPD riconosce che il principio secondo cui le autorità competenti possono accedere coattivamente ai dati personali solo quando ciò è necessario e proporzionato allo scopo, e sulla base di un mandato, corrisponde alle principali garanzie essenziali previste dal diritto dell'UE e dalla CEDU. In seguito ai riscontri sopra menzionati, il CEPD chiede alla Commissione di monitorare l'ambito di applicazione di tali misure, l'ambito di applicazione della procedura di divulgazione volontaria e l'applicazione di tali principi da parte della polizia prefettizia e dei giudici nella pertinente giurisprudenza e di monitorare altresì se il quadro giuridico del Giappone fornisca attualmente le garanzie essenziali delineate dalla CGUE sulla base della Carta e dalla Corte EDU sulla base della Convenzione.

4.1.2 Controlli in materia penale

153. La decisione di adeguatezza nonché l'allegato II presentano quattro tipi di controlli aventi ad oggetto la polizia, i ministeri e le agenzie pubbliche.

4.1.2.1 Controllo giurisdizionale

4.1.2.1.1 Nei casi in cui l'informazione in formato elettronico è raccolta coattivamente (perquisizione e sequestro)

154. Secondo il progetto di decisione di adeguatezza, in tutti i casi in cui l'informazione in formato elettronico è raccolta coattivamente (perquisizione e sequestro), la polizia deve prima ottenere il mandato di un giudice. Vi è tuttavia un'eccezione a questa regola[70]. Invero, l'articolo 220, paragrafo 1, del codice di procedura penale consente al pubblico ministero, a un suo assistente o a un funzionario di polizia giudiziaria, nel momento in cui arrestano un indagato, di effettuare una perquisizione o sequestrare le informazioni in formato elettronico nel luogo di arresto. In tale situazione, vi è la possibilità che un giudice non ammetta tali informazioni come prove.

155. Il CEPD è consapevole che eccezioni analoghe esistono anche nel diritto dell'UE. Rileva che non sempre vi è un controllo giurisdizionale nei casi in cui l'informazione in formato elettronico è raccolta coattivamente, come si dichiara nel progetto di decisione di adeguatezza. In tale contesto, il CEPD richiama la giurisprudenza della Corte EDU sul controllo giurisdizionale a posteriori[71].

[70] Vedere l'allegato II.
[71] Corte EDU, Modestou/Grecia, N° 51693/13.

4.1.2.1.2 In caso di richieste di divulgazione volontaria

156. Secondo il progetto di decisione di adeguatezza, nel caso di richieste di divulgazione volontaria, non vi è un controllo ex ante da parte di un giudice. In tal caso, la polizia prefettizia opera sotto la supervisione del pubblico ministero. Il progetto di decisione di adeguatezza menziona gli articoli 192, paragrafo 1, e 246 sulla mutua cooperazione e il coordinamento fra i pubblici ministeri, la commissione prefettizia di pubblica sicurezza e i funzionari di polizia giudiziaria e sullo scambio di informazioni tra loro. Fa inoltre riferimento all'articolo 193, paragrafo 1, secondo il quale il pubblico ministero può impartire le necessarie istruzioni alla polizia giudiziaria nonché fissare le regole per una corretta indagine. Infine, cita l'articolo 194 sulle azioni disciplinari contro la polizia giudiziaria per mancato rispetto dei pubblici ministeri adottate dalla Commissione nazionale o prefettizia di pubblica sicurezza.

157. Il CEPD riconosce l'istituzione delle misure sopra descritte e il controllo operato sulla polizia giudiziaria dalla Commissione nazionale e prefettizia di pubblica sicurezza (vedi oltre).

4.1.2.2 Controllo sulla polizia da parte delle Commissioni di pubblica sicurezza

158. Secondo l'allegato II del progetto di decisione di adeguatezza, sono due le commissioni che esercitano un controllo sulla polizia. Lo scopo di entrambe è garantire la gestione democratica e la neutralità politica dell'attività di polizia.

4.1.2.2.1 Controllo da parte della Commissione nazionale di pubblica sicurezza

159. L'allegato II del progetto di decisione di adeguatezza citava il controllo operato dalla Commissione di pubblica sicurezza sulla NPA. La legge di polizia contiene un elenco dei compiti della commissione da cui promanano i suoi poteri di vigilanza (vedi articolo 5).

160. Secondo l'articolo 4 della legge di polizia, la commissione nazionale di pubblica sicurezza è istituita sotto la giurisdizione del primo ministro ed è composta da un presidente e da cinque membri. L'articolo 7 fissa alcuni limiti alla nomina dei membri della commissione. La durata del mandato dei membri della commissione è di cinque anni e può essere rinnovato una sola volta, come prescritto all'articolo 8. Sembra inoltre che la Dieta (il Parlamento del Giappone) abbia un rilevante potere sulla nomina e la revoca dei membri della commissione, il che garantisce l'indipendenza della commissione nazionale di pubblica sicurezza.

161. Tali norme giuridiche potenziano la neutralità politica della commissione nazionale di pubblica sicurezza.

4.1.2.2.2 Controllo da parte delle commissioni prefettizie di pubblica sicurezza

162. La polizia prefettizia è soggetta al controllo delle commissioni prefettizie di pubblica sicurezza istituite in ogni prefettura. Ai sensi degli articoli 2 e 36, paragrafo 2, della legge di polizia, le commissioni prefettizie di pubblica sicurezza sono responsabili per "la tutela dei diritti e della libertà di un individuo". L'articolo 38 nonché l'articolo 42 della legge di polizia elencano le funzioni delle commissioni prefettizie di pubblica sicurezza. Tali commissioni hanno anche lo scopo di garantire la gestione democratica e la neutralità politica dell'attività di polizia, come sancito all'articolo 43, paragrafo 2, inviando alla polizia prefettizia singoli casi laddove lo ritengano necessario nel contesto di un controllo sulle attività della polizia prefettizia o di condotta illecita del suo personale.

163. Non è tuttavia chiaro se tali commissioni abbiano altri poteri oltre al controllo sul comportamento della polizia. Il CEPD si chiede se il termine "condotta illecita" includa l'accesso illecito ai dati e, in tal caso, se tali commissioni abbiano il potere di ordinare la cancellazione dei dati o meno.

164. Per quanto riguarda la neutralità e l'indipendenza di tali commissioni, secondo quanto dichiarato nel progetto di decisione di adeguatezza[72], le commissioni prefettizie di pubblica sicurezza sono istituite sotto la giurisdizione del governatore della prefettura, che deve nominare i componenti della commissione con il consenso dell'assemblea di prefettura. I componenti della commissione prefettizia di pubblica sicurezza restano in carica per tre anni e possono essere rinnovati per due volte. L'articolo 39 della legge di polizia prevedeva alcuni limiti in relazione alla nomina dei membri. Il progetto di decisione di adeguatezza cita anche il controllo sulla polizia prefettizia da parte dell'assemblea locale, facendo riferimento all'articolo 100 della legge sull'autonomia locale. Questa legge non è stata però fornita al CEPD[73].

165. Inoltre, ai sensi dell'articolo 42, paragrafi 2 e 3, della legge di polizia, "Nessun membro della commissione può essere contemporaneamente un membro dell'assemblea o del personale in servizio a tempo pieno presso gli enti pubblici locali o essere assunto a tempo parziale nel servizio di cui al comma 1 dell'articolo 28, paragrafo 5, della legge sul servizio pubblico locale["].

166. In base ai suddetti elementi e considerando la collaborazione fra le commissioni prefettizie di pubblica sicurezza e la commissione nazionale di pubblica sicurezza, il CEPD concorda con il progetto di decisione di adeguatezza e accoglie con favore la neutralità e l'indipendenza dei membri delle commissioni prefettizie di pubblica sicurezza. Il CEPD intende che le commissioni prefettizie di pubblica sicurezza hanno solo il potere di indagare sul comportamento della polizia e non hanno altri poteri di vigilanza, compresa la cancellazione dei dati raccolti dalla polizia prefettizia. Sembrano pertanto necessari ulteriori chiarimenti sull'idoneità del controllo operato dalle commissioni prefettizie di pubblica sicurezza rispetto agli standard fissati nel diritto dell'UE.

4.1.2.2.3 Controllo da parte della Dieta

167. Il progetto di decisione di adeguatezza[74] e l'allegato II[75] forniscono alcune informazioni circa il controllo operato dalla Dieta sul governo, anche per quanto riguarda la legittimità della raccolta di dati da parte della polizia. Invero, entrambi citano l'articolo 62 della Costituzione, secondo cui la Dieta può chiedere la produzione di documenti e la deposizione di testimoni. Entrambi citano anche norme giuridiche della legge sulla Dieta, in particolare l'articolo 104, sui poteri della Dieta, nonché l'articolo 74, sulla trasmissione di richieste scritte, cui il governo deve rispondere per iscritto entro sette giorni, come disposto dall'articolo 75. Il progetto di decisione di adeguatezza aggiunge inoltre: "La funzione della Dieta di controllo sull'esecutivo è assistita da obblighi di segnalazione, ad esempio ai sensi dell'articolo 29 della legge sulle intercettazioni".

168. Il CEPD riconosce il coinvolgimento della Dieta nel controllo del governo e della polizia in relazione alla liceità della raccolta di dati.

4.1.2.2.4 Controllo da parte dell'esecutivo

169. Ai sensi dell'allegato II del progetto di decisione di adeguatezza, da un lato, il ministro o il vertice di ciascun ministero o agenzia ha poteri di controllo ed esecutivi ai sensi della APPIHAO[76]. Dall'altro lato, il ministro dell'Interno e delle comunicazioni (MIC) ha poteri d'indagine in relazione all'applicazione

[72] Vedere il progetto di decisione di adeguatezza, pag. 31.
[73] Vedere il progetto di decisione di adeguatezza, pag. 33.
[74] Vedere il progetto di decisione di adeguatezza, pag. 30.
[75] Vedere l'allegato II, pag. 12.
[76] Vedere allegato II, pag. 10.

della APPIHAO da parte di tutti gli altri ministeri, compreso il ministro della Giustizia con riguardo alla polizia, come indicato nel progetto di decisione di adeguatezza[77].

170. Il ministro può chiedere al vertice di un organo amministrativo di presentargli i materiali e le spiegazioni relative alla gestione di informazioni personali da parte dell'organo amministrativo interessato, ai sensi dell'articolo 50 della APPIHAO. Può chiedere una revisione delle misure quando vi è il sospetto che si sia verificata una violazione o un'applicazione non corretta della legge, e può chiedere pareri sulla gestione delle informazioni personali da parte dell'organo amministrativo interessato, ai sensi degli articoli 50 e 51 della APPIHAO.

171. Il progetto di decisione di adeguatezza e l'allegato II citano anche l'istituzione di 51 centri di informazione globale che stanno "garantendo la regolare attuazione della presente legge", ai sensi dell'articolo 47 della APPIHAO. Il CEPD rileva che la APPIHAO non illustra ulteriormente il ruolo e i poteri di tali centri di informazione, ma il progetto di decisione di adeguatezza fornisce alcune precisazioni.

172. Pertanto, il CEPD accoglie con favore il fatto che vi sia un controllo dell'esecutivo sul rispetto della APPIHAO da parte dei ministeri e degli organi amministrativi a cura del MIC.

173. In conclusione, le normative dell'UE e la CEDU, nella giurisprudenza delle rispettive corti, stanno fissando standard e garanzie in base alle quali il controllo deve essere completo, neutrale e indipendente. Il CEPD osserva che la PPC non ha poteri di vigilanza in materia di attività di polizia e/o giudiziarie. Inoltre, seppure il controllo operato dalla Dieta, dalla commissione nazionale e prefettizia di sicurezza pubblica sembri essere neutrale e indipendente, occorrono ulteriori chiarimenti sui poteri di vigilanza delle commissioni prefettizie di pubblica sicurezza.

4.1.3 Mezzi di ricorso nel campo del diritto penale

174. Il progetto di decisione di adeguatezza, integrato dall'allegato II, indica varie modalità mediante le quali i singoli possono presentare i propri reclami dinanzi alle autorità indipendenti e ai giudici.

175. Tali modalità e gli elementi fondamentali di queste procedure, che derivano dalla documentazione disponibile, sono esposti in appresso, dopo una breve panoramica dei diritti disponibili, per chiarire cosa possono attendersi gli interessati dalle pubbliche autorità nel contesto del trattamento dei dati nel campo dei procedimenti penali.

4.1.3.1 Diritti a disposizione degli interessati nel contesto dei procedimenti penali

176. Al fine di poter proporre ricorso, gli interessati devono disporre di diritti previsti dalla legge che consentano loro di sostenere che tali diritti non sono stati rispettati. Pertanto, il CEPD ha valutato anche i diritti disponibili nel contesto dei procedimenti penali così come esposti nel progetto di decisione di adeguatezza.

4.1.3.1.1 Limitazioni generali ai diritti degli interessati ai sensi della APPIHAO

177. Nel suo progetto di decisione di adeguatezza, la COM si riferisce a e si basa sui principi generali di protezione dei dati che le pubbliche autorità devono rispettare, una volta che hanno raccolto dati personali. Tali principi sono ulteriormente delineati nell'allegato II, di modo che il CEPD ha deciso di fare osservazioni anche su essi.

178. Per quanto riguarda i diritti disponibili, il CEPD osserva che, secondo l'allegato II del progetto di decisione di adeguatezza, alcuni dei diritti generali conferiti agli interessati nel contesto del trattamento dei dati da parte degli organi amministrativi, restano disponibili anche nel contesto delle

[77] Vedere allegato II, pag. 11.

indagini penali. Tuttavia, dalla medesima APPIHAO derivano anche ulteriori limitazioni per quanto riguarda la raccolta e la successiva gestione delle informazioni personali in tale contesto.

179. Tali limitazioni, che sembrano applicabili sia nel contesto dei dati raccolti sulla base di un mandato, sia sulla base di un foglio di richiesta nel contesto della divulgazione volontaria, sollevano interrogativi su vari aspetti.

180. In merito al principio della limitazione della finalità, sebbene in teoria gli organi amministrativi siano tenuti a specificare la finalità per la quale conservano i dati personali e non devono conservarli al di là dell'ambito necessario per il conseguimento della finalità di utilizzo specificata, essi possono modificare la finalità se ciò "può essere ragionevolmente ritenuto adeguatamente rilevante rispetto alla finalità originaria".

181. La APPIHAO prevede anche il principio di non-divulgazione, secondo cui un dipendente non deve divulgare ad altri senza giustificato motivo le informazioni personali acquisite, né utilizzare tali informazioni per una finalità illecita. Non è però fornita alcuna ulteriore informazione sull'interpretazione di ciò che potrebbe rientrare nel "giustificato motivo" o nella "finalità illecita", sicché per la compiere la valutazione sarebbero necessari ulteriori chiarimenti.

182. L'articolo 8, paragrafo 1, della APPIHAO stabilisce anche il divieto di utilizzare o divulgare dati "salvo se diversamente previsto da leggi e regolamenti". Tuttavia, sebbene detta norma non sia in linea di principio contraria al livello di protezione apprestato dal diritto dell'UE, il CEPD non ha altri elementi relativi alla misura in cui sia operata un'eventuale vigilanza o siano effettuati eventuali controlli, quando la divulgazione è disposta da leggi o regolamenti. Inoltre, ai sensi dell'articolo 8, paragrafo 2, a questa regola si applicano ulteriori eccezioni laddove "tale divulgazione eccezionale non possa verosimilmente arrecare un danno ingiusto ai diritti e interessi dell'interessato o di un terzo". In mancanza di ulteriori elementi su questo punto, l'eccezione in esame, che si fonda sulla nozione poco chiara di "danno ingiusto ["], necessita di ulteriore chiarimento per comprendere se sia sufficientemente ristretta.

183. Infine, l'articolo 9 della APPIHAO prevede ulteriori restrizioni relative alla finalità o alla modalità di utilizzo o eventuali altre restrizioni, la cui imposizione spetta al capo di un organo amministrativo laddove le informazioni personali conservate siano fornite a un'altra persona. Poiché le nozioni di "eventuali altre restrizioni necessarie" e "fornite a un'altra persona" sono molto ampie, tali restrizioni aggiuntive ai diritti degli interessati sollevano preoccupazioni, in mancanza di ulteriori chiarimenti sull'ambito di applicazione di questa norma.

184. Sebbene il CEPD sia pienamente consapevole del fatto che i diritti di accesso e gli altri principi di protezione dei dati sono soggetti a limitazioni nei procedimenti penali anche ai sensi del diritto dell'UE, quando sono previste tali limitazioni si prevedono però garanzie aggiuntive, anche in termini di vigilanza, controllo e mezzi di ricorso. In mancanza di sufficiente giurisprudenza su queste limitazioni o di ulteriori elementi che chiariscano l'ambito di applicazione di tali norme, il CEPD non è in grado di valutare se tali limitazioni ai diritti degli interessati non travalichino ciò che sarebbe considerato strettamente necessario e proporzionato ai sensi del diritto dell'UE, e siano pertanto sostanzialmente equivalenti ai diritti conferiti agli interessati dell'UE.

4.1.3.1.2 Ulteriori limitazioni ai diritti della APPIHAO derivanti dal codice di procedura penale e dalle ordinanze della polizia prefettizia

185. Il CEPD rileva che sebbene la APPIHAO sembri essere applicabile a tutti i trattamenti operati in Giappone dagli organi amministrativi, alcune importanti limitazioni ai diritti degli interessati derivano

da specifiche normative. In particolare, l'articolo 53, paragrafo 2, del codice di procedura penale[78] prevede che "le informazioni personali registrate in documenti relativi al dibattimento e ai reperti sequestrati" sono escluse dal campo di applicazione dei diritti individuali di cui al capitolo IV della APPIHAO["]. In pratica, il CEPD ne deduce pertanto che nel contesto dei procedimenti penali, gli interessati non godono dei diritti di informazione, accesso, rettifica o cancellazione in relazione ai dati personali registrati in documenti relativi al dibattimento e ai reperti sequestrati.

186. Con riferimento a dette limitazioni, il CEPD deduce che esse si applicano nel contesto di dati raccolti sulla base di mandati, nonché nel contesto di dati raccolti a seguito della divulgazione volontaria mediante fogli di richiesta (vedi oltre). Infatti, poiché la base giuridica delle due procedure di accesso ai dati (mediante mandato e mediante un foglio di richiesta) si trova nel codice di procedura penale, l'articolo 53-2 di tale codice sembra si applichi a entrambe le fattispecie di raccolta. Tuttavia, poiché l'articolo 53-2 fa riferimento ai reperti "sequestrati" si potrebbe chiarire se le limitazioni ai diritti previste da questa norma si applicano anche nel contesto della divulgazione volontaria.

187. Il CEPD si rammarica di non aver avuto a disposizione le ordinanze della polizia prefettizia, che si afferma proteggano le informazioni personali, i diritti e gli obblighi analogamente alla APPIHAO. Date le incertezze relative all'interpretazione della APPIHAO e la mancata disponibilità delle ordinanze della polizia prefettizia, il CEPD si chiede se i diritti conferiti ai singoli in questo contesto e la vigilanza e/o i meccanismi di ricorso aggiuntivi siano sufficienti per compensare la mancanza di diritti.

4.1.3.2 Ricorso tramite autorità indipendenti

4.1.3.2.1 Ricorso amministrativo

188. Il CEPD rileva che gli organi amministrativi impegnati nella raccolta di dati, quali la polizia prefettizia, sono competenti a trattare le richieste provenienti dai singoli aventi ad oggetto i diritti - limitati – loro riconosciuti con riguardo ai dati raccolti nel contesto di indagini penali (vedere sopra per quanto riguarda i diritti disponibili), il che sembra includere sia la raccolta di dati sulla base di un mandato sia quella sulla base di fogli di richiesta. In pratica, questi diritti sembrano limitarsi ai principi generali, quali la necessità della conservazione dei dati in relazione alla finalità (vedere l'articolo 3.1 della APPIHAO), il principio di limitazione della finalità (articolo 4) o l'accuratezza dei dati (articolo 5), mentre i diritti individuali quali il diritto all'informazione, accesso, rettifica o cancellazione sono esclusi per i dati personali registrati nei documenti relativi al dibattimento e a reperti sequestrati[79]. Sebbene tali organi non possano essere considerati indipendenti né pertanto fornitori di mezzi di ricorso o di controllo indipendenti, il CEPD accoglie con favore tale strumento. Sottolinea tuttavia che i reclami presentati in tale contesto restano confinati a un numero molto basso di diritti degli interessati, date le limitazioni ai diritti previste dalla APPIHAO.

189. Inoltre, poiché le "informazioni personali registrate in documenti relativi al dibattimento e ai reperti sequestrati" sono escluse dal campo di applicazione dei diritti individuali di cui al capitolo IV della APPIHAO a norma degli articoli 53-2 del codice di procedura penale, le possibilità di chiedere l'accesso alle informazioni personali sono limitate alle procedure previste da altre disposizioni del codice di procedura penale. Sembra che soltanto le vittime, gli indagati o gli imputati possano agire in questo contesto e comunque in base alla fase del procedimento penale. Pertanto, il CEPD è preoccupato del fatto che gli interessati, ai sensi del diritto processuale penale giapponese, non hanno a disposizione

[78] Disponibile qui http://www.japaneselawtranslation.go.jp/law/detail/?printID=&id=2283&re=02&vm=02 e citato nell'allegato II del progetto di decisione di adeguatezza, nota a piè di pagina n. 25.

[79] Vedi sopra per quanto riguarda le limitazioni alla APPIHAO e in particolare l'articolo 53-2 del codice di procedura penale (non fornito ma citato nell'allegato II del progetto di decisione di adeguatezza, nota a piè pagina 25).

un diritto generale di accedere e/o rettificare o cancellare le informazioni, e che tutte le vie di ricorso a disposizione presuppongono la qualifica di vittima (nel qual caso la persona probabilmente sa che i suoi dati sono stati raccolti) o di indagato o imputato, o la dimostrazione di un danno, mentre gli interessati dovrebbero avere il diritto di accedere ai propri dati ed eventualmente di ottenerne la rettifica o la cancellazione anche quando non hanno subito alcun danno (neppure ipotetico) e/o quando non sono né vittime, né indagati né imputati, ma ad esempio testimoni.

4.1.3.2.2 Ricorso amministrativo mediante le commissioni prefettizie di pubblica sicurezza

190. Inoltre, sembra che le commissioni prefettizie di pubblica sicurezza siano competenti a gestire i reclami. Secondo l'articolo 79 della legge di polizia, cui si fa riferimento nel progetto di decisione di adeguatezza, i singoli possono presentare reclamo avverso qualsiasi comportamento illecito o improprio di un agente nell'esercizio delle sue funzioni.

191. Il CEPD chiede che sia chiarito se qualsiasi trattamento di dati personali "illecito" rientri nella definizione di "comportamento illecito o improprio di un agente" e chiede chiarimenti sulla necessità per l'interessato, a quanto sembra, di dimostrare il detrimento subito. Invero, la comunicazione inviata dalla NPA alle commissioni prefettizie di pubblica sicurezza sulla corretta gestione dei reclami riguardanti l'esercizio delle attività di funzionari di polizia limita i reclami a pretese concrete relative alla "riparazione di eventuali specifici svantaggi inflitti in conseguenza di una condotta illecita o inadeguata, o dell'omissione di una azione necessaria, da parte di un funzionario di polizia nell'esercizio delle sue funzioni" e alla possibilità di "presentare doglianze/dichiarazioni di insoddisfazione circa una modalità inadeguata di esercizio della funzione da parte di un funzionario di polizia". Si chiarisce espressamente che "i reclami sull'inadempienza di un funzionario di polizia che riguardano questioni che non si ritengono rientrare nelle funzioni di un funzionario di polizia, nonché quelli che esprimono generiche opinioni o proposte, che non incidono direttamente sulla parte reclamante medesima, dovranno essere rigettati".

192. Per quanto riguarda i requisiti processuali di presentazione dei reclami, sebbene questi debbano essere presentati per iscritto, il CEPD rileva che in tale contesto il diritto del Giappone prevede che venga fornita assistenza per la redazione del reclamo, anche a stranieri. Inoltre, il governo giapponese sembra aver conferito alla PPC anche il compito di fornire assistenza agli interessati dell'UE al fine di gestire e risolvere i reclami in questa materia, cosa che il CEPD accoglie favorevolmente. Il CEPD sottolinea che, per quanto consta, in tale contesto, la PPC fungerà solo da punto di contatto tra gli interessati dell'UE e le competenti autorità giapponesi.

193. Le decisioni della commissione prefettizia di pubblica sicurezza su un reclamo non dovranno essere comunicate nei casi elencati all'articolo 79-2 della legge di polizia, compreso il caso in cui l'attuale "residenza del reclamante è sconosciuta". Il CEPD riconosce che il riferimento alla residenza non comporta la conseguenza che gli interessati dell'UE saranno sempre esclusi dalla comunicazione degli esiti dei loro reclami perché non sono residenti in Giappone.

4.1.3.2.3 Meccanismo ad hoc riguardante la PPC

194. In considerazione dei predetti riscontri, il CEPD accoglie con favore il fatto che il governo del Giappone e la Commissione dell'UE abbiano concordato un ulteriore meccanismo di ricorso che mette a disposizione dei singoli dell'UE un ulteriore strumento di ricorso in Giappone, tramite il quale essi possono agire anche contro indagini illecite o improprie intraprese da pubbliche autorità. Il CEPD rileva e accoglie con favore il fatto che le richieste possono essere presentate anche presso la PPC, piuttosto che presso un altro funzionario amministrativo, estendendo così l'ambito della competenza della PPC al settore di polizia e giustizia e a quello della sicurezza nazionale.

195. L'impegno fondamentale del CEPD nell'analisi del nuovo meccanismo è stato capire i poteri di cui gode la PPC in tale contesto.

196. Sebbene la formulazione non sia del tutto chiara, il CEPD intende che il meccanismo aggiuntivo di ricorso non richieda la "legittimazione processuale" nel senso che l'istante non è tenuto a dimostrare che i suoi dati personali sono stati probabilmente sottoposti a vigilanza da parte di un'autorità del Giappone. Il CEPD vorrebbe comunque chiederne conferma alla Commissione.

197. In linea con la propria valutazione del meccanismo del mediatore (Ombudsperson) istituito ai sensi dello scudo per la privacy, il CEPD rimarca la necessità che siano conferiti poteri effettivi in capo al destinatario della richiesta, nella fattispecie la PPC, affinché il meccanismo di ricorso possa considerarsi sostanzialmente equivalente a un ricorso effettivo ai sensi dell'articolo 47 della Carta dei diritti fondamentali.

198. Nell'illustrare il meccanismo di ricorso, il governo del Giappone fa riferimento agli articoli 6, 61, punto (ii) e 80 della APPI ed espone tali poteri nell'allegato II. Il CEPD ritiene che la procedura descritta nell'allegato II precisi o estenda i poteri della PPC, in quanto la formulazione degli articoli 6, 61, punto (ii) e 80 della APPI è alquanto vaga e generica. Nella misura in cui l'allegato II precisa o estende i poteri della PPC, il CEPD vorrebbe chiedere chiarimenti sul fatto che le altre agenzie del governo del Giappone siano vincolate da tali poteri.

199. Sulla base della procedura di cui all'allegato II, il CEPD rileva che le pubbliche autorità competenti del Giappone sono tenute a collaborare con la PPC, "anche fornendole le necessarie informazioni e il materiale rilevante affinché la CEPD possa valutare se la raccolta o il successivo utilizzo delle informazioni personali sia avvenuto nel rispetto delle norme applicabili". Per valutare l'efficacia del sistema, è dunque importante fare ancora riferimento ai poteri di cui sono dotate le autorità competenti con le quali collabora la PPC. Il CEPD ritiene che tali poteri non sarebbero estesi mediante le rassicurazioni di cui all'allegato II.

200. Il CEPD rileva inoltre che se viene riscontrata una violazione delle norme, "la collaborazione delle pubbliche autorità interessate con la PPC include l'obbligo di sanare la violazione", il che include espressamente la cancellazione dei dati raccolti in violazione delle norme applicabili. Il CEPD ritiene che l'obbligo delle autorità competenti derivi dalla "collaborazione con la PPC" piuttosto che da una decisione della PPC.

201. Infine, la PPC informerà il richiedente sull'"esito della valutazione, comprese eventuali azioni riparatorie adottate, laddove possibile". Inoltre, la PPC informerà il richiedente sulla "possibilità di chiedere conferma dell'esito alla pubblica autorità competente e dell'autorità alla quale tale richiesta di conferma dovrà essere presentata".

202. Inoltre, la PPC si è impegnata ad assistere il richiedente nelle ulteriori azioni legali ai sensi del diritto del Giappone che questi vorrà intraprendere, qualora il richiedente non sia soddisfatto dell'esito della procedura.

203. In considerazione della necessità di un efficace meccanismo di ricorso che sia sostanzialmente equivalente agli standard dell'UE, il CEPD si chiede tuttavia se la PPC abbia poteri specifici ulteriori rispetto alla valutazione della conformità dell'attività di raccolta e di successivo utilizzo delle informazioni personali con le norme applicabili e al potere di richiedere alle autorità competenti di esercitare i loro rispettivi poteri e di gestire i reclami inoltrati loro dalla PPC. Se la PPC fungesse solo da punto di contatto per i singoli dell'UE, il CEPD lo riterrebbe insufficiente a fornire un meccanismo di ricorso effettivo sostanzialmente equivalente agli standard dell'UE. Il CEPD chiede quindi alla

Commissione di fornire chiarimenti sui punti citati nel presente sotto-capitolo, in particolare sul se e sul come il meccanismo estenda gli obblighi delle autorità competenti, su come queste siano vincolate dal meccanismo e su come la PPC possa garantire effettivamente la conformità e non fungere solo da punto di contatto per i singoli dell'UE.

4.1.3.3 Ricorso giurisdizionale

4.1.3.3.1 Meccanismo di quasi-reclamo

204. La cosiddetta procedura di "quasi reclamo" consente di opporsi alla raccolta coattiva di informazioni sulla base di un mandato per ottenere la revoca o la modifica di un sequestro illecito.

205. Questo mezzo di ricorso implica che il singolo sia a conoscenza del fatto che i dati sono oggetto di sequestro. Tuttavia, al CEPD risulta che la procedura di raccolta di dati sulla base di un mandato non viene comunicata all'interessato e, parimenti , che la divulgazione volontaria non implica l'obbligo per le società destinatarie della richiesta di informare gli interessati sulle richieste ricevute e alle quali hanno ottemperato. Pertanto, sebbene nell'allegato II si ponga l'accento sul fatto che "tale impugnazione può essere proposta senza che il singolo debba attendere la conclusione del procedimento", in concreto, eccezion fatta per i mandati che autorizzano le intercettazioni, per i quali si precisa che la legge prevede un requisito di notifica[80], questo mezzo di ricorso sembra essere di fatto esperibile soltanto una volta che l'interessato venga a conoscenza della raccolta a seguito di una citazione in giudizio.

4.1.3.3.2 Provvedimenti cautelari

206. Inoltre, al fine di ottenere la cancellazione di dati raccolti nel contesto di un procedimento penale (attraverso il cosiddetto "provvedimento cautelare") o per ottenere il risarcimento dei danni, i singoli possono proporre un'azione legale civile in sede giudiziaria.

207. Per quanto riguarda il risarcimento, il CEPD rileva che la procedura sembra essere circoscritta a situazioni in cui un pubblico ufficiale nell'esercizio delle sue funzioni cagioni illecitamente un danno al singolo interessato, con colpa o dolo,. Per quanto consta al CEPD, il concetto di danno sembra includere il danno morale. Non è però indicato con ulteriori dettagli quali elementi probatori debbano essere forniti dal singolo a dimostrazione del danno lamentato. Il CEPD non è stato in grado di valutare la giurisprudenza sul riconoscimento di risarcimenti, e pertanto non può valutare se tale strumento fornisca un mezzo di ricorso efficace in caso di danni.

208. Per quanto riguarda il "provvedimento cautelare", il CEPD rileva altresì che per farne richiesta il singolo dovrebbe in primo luogo essere a conoscenza del fatto che i suoi dati sono stati raccolti e che sono tuttora conservati. Pertanto, considerati i limitati diritti di informazione e accesso di cui godono i singoli nel contesto delle indagini e delle procedure penali, anche l'efficacia di tale procedura sembra essere alquanto limitata.

4.1.3.4 Valutazione complessiva dei mezzi di ricorso

209. In seguito alla valutazione di tutti i mezzi di ricorso a disposizione dei singoli ai sensi del diritto del Giappone nonché a disposizione degli interessati dell'UE dinanzi alla PPC, il CEPD accoglie con favore il meccanismo ad hoc di risoluzione delle controversie, che coinvolge la PPC. È un valore aggiunto per gli interessati dell'UE, in particolare poiché consente loro di capire quali mezzi di ricorso hanno a disposizione al fine di ottenere un ristoro e/o un risarcimento, nonché di presentare le loro richieste

[80] L'articolo 23 della legge sulle intercettazioni è citato alla pagina 33 del progetto di decisione di adeguatezza, ma al CEPD questo testo non è stato fornito e pertanto non è in grado di valutare in quale misura tale obbligo di notifica si applichi e in quali casi possa essere limitato.

secondo i requisiti procedurali applicabili ai sensi del diritto del Giappone. Sono tuttavia necessari ulteriori chiarimenti, in particolare sul se e come il meccanismo si estenda agli obblighi delle autorità competenti, su come queste siano vincolate dal primo e su come la PPC possa effettivamente garantire la conformità, al fine di accertare che tale nuovo meccanismo costituisca un ricorso effettivo.

210. La presente valutazione mostra che nessun meccanismo di ricorso nel diritto del Giappone sembra consentire l'accesso, la rettifica o la cancellazione di dati agli interessati che non sono vittime, indagati o imputati nel contesto di un procedimento penale, ad esempio al fine di rimediare alla raccolta o conservazione illecita dei loro dati. Si evidenzia anche che tutti i meccanismi e le procedure di ricorso e di risarcimento a disposizione delle vittime, degli indagati o degli imputati ai sensi del diritto del Giappone presuppongono la conoscenza della raccolta dei dati, il che nella pratica sembra verificarsi limitatamente, dato che sono conferiti limitati diritti di accesso e informazione in casi del genere. Sembrano inoltre necessari ulteriori chiarimenti sui requisiti previsti a dimostrazione di una condotta illecita da parte delle autorità, in particolare se tale condotta includa qualsiasi trattamento illecito di dati personali, nonché a dimostrazione del danno patito dal singolo.

211. Pertanto, in mancanza di ulteriore documentazione ed elementi, il CEPD dubita che i mezzi di ricorso previsti dal diritto del Giappone e dal progetto di decisione di adeguatezza siano sufficientemente efficaci rispetto agli standard del diritto dell'UE.

4.2 Accesso per finalità di sicurezza nazionale

4.2.1 Finalità della vigilanza

212. Nel progetto di decisione di adeguatezza, il capitolo sull'"accesso e utilizzo da parte delle pubbliche autorità del Giappone per finalità di sicurezza nazionale" è introdotto da una dichiarazione generale, conforme alla rassicurazione fornita dal governo del Giappone nell'allegato II, secondo cui il diritto del Giappone non prevedrebbe e quindi non consentirebbe "richieste coattive di informazioni o di 'intercettazioni amministrative' al di fuori delle intercettazioni di carattere penale". Si conclude affermando che "sul fondamento della sicurezza nazionale, le informazioni possono essere ottenute soltanto da una fonte di informazioni liberamente accessibile da chiunque o mediante divulgazione volontaria. Ciò esclude qualsiasi sorveglianza occulta in questo settore. Gli operatori economici che ricevono una richiesta di divulgazione volontaria (sotto forma di divulgazione di informazioni in formato elettronico) non sono giuridicamente obbligati a fornire tali informazioni"[81].

213. All'interno di tali limiti, sono elencati quattro enti governativi che hanno il potere di raccogliere informazioni in formato elettronico detenute dagli operatori economici giapponesi per motivi di sicurezza nazionale. Per quanto riguarda il ministero della Difesa, che è uno dei predetti quattro enti, si afferma che esso "ha solo il potere di raccogliere informazioni (in formato elettronico) mediante divulgazioni volontarie"[82].

214. Nella propria valutazione del sistema generale della raccolta di dati per finalità di sicurezza nazionale, il CEPD intende richiamare la prima delle cosiddette "garanzie essenziali", secondo la quale "il trattamento dovrebbe basarsi su norme chiare, precise e accessibili"[83]. Più in particolare, la Corte EDU è stata molto chiara nel dichiarare che i programmi di sorveglianza sono "conformi alla legge" solo se

[81] Decisione di adeguatezza, punto 151.
[82] Decisione di adeguatezza, punto 153.
[83] WP29, WP 237: Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) [Documento di lavoro 01/2016 sulla giustificazione delle interferenze con i diritti fondamentali alla vita privata e alla protezione dei dati mediante misure di sorveglianza nel contesto del trasferimento di dati personali (Garanzie essenziali europee)].

le misure di sorveglianza "hanno un qualche fondamento nella legge nazionale". La corte ha chiarito che la compatibilità con lo stato di diritto richiede che la legge che autorizza la misura sia accessibile e che i suoi effetti siano prevedibili. Per quanto riguarda il rischio di arbitrarietà, la corte ha richiesto "norme chiare e dettagliate sulle misure di sorveglianza occulta"; "sufficientemente chiare per fornire ai cittadini indicazioni adeguate sulle circostanze e le condizioni in cui le pubbliche autorità hanno il potere di fare ricorso a tali misure"[84].

215. Per quanto riguarda l'applicazione di tali garanzie essenziali all'ordinamento giuridico del Giappone, il CEPD è consapevole non solo del fatto che, in materia di sicurezza nazionale, gli stati hanno un ampio margine di discrezionalità, riconosciuto dalla Corte europea dei diritti dell'uomo, ma anche che i poteri relativi alla sicurezza nazionale rispecchiano le esperienze storiche attraversate dalle nazioni. Il CEPD riconosce che, come sottolineato dal governo del Giappone, dopo la seconda guerra mondiale ai servizi di informazione del Giappone sono stati conferiti poteri più limitati rispetto a quelli di altri stati.

216. Nella lettura del CEPD, il progetto di decisione di adeguatezza, conformemente alle rassicurazioni del governo del Giappone, suggerisce che gli enti governativi del Giappone non attuano programmi che monitorano in modo strategico o sorvegliano in senso ampio la comunicazione (su Internet). Come detto prima, il governo del Giappone ha fornito rassicurazioni, in una lettera firmata dal ministro della Giustizia, che "per motivi di sicurezza nazionale, le informazioni possono essere ottenute soltanto da una fonte di informazioni liberamente accessibile da chiunque o mediante divulgazione volontaria".

217. Per quanto riguarda la base giuridica del ministero della Difesa, il CEPD osserva che il progetto di decisione di adeguatezza contiene informazioni generali sui suoi poteri e cita la sua missione di "condurre gli affari ad essi relativi al fine di garantire la pace e l'indipendenza nazionali, e la sicurezza della nazione". Tuttavia, al CEPD non è stata fornita una traduzione in inglese della base giuridica.

218. Allo stesso tempo, il CEPD è a conoscenza delle notizie pubblicate in vari mezzi di comunicazione, dalle quali risulterebbe che vi sono programmi di sorveglianza gestiti dalla Direzione per l'intelligence dei segnali del ministero della Difesa (MOD) del Giappone[85]. Nei suddetti articoli, si afferma altresì che il ministero della Difesa del Giappone, pur rifiutando di commentare nel dettaglio, ha "riconosciuto che il Giappone mantiene 'uffici in tutto il paese' che intercettano comunicazioni" che "sarebbero concentrati sulle attività militari e sulle 'minacce informatiche' e non 'raccolgono le informazioni del pubblico in generale'". Quest'ultima affermazione (che il MOD non raccoglie informazioni sul pubblico in generale) fa parte di una dichiarazione di conferma da parte del governo del Giappone.

219. Resta il fatto che il governo del Giappone ha confermato, in una lettera firmata dal Ministro della giustizia, che il MOD non raccoglie informazioni sul pubblico in generale.

220. Esula dalle funzioni del CEPD effettuare una valutazione generale delle eventuali capacità di sorveglianza del governo del Giappone. Una tale valutazione è pertinente solo se le attività suddette investono il trasferimento di dati personali fra l'UE e il Giappone. In questo contesto, il CEPD vorrebbe ribadire l'approccio, già adottato dal suo predecessore [cioè il Gruppo di lavoro "Articolo 29"] quando è stato richiesto di un parere sullo scudo UE-USA per la privacy. Nel fornire un parere sullo scudo per la privacy, il Gruppo di lavoro "Articolo 29" ha inserito nella propria analisi i poteri e limiti degli USA afferenti la sorveglianza dei dati "in transito" verso gli USA[86]. Applicando lo stesso criterio alla decisione

[84] Vedere ad esempio Big Brother Watch e altri / Regno Unito, punto 305.

[85] Nel maggio 2018, la testata giornalistica online "The Intercept" ha pubblicato un articolo intitolato "The untold story of Japan's secret spy agency [La storia mai raccontata dell'agenzia di spionaggio segreta del Giappone"]).

[86] Vedere WP255, EU-U.S. Privacy Shield –First annual joint review [scudo per la privacy UE-USA - Prima revisione congiunta annuale], adottato il 28 novembre 2017, pag. 16: "Il WP29 è del parere che l'analisi delle normative del paese terzo oggetto dell'adeguatezza non dovrebbe limitarsi al diritto e alla prassi che consente la

di adeguatezza sul Giappone, il CEPD ritiene che siano pertinenti le informazioni sui poteri delle autorità del Giappone afferenti la sorveglianza sui dati "in transito" verso il Giappone. Qualora tali poteri di sorveglianza esistano, anche la pronuncia della Corte EDU nella causa Big Brother Watch sembra suggerire che tali poteri dovrebbero essere regolati secondo i criteri fissati dalla Corte EDU stessa.

221. Di conseguenza, se le intercettazioni fossero limitate al "supporto di azioni militari", potrebbero senz'altro risultare irrilevanti ai fini della valutazione della decisione di adeguatezza. È quindi interesse del CEPD ricevere dagli enti governativi del Giappone chiarimenti sulle misure di sorveglianza. Al riguardo, tali chiarimenti sarebbero accolti con favore al fine di stabilire se i dati trasferiti ai sensi del quadro di adeguatezza in esame potrebbero essere oggetto di accesso da parte delle competenti autorità del Giappone per scopi di sicurezza nazionale.

4.2.2 Divulgazione volontaria in caso di sicurezza nazionale

222. Il progetto di decisione di adeguatezza afferma che i quattro enti governativi hanno soltanto il potere di raccogliere informazioni (in formato elettronico) mediante la divulgazione volontaria. Secondo il progetto di decisione di adeguatezza e l'allegato II, vi sono alcune limitazioni di natura legislativa, nel senso che la raccolta dei dati è limitata a quanto necessario per l'esercizio delle funzioni degli enti.

223. In materia di diritto penale, come citato nella sezione relativa alle attività giudiziarie e di polizia, la divulgazione volontaria è consentita solo nel contesto di un'indagine penale, il che presuppone un concreto sospetto di un reato che è già stato commesso. Le indagini in materia di sicurezza nazionale differiscono dalle indagini di polizia e giudiziarie. Il CEPD riconosce che, ai sensi dell'allegato II, i principi fondamentali della "necessità dell'indagine" e della "adeguatezza del metodo" si applicano in modo analogo al settore della sicurezza nazionale e devono essere rispettati tenendo nel dovuto conto le circostanze specifiche di ciascun caso[87]. Si rammarica del fatto che la relativa applicazione non sia ulteriormente chiarita, anche mediante ulteriori riferimenti alla giurisprudenza. Tuttavia, il CEPD afferma che l'utilizzo di tale procedura deve essere proporzionato o necessario.

224. Secondo il progetto di decisione, quando siano state raccolte ("ottenute") informazioni personali, la loro gestione è regolata dalla APPIHAO, tranne per quanto riguarda la polizia prefettizia[88]. L'allegato II afferma che la gestione delle informazioni personali da parte della polizia prefettizia è regolato da ordinanze prefettizie che sanciscono principi a tutela delle informazioni personali, diritti e obblighi equivalenti a quelli previsti dalla APPIHAO[89]. Poiché non sono disponibili traduzioni in inglese di tali ordinanze, il CEPD non è in grado di valutare se i principi siano equivalenti a quelli di cui alla APPIHAO.

225. Per gli altri commenti sulla divulgazione volontaria, si fa riferimento alla sezione relativa alle attività di polizia e giudiziarie.

4.2.3 Supervisione

4.2.3.1 Considerazioni generali

226. I quattro enti governativi abilitati a raccogliere informazioni in formato elettronico detenute dagli operatori economici giapponesi per motivi di sicurezza nazionale sono: (i) l'Ufficio ministeriale

sorveglianza all'interno delle frontiere fisiche di quel paese terzo, ma dovrebbe anche includere l'analisi dei fondamenti giuridici del diritto di quel paese che gli consentono di esercitare la sorveglianza al di fuori del suo territorio, nella misura in cui sono interessati dati dell'UE["]. Come già sottolineato nel suo precedente parere, "dovrebbe essere chiaro che i principi dello scudo per la privacy si applicheranno dal momento in cui ha luogo il trasferimento di dati, il che significa anche per quanto riguarda i dati "in transito" verso quel paese".

[87] Vedere allegato II, pag. 23.

[88] Decisione di adeguatezza, punti 118 e 157.

[89] Vedere allegato II, pag. 3.

informazioni e ricerca (CIRO, Cabinet Intelligence and Research Office); (ii) il ministero della Difesa ("MOD"); (iii) la polizia (sia l'agenzia nazionale di polizia (NPA)[90] sia la polizia prefettizia); e (iv) l'agenzia di informazioni per la sicurezza pubblica ("PSIA", Public Security Intelligence Agency).

227. Secondo il progetto di decisione di adeguatezza, tali enti governativi sono soggetti a vari livelli di supervisione da tre rami del governo[91]. Il CEPD rileva che esistono meccanismi di supervisione all'interno dell'organo legislativo (Dieta del Giappone) e dell'organo esecutivo (Ufficio dell'Ispettore generale per la conformità alla legge (IGO), commissioni prefettizie di pubblica sicurezza e commissione di controllo sulla sicurezza pubblica). Il CEPD sottolinea che la Commissione dovrebbe fornire chiarimenti sulla supervisione giurisdizionale (d'ufficio/garanzia C del WP 237, per i mezzi di ricorso vi è un capitolo separato nel progetto di decisione e una garanzia extra nel WP 237) sui predetti organi di governo, in quanto non è chiaro se vi sia un controllo giurisdizionale in materia di raccolta di informazioni personali per finalità di sicurezza nazionale senza mezzi coattivi.

4.2.3.2 Controllo da parte della Dieta del Giappone

228. Il CEPD rileva che la Dieta del Giappone può svolgere indagini sulle attività delle pubbliche autorità, e pertanto anche su tutti i predetti enti governativi. Inoltre, la Dieta può anche richiedere la produzione di documenti e la deposizione di testimoni (*articolo 62 della Costituzione, articolo 104 della legge sulla Dieta*). Il CEPD rileva altresì che, ai sensi degli *articoli 74 e 75 della legge sulla Dieta*, i membri della Dieta possono formulare domande scritte al governo che possono avere come esito una risposta fornita dal governo stesso (*articolo 75 della legge sulla Dieta*). Infine, si rileva che vi sono anche specifici obblighi di resoconto, ad esempio in capo all'agenzia di informazioni per la sicurezza pubblica (PSIA) (articolo 36 SAPA/articolo 31 ACO) mediante la presentazione di una relazione annuale alla Dieta. Tale relazione non è stata fornita al CEPD.

4.2.3.3 Supervisione da parte dell'Ufficio dell'Ispettore generale sulla conformità alla legge (IGO)

229. Il CEPD osserva che vi è un organo di supervisione per il MOD, detto IGO. Al CEPD non è stata fornita la legge istitutiva del MOD (Legge di istituzione del MOD), ma solo le dichiarazioni di cui all'allegato II del progetto di decisione. Ai sensi dell'allegato II, l'IGO è un ufficio indipendente interno al MOD, posto sotto la diretta vigilanza del ministero della Difesa, ai sensi dell'articolo 29 della legge istitutiva del MOD. L'IGO ha i poteri di svolgere ispezioni sull'osservanza di leggi e regolamenti da parte dei funzionari del MOD (cosiddette "ispezioni difensive"), in tutto il ministero, comprese le forze di difesa.

230. Ai sensi dell'allegato II, l'IGO esercita le proprie funzioni in modo autonomo rispetto ai dipartimenti operativi del MOD. Il CEPD osserva che l'IGO è un organo di supervisione *interno*.

231. Le ispezioni hanno come esito accertamenti e, allo scopo di garantire la conformità, misure che sono segnalate direttamente al ministro della Difesa. Sulla base della relazione dell'IGO, il ministro della Difesa può emettere provvedimenti di attuazione delle misure necessarie a risolvere la situazione. Il viceministro della Difesa è responsabile per l'attuazione di tali misure e deve relazionare al ministro della Difesa sullo stato di tale attuazione.

232. Analizzando l'allegato II, e non disponendo delle norme giuridiche (Legge istitutiva del MOD), il CEPD accoglie con favore la possibilità di ordinare le necessarie misure di conformità per risolvere la situazione. Tuttavia, il CEPD solleva preoccupazioni riguardo l'indipendenza dell'IGO, in quanto si tratta di un ufficio interno al MOD sotto la diretta vigilanza del ministro della Difesa ai sensi dell'allegato II

[90] Tuttavia, in base alle informazioni ricevute, la funzione principale della NPA è coordinare le indagini dei vari dipartimenti della polizia prefettizia e le sua attività di raccolta di informazioni sono limitate agli scambi con autorità estere.

[91] Vedere allegato II, pag. 39.

(secondo il *WP 237 "l'autonomia funzionale non è di per sé sufficiente a tutelare quell'autorità di vigilanza da ogni influenza esterna*").

233. Conformandosi alla giurisprudenza della Corte EDU e al WP 237 seguendo rispettivamente le considerazioni di cui all'allegato II, l'Ispettore generale può chiedere relazioni agli uffici interessati (documenti, siti, spiegazioni). Secondo il CEPD, sono necessari chiarimenti sull'eventuale obbligo a carico degli uffici interessati di dare seguito a queste richieste e sulla questione se i documenti richiesti includano materiali riservati, come cita il WP 237, o meno.

234. Sebbene il CEPD accolga con favore il fatto che a capo dell'IGO siano posti giuristi molto esperti (già procuratori sovrintendenti), sembrano necessari chiarimenti sulle modalità di nomina di quest'organo di vigilanza.

4.2.3.4 Supervisione da parte della Commissione di controllo sulla sicurezza pubblica

235. Secondo l'allegato II (pagina 25), la PSIA svolge ispezioni periodiche e specifiche sull'attività dei suoi singoli uffici e dipartimenti (Ufficio informazioni per la sicurezza pubblica, Dipartimenti e sotto dipartimenti di informazioni per la sicurezza pubblica, ecc.). Ai fini delle ispezioni periodiche, sono nominati ispettori un assistente direttore generale e/o un direttore. Tali ispezioni dovrebbero anche riguardare la gestione delle informazioni personali.

236. Ai sensi del considerando 163 del progetto di decisione di adeguatezza, la commissione di controllo sulla sicurezza pubblica opera come organo indipendente di vigilanza preventiva per conto della PSIA, con riferimento alle materie oggetto della ACO[92] e della SAPA[93]. Il CEPD accoglie con favore quanto sopra.

237. Sebbene il sito web del ministero della Giustizia del Giappone fornisca alcune informazioni[94], il CEPD non è in grado di valutare con precisione in misura ulteriore l'indipendenza della Commissione di controllo sulla sicurezza pubblica, in quanto non sono state fornite né la legge istitutiva della commissione di controllo sulla sicurezza pubblica[95], né le norme della commissione di controllo sulla sicurezza pubblica[96].

4.2.3.5 Supervisione da parte della commissione nazionale di pubblica sicurezza, delle commissioni prefettizie di pubblica sicurezza e della APPIHAO (esecutivo)

238. Vedere 3.1.2.2.1 (Commissione nazionale di pubblica sicurezza), 3.1.2.2.2. (Commissioni prefettizie di pubblica sicurezza) e 3.1.2.2.4. (Esecutivo)

4.2.3.6 Supervisione da parte della PPC

239. Il CEPD invita la COM a citare nel considerando 164 che la PPC non è un organo di supervisione sui predetti enti governativi e che essa è competente solo sui ricorsi dei singoli, oppure a spostare il passaggio sulla PPC presente nel considerando 164 nella sezione "ricorso individuale".

---

[92] Legge sul controllo delle organizzazioni che hanno commesso atti di strage (legge n. 147 del 7 dicembre 1999).
[93] Legge sulla prevenzione delle attività sovversive (legge n. 240 del 21 luglio 1952).
[94] Vedere http://www.moj.go.jp/ENGLISH/MEOM/meom-01.html (settembre 2018): L'organo non ministeriale *"è composto da un presidente e sei membri. Essi sono scelti fra persone di buona reputazione in grado di emettere un giudizio equo sul controllo delle organizzazioni e con ampia conoscenza ed esperienza sia giuridica sia sociale. Sono nominate dal primo ministro e devono essere approvate da entrambe le camere della Dieta. Per quanto riguarda l'applicazione delle predette leggi (SAPA/ACO), i membri esercitano le loro funzioni con piena indipendenza, liberi da qualsiasi direttiva o vigilanza da parte del primo ministro o del ministro della Giustizia."*
[95] http://www.japaneselawtranslation.go.jp/law/detail_main?re=&vm=2&id=613 (settembre 2018).
[96] Articolo 28 della ACO.

4.2.4 Meccanismo di ricorso

240. Per l'analisi del meccanismo di ricorso oggetto del nuovo negoziato, si fa riferimento alla sezione sulle attività di polizia e giudiziarie.

241. Inoltre, occorre rilevare che il diritto del Giappone prevede uno specifico mezzo di ricorso individuale in materia di sicurezza nazionale. A giudizio del CEPD, ogni persona, compresi gli interessati dell'UE, può chiedere agli organi amministrativi in via generale la comunicazione, la correzione (compresa la cancellazione) o la sospensione dell'utilizzo, anche se il trattamento è operato per finalità di sicurezza nazionale. Qualora tale richiesta sia "respinta con la motivazione che l'informazione in oggetto è ritenuta non divulgabile", si può proporre un'impugnazione per il riesame e deve essere consultato il "comitato di riesame sulla divulgazione di informazioni e la tutela delle informazioni personali" Il comitato è composto da membri nominati dal primo ministro con il consenso di entrambe le camere, è dotato di poteri investigativi ed emette una relazione scritta diretta al singolo interessato, che non è giuridicamente vincolante ma è quasi sempre rispettata[97]. Secondo l'allegato II, in soli due casi su 2000 si è verificato che un'autorità amministrativa si sia pronunciata in senso difforme dalle conclusioni del comitato[98].

242. Dalle spiegazioni fornite sembra derivare che il riesame non è esperibile se l'informazione può essere "divulgata" ma il singolo non è soddisfatto del risultato. Il CEPD prende atto di tale mezzo di ricorso, ma vorrebbe chiedere ulteriori chiarimenti su quest'ultimo aspetto, che potrebbe limitarne significativamente la portata.

Per il comitato europeo per la protezione dei dati

La presidente

(Andrea Jelinek)

[97] Allegato II, pagg. 25, 26. Legge istitutiva del comitato di riesame sulla divulgazione di informazioni e la tutela delle informazioni personali, articoli 4, 9, 11.
[98] Allegato II, nota a piè di pagina n. 35.